Cyberdefense

Security Navigator 2024

Research-driven insights to build a safer digital society

Hugues Foulon

Executive Director at Orange and
CEO Orange Cyberdefense

We are very pleased to provide to the cyber security community the next edition of the Security Navigator. Our position as part of one of the largest telecom operators in the world, and as a leader in cyber security services and research, gives us profound insights. It has become our custom to share this unique view of the cyber security landscape.

There is no denying that this has been a year of fundamental changes for most of us.

Geopolitical disorder has hit countries and society at probably the worst possible time and will severely decelerate recovery after COVID for years. The digital world is becoming a virtual battleground for state-backed APT groups and political hacktivists. Not only businesses, but whole economies find themselves being targeted for political reasons, or at risk of becoming collateral damage. Shifting the focus from monetary gain to mere destruction of "the enemy" has left the threat landscape in turmoil.

But aside from all the crisis we are also on the brink of yet another technological revolution. With incredible speed Generative Artificial Intelligence has started to impact and shift the way we think about and interact with computer technology. The transformative power this has on shaping our economy, security and our everyday life is yet to be determined.

Being aware of one's vulnerabilities is key to avoid becoming the weak link. We all must join our efforts to build up resilience and protect the digital space. Not only for ourselves, but for our customers, suppliers, employees and the community. Hence our mission is to build a safer digital society. CISOs do that every day.

This is not an easy job. Cyber security is complex. Keeping track of technological evolution means to constantly re-learn, re-evaluate and re-educate yourself and your peers. At Orange Cyberdefense we are tirelessly working to offer you the best guidance and support along this way.

With that goal in mind, our multi-disciplinary experts have digested all this unique information and synthesized our key findings in this report, to the benefit of our clients and of the broader cyber security community. These insights are also crucial for us to keep being relevant as a company.

Trends got confirmed, others are emerging. Cyberextortion emerges as the most prominent form of attack with a strong increase in the past year and a geographical shift towards EMEA and Asia Pacific. Small and medium companies are gaining ground as favourite vulnerable targets. Insightful observations like that should help us navigate the threat landscape – as a closely-knit community. We are proud and humbled every day to be trusted with the security of our clients' most important assets, and we are deploying the best expertise and technology in all domains to protect their business.

Thank you for your trust and we hope you enjoy reading this edition of the Security Navigator!

Hugues Foulon

Table of contents

Introduction:

What you need to know

Olivier Bonnet De Paillerets
EVP Marketing & Technology
Orange Cyberdefense

> **In our shared technological adventure, people and safety must be our primary concern.”**

The Security Navigator reflects first and foremost the reality of the conflictual nature of cyber warfare. It mirrors the disinhibition of threat actors motivated by state strategies or hacktivism as well as criminal opportunities. In this environment, espionage, sabotage, disinformation and extortion are becoming increasingly intertwined.

The long-term state of war on Europe's doorstep, the risks of polarization of the Hamas-Israel war, and the rise in tensions in the Indo-Pacific arc all remind us that security remains and will remain even more so tomorrow at the heart of organizations' technological and human development strategies.

This unstable and unpredictable environment must convince us of the need to unwaveringly pursue a policy of prevention and support for our increasingly interconnected organizations. We must integrate the major comparative advantage of an independent analysis of cyber threats in its technical and geopolitical dimensions in order to refine organizational cyber risk management. Equally we must complement it with a cyber crisis management capability firmly anchored in corporate governance.

I also feel it is necessary to stress the extent to which the sovereignty of our data and its use, as well as the implementation of standards, will gradually become necessary to frame our security policies.

It is in this context that Orange Cyberdefense regularly reviews the state of the threat. Once again this year, it is thanks to the incidents investigated by our security monitoring centers (SOCs and CyberSOCs), the vulnerability scans carried out by our Vulnerability Operations Center (VOC), the reports of our teams carrying out penetration tests, and finally, our network analyses that our Security Navigator 2024 is born.

Our very singular ability to gather data from very different sources both within Orange and externally, cross-referencing and analyzing them assures the relevance of this report.

Data from the Security Navigator 2024 highlights a few trends, including:

- A dynamic cybercrime ecosystem, that expands its operational mode by directly targeting company personnel in order to better penetrate their systems.
- Cyber criminals accelerating the geographical lateralization of their attacks, targeting not only Anglo-Saxon countries or Europe which nevertheless are still strongly impacted.
- An increase in cyberattacks that should be seen on mobile devices, where our personal and business data are increasingly concentrated.
- Continued targeting of Scientific and Technical IP, the financial sector, and particularly of Industrial and Manufacturing infrastructure.
- An explosion of Cyber hacktivism over the past two years to support political or social demands.

Today, the Security Navigator is one of the central elements of Orange Cyberdefense’s threat analysis, insights of which must go beyond Chief Information Security Officers (CISOs) and security experts. It is complemented by the ‘Executive Security Navigator’, a dedicated report intended to support them in raising awareness and driving actions with their organization’s leadership, anchored on the reality of the risks induced by this cyber threat.

This document is also intended to become the cornerstone of the partnership of trust that we wish to build with you. It must enrich our debates within a community that is still too isolated. For example, we invite you to take advantage of all our analytical capabilities through articles reflecting on the importance of the human factor in an attack, and stories from our response teams, in order to continue to acculturate your environment on cyber security.

Above all, it emphasizes the extent to which in our common technological adventure, people and security must be our primary concern.

I hope you enjoy reading!

Charl van der Walt
Head of Security Research
Orange Cyberdefense

Summary

This is what happened

We've never used the word 'unprecedented' in a Security Navigator before, and we won't do it this year either. But there's no denying that the 12 months of cybersecurity captured in this report have been extraordinary.

The tempo, the severity, the complexity, and the consequences of developments in our domain have accelerated to dizzying levels.

Our World Watch service published 491 advisories for the period October 2022 through September 2023, averaging over 40 advisories per month. No advisories with Urgency Critical were issued for the period. This is somewhat astonishing given the almost overwhelming scale and frequency of security 'drama' that occupied our minds. Yet the CISOs we speak to universally wear a kind of 'thousand yard' stare and report being nearly overwhelmed by the ferocity of the security news cycle.

No single effort could hope to capture, comprehend, and convey all the security industry has seen and learned since we last published this report. Instead, we aim to share what we at Orange Cyberdefense have observed or considered first-hand. We cross-reference and analyze the data we collect from our diverse operations and own research. We describe the pictures we see in that data and share our efforts to answer the questions it raises for us. With this somewhat lopsided effort we hope to illuminate in some small way those parts of the landscape we can shine a light on, and present insights and observations we hope will enable security practitioners to make better-informed decisions that deliver the positive security outcomes our digital world desperately needs.

We begin with a summary of key events, themes and observations.

Incidents & Attacks

Cl0p, Cl0p, Cl0pping on heaven's door

The security incident that 2023 will probably be remembered for was the series of attacks with cascading impacts by the Cl0p Cy-X group. Cl0p was credited with exploiting vulnerabilities in the public facing managed file transfer (MFT) solution of MOVEit Transfer by vendor Progress Software. This was the third MFT solution Cl0p exploited in almost three years. In early February 2023 news reports of victims associated with another MFT called GoAnywhere emerged[1]. This time a 0-day was targeted in Internet-facing GoAnywhere services and was a repeat of the playbook that CL0p was starting to perfect.

We've been tracking Cl0p for 41 months now. While they've historically been a relatively low-profile actor, their recent successes against prominent enterprise platforms completely changed their profile.

Cl0p has claimed 514 victims in 43 different countries, but the effectiveness of their unique modus operandi in 2023 is clear to see.

Cl0p impacted so many 2nd and 3rd level victims that it completely distorted our Cyber Extortion (Cy-X) victim data, which we explore extensively in this report. Cl0p accounts for 373 victims in 2023, significantly inflating the 2563 victims recorded for this period from other actors.

The 'Finance and Insurance' sector in particular recorded a 106% increase in Cy-X victims, largely at the hands of Cl0p.

The Cl0p incidents illustrated just how much damage a single well-placed security blow can do. It spawns passionate arguments about software supply chain security and raises concerns about the resilience of the cloud and SaaS offerings so many businesses rely on. But it also reminds us of the issue of 'interdependence', which is a fundamental characteristic of cyberspace and cybersecurity.

Microsoft faces the STORM (-0558)

In 2023, Microsoft announced that an attacker, identified as STORM-0558, gained unauthorized access to Exchange Online data hosted in Azure by abusing Outlook Web Access (OWA)[2]. The attackers had targeted a subset of accounts belonging to specific organizations. At the time, Microsoft conceded that they couldn't explain how the attackers had obtained the private key of the MSA certificate used in the attack and was still investigating the matter. This inactive MSA key enabled attackers to fool the process that checks authentication token signatures, as the forged authentication token was signed by the trusted certificate. In a follow-up post by Microsoft, the firm speculated that the attacker obtained the private MSA key material from an unredacted crash dump of a host that had the key material in its memory. The crash dump was allegedly obtained from a compromised Microsoft engineer's debug workstation, to which the dump file had been copied[3].

The higher we Jump(Cloud) the harder we fall

JumpCloud was the victim of a cyberattack in mid-2023 that prompted them to force a rotation of privileged API keys. Shortly after this Mandiant published a report in which they described how attackers gained access to a victim's network and deployed malicious scripts using JumpCloud Agents. Mandiant reported that the activity matched adversaries with strong links to the Democratic People's Republic of North Korea (DPRK).

Incidents like the STORM-0558 attack against Microsoft, the JumpCloud compromise, and more attacks impacting Okta and in turn impacting 1Password, BeyondTrust, and Cloudflare show us how we have collectively been shifting our attack surface from the Internet perimeter to the desktop, to the cloud[4][5][6][7]. The homogeneous Microsoft desktop environment has historically enabled massive ROI for threat actors, but the same homogeneity is characteristic of successful enterprise-oriented cloud offerings and similarly presents attackers with a compelling ROI.

The STORM-0558 breach of Microsoft' Outlook cloud offering was broadly attributed to a (Chinese) state actor, and state-backed actors of various forms have been as active as ever over the past year.

(In)Security impacts governments

In July 2023 the Norwegian government announced that 12 government departments were impacted by a cyberattack[8]. The attackers leveraged a previously unknown critical vulnerability in the Ivanti Endpoint Manager Mobile (EPMM)[9] that allowed the attackers to access users' Personally Identifiable Information (PII). A second vulnerability was also reported a few days later that could, if combined with the first, result in a fully functioning backdoor[10]. A Proof-Of-Concept (POC) was published shortly thereafter, putting the exploit in the hands of anyone wanting to test it[11]. Ivanti then announced a third vulnerability[12]. The publicly available POC means that these older versions are at great risk of being exploited.

A Volt of lightning

In May 2023, Microsoft reported[13] on the activities of a Chinese threat actor named 'Volt Typhoon', that is considered responsible for targeting critical infrastructure providers and other sectors in Guam and elsewhere in the United States.

According to Microsoft, Volt Typhoon has been breaching critical infrastructure in the USA since 2021[14]. Volt Typhoon was compromising vulnerable 'internet-facing Fortinet FortiGuard devices' and then moved further through the victim's infrastructure using features and capabilities available on the network in a technique known as Living-Off-the-Land. Microsoft's report states that Volt Typhoon also used compromised routers and Small Office Home Office (SOHO) network equipment to act as a proxy, making the attacker's network traffic look mundane.

Microsoft claims that Volt Typhoon is allegedly affiliated with the Peoples Republic of China (PRC). Notable about the incident is Microsoft's assessment that Volt Typhoon is 'pursuing development of capabilities that could disrupt critical communications infrastructure between the United States and Asia region during future crises'.

The case is an important first glimpse at an inevitable and anticipated next evolution of conflict in cyberspace, in which one of the crucial weaknesses of offensive cyber capabilities is addressed: the outcome of cyber operations is not a linear certainty. Unlike a missile that can be deployed, loaded, and fired with predictable results at a moment's notice, a cyber operation is more like the deployment of ground troops or an aircraft carrier - complex, nuanced, unpredictable. Cyber operations can take an indeterminate amount of time to have an effect.

When governments play (smaller countries lose)

The war against Ukraine has of course continued to fuel ongoing cyber activities. Mandiant detailed the strategic cyberattack playbook used by Russian attackers against Ukrainian targets[15]. Pre-invasion actions involved reconnaissance, followed by destructive attacks just before the Russian invasion of Ukraine in February 2022. Pressure was sustained against targets throughout 2022. The report also mentions the introduction of new personas in the form of hacktivists such as the CyberArmyofRussia_Reborn, to amplify and propagate falsehoods about Russia's progress in the war.

Hacktivism and pre-emptive attacks by state-backed actors will feature again later in this report.

There have been countless other examples of government hacking campaigns against multiple targets – too many to mention in this report – so we highlight just a few here:

- The United Kingdom's Electoral Commission announced in August 2023 that 'hostile actors' had breached it and accessed Personal Identifiable Information (PII) of registered voter's data[16]. At the time of writing, the Electoral Commission had not provided details besides the fact that PII was stolen[17]. Some speculated that a vulnerable Microsoft Exchange Server could be linked to the incident, but that has not been explicitly confirmed[18].
- In August 2023, the China National Computer Virus Emergency Response Center (CVERC), along with a cyber security company, announced that they had discovered the compromise of a data collection station at the Wuhan Earthquake Monitoring Center[19]. The CVERC attributed the attack to intelligence agencies of the United States of America. CVERC claim that the goal of the implant was to allow the attackers to steal monitoring data as part of reconnaissance and intelligence gathering procedures.
- A threat actor with ties to the Chinese government, tracked as UNC4841 by Mandiant, have allegedly exploited an unknown weakness (0-day) in the Barracuda Email Security Gateway (ESG) since October 2022[20][21]. Attacks spread across 16 countries and were so persistent, it prompted Barracuda to instruct their clients to completely replace the hardware appliance rather than rely on the software fix to close the backdoor.

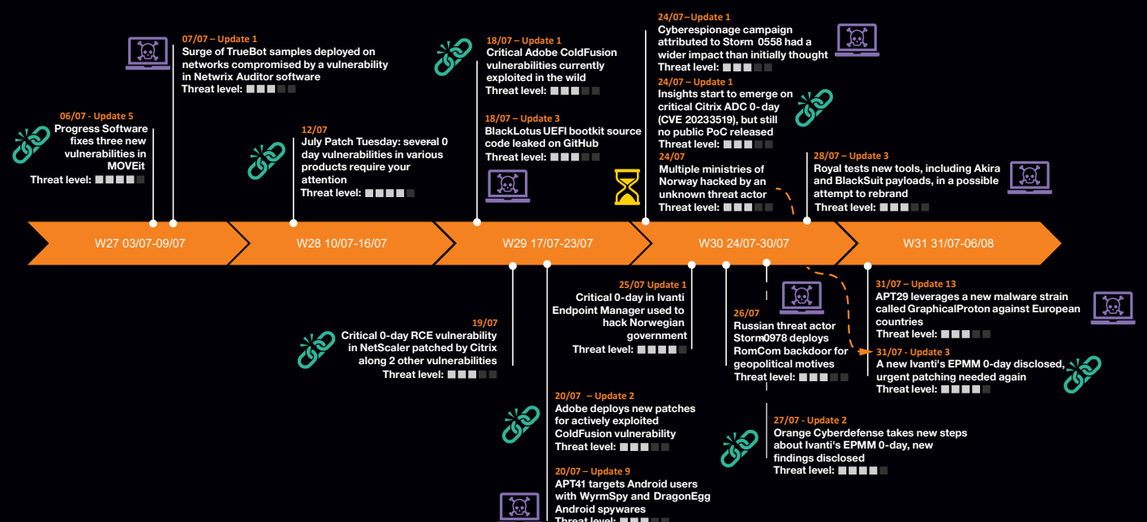
The Belfer Center's National Cyber Power Index[22] ranks countries that have some degree of "cyber power". In 2022 the ten "most powerful cyber nations" were considered to be the U.S.A, China, Russia, the United Kingdom, Australia, the Netherlands, Republic of Korea, Vietnam, France and Iran. But the index tracks 30 such countries, there are doubtless others, and the list is growing.

With practice, cyber operations have become an effective tool, and at a relatively low price point they are becoming increasingly popular.

Smaller and developing nations also become victims of compromise by other nations, either as direct targets or as simple staging positions for operations with other objectives.

Losing control over technology implies losing control over autonomy. Every government is an 'e' Government. And every human is a citizen of cyberspace. This is a digital world and digital security is an essential part of the core infrastructure on which this world is built. National security therefore demands robust and consistent national cybersecurity but achieving that is far from trivial. The larger and more complex technology and systems become, the more difficult it is to defend, to the point where a tenable defense tends toward a practical impossibility.

Main cybersecurity advisories produced by Orange Cyberdefense World Watch in July



0h (days) my goodness

July 2023 was a particularly busy time for 0-days, with news breaking of a vulnerability in Citrix ADC (CVE-2023-3519) that was potentially being exploited in the wild. There were several others.

By their very nature, it's hard to keep track of the number of 0-days. In September this year Ars Technica asserted[23] that with 70 zero-days uncovered so far this year, 2023 is on track to beat the previous record of 81 set in 2021.

Our own internal 'Vulnerability Watch' Exploit Database (EDB) records 109 CVEs tagged with "Exploited in the Wild", but of course those are not necessarily 0-day.

The practice of vulnerability management, prioritization and patching is still far from mature, and is becoming ever more urgent.

Hacktivism

Hacktivism can be understood as a form of cyberattack that is conducted to further the goals of political or social activism. It aims to draw public attention to an issue or cause the hacktivist believes in[24].

Hacking, crime, espionage, politics, and ideology have long been difficult to tease apart, and hacktivism has always been a central, if somewhat benign, element of this complex mix.

But the past 2 years we have seen an apparent increase of activity in the hacktivism space.

With the war against Ukraine, we observed a significant surge in hacktivist activity supporting both sides of the conflict.

Examples included the hacker collective Anonymous declaring 'war' on Russia[25] and the Ukrainian Minister of Digital Transformation Mykhailo Fedorov calling on individual hackers on the internet for help[26][27], thus creating the first IT Army of Ukraine[28].

While the geopolitical rhetoric escalated, so too did the force and impact of the Denial-of-Service attacks recently favored by hacktivists.

Indeed, hacktivism and mis/disinformation have emerged as two sides of the same coin and have increasingly come to characterize the use of cyber within geopolitical conflicts.

Two hacktivist groups that we have been tracking are Anonymous Sudan and Noname057(16). Both are directly or indirectly engaged with the ongoing war against Ukraine.

In investigating these two active pro-Russian hacktivist groups, we discover major differences in the groups' modus operandi, but note how powerful hacktivist activity can be in creating fear, uncertainty, and doubt (FUD). Anonymous Sudan has apparently succeeded in this, especially in the Nordics. Geopolitical tensions in the region escalated to the point that Sweden and Denmark had to introduce measures to preserve safety, and Sweden raised their terror threat level after encountering heavy international unrest. Denmark introduced a bill prohibiting the burning of religious scripts.

We are seeing a continuous evolution towards 'cognitive' attacks, which seek to shape perception through technical activity. The impact has less to do with the disruptive effect of the attack or the value of the data or systems that are affected but with the impact that these attacks will have on societal perception.

Cyber Extortion

We recorded 8,948 victims of Cyber Extortion between January 2020 and the writing of this report.

This is just a partial view of the whole problem of Cyber Extortion, however. With insights gleaned from the recent take-down of the Hive group, for example, we estimate that actual victim numbers may be 5 or 6 times higher than what we see.

2023 sees the highest number of victims we have ever collected, with the number of Threat Actors also returning to the (previous high) levels of 2021. In this year's report we note with concern that roughly the same number of actors can cause much more damage than they did 2 years ago.

Big game harvest

We believe that Cy-X payments decreased significantly in 2022 because of the disruptive impact of the war against Ukraine. Cy-X was further impacted by improved security practices, resilient data backup, and regulatory efforts like sanctions, cryptocurrency controls, and Law Enforcement actions. But also, simply because victims were refusing to pay.

In 2023, the industry is increasingly talking about the resurgence of 'Big Game Hunting', but we prefer the term 'harvest' over 'hunt'. As we describe in detail in this report, Cyber Extortion is largely opportunistic, and victim groups are impacted primarily due to their population size and vulnerability, rather than the discretion of Threat Actors.

Acting poorly

We have never recorded as many threat actors as in the past 12 months. The war against Ukraine appears to have distracted actors and disrupted activity in the Cy-X space. Almost exactly a year after the start of the war, activity has accelerated again, and new Cy-X operations are emerging rapidly.

Crossing over

Current geopolitical events have also politicized some Cy-X actors[29], some of whom have become more politically driven.

Conti, CoomingProject, and Stormous all proclaimed their full support for Russia in the war against Ukraine[30]. Ransomedvc suggested an intent to attack Iran and Palestine after the Hamas-Israel war broke out[31]. And Cuba group members have reportedly run espionage operations targeting government and military officials in Ukraine[32][33].

"Crossovers" have gone in the other direction also. The hacktivist group Anonymous Sudan, for example, at one point was demanding ransoms to stop their ongoing DDoS attacks[34]. The hacktivist group GhostSec also turned to ransomware and launched their own RaaS offering and released its own ransomware strain[35].

But confusion between cybercrime and hacktivism has grown deeper than that.

A pro-Ukraine hacktivist group called 'Ukrainian Cyber Alliance' apparently took down the Trigona ransomware leak site and its servers.[36]

The Trigona take down was not an action against cybercrime, however, but part of a politically driven effort to disrupt any Russian cyber operation.

Not a victimless crime

It's not only hacktivism that has a detrimental effect on society. Our analysis in this report shows that Cy-X has impacted every single industry (a total of 20 industries) and spread across 108 countries this year. Some of the sectors impacted provide essential services for society, including Telecommunications and Broadcasting, Passenger, Water, Air, and Rail Transportation, Education, and Healthcare, which have all seen significant increases in the past 12 months.

This year we report an increase in victim numbers almost everywhere we look, not only in the commonly impacted large, Anglophile economies, but also in South East Asia, India, Africa, Oceania and elsewhere. We believe Cyber Extortion is primarily a crime of opportunity so this year we continue to explore why some countries or regions are impacted more than others.

We argue again in this year's Navigator that the primary factor influencing victim demographics is the size of the target population. Bigger economies and bigger industries will in general tend to be impacted more. Where we see deviations from this general pattern, as we describe in this report for countries like Japan, or industries like Manufacturing, these emerge primarily from attributes of the victims rather than deliberate choices made by the Threat Actor.

Law Enforcement Activities

In this year's report we explore the increased efforts by governments, local authorities, and international collaborations to counter cybercrime. In the last two and a half years we've seen a steady increase in Law Enforcement (LE) activity, recording 102 actions to counter cybercrime in some way. Cyber Extortion is the leading target of these actions, followed by Hacking, Crypto Crime, and Fraud. Almost 60% of LE activities involved arrests and the sentencing of individuals or groups. These actions were supported by technical takedowns, which was the next most common activity.

Later in this report we examine how effective LE disruption efforts have been thus far, by examining the lifespan of Threat Actors and noting how they have changed over time. 54% of Cy-X 'brands' disappear after 1 to 6 months. 2023 has seen a further escalation in volatility: While 25 groups disappeared after 2022, a further 23 survived from the previous year, and a record 31 new Cy-X brands were identified.

Distributing DDoS

Besides Data Extortion and the classic ransomware, we also observed a small amount of DDoS threats made by the Cy-X group NoEscape. This is interesting since we last saw threats to DDoS from a long-gone group called Avaddon.

Most of the hacktivist attacks we've recorded also use Distributed-Denial-of-Service (DDoS) attacks, and some have developed sophisticated DDoS capabilities, which are also becoming more available as services.

In June 2023 Microsoft detailed[37] ongoing DDoS activity by the threat actor they track as STORM-1359. They assessed that the attacks relied on access to multiple virtual private servers (VPS), in conjunction with rented cloud infrastructure, open proxies, and DDoS tools. More interestingly, the DDoS activity targeted Layer 7 (L7) rather than the OSI Layer 3 or 4, as is most often the case.

We reported at the time that these types of attacks require a different approach. A cleverly designed L7 attack is more difficult to execute, but can demand even more processing by the server, creating a kind of asymmetry and quickly depleting server resources.

DDoS has sometimes been thought of as a mere nuisance in the past, but it's been becoming more effective and available to actors of all kinds. In the current convergence between politically motivated attacks and Cyber Extortion – both of which involve a form of psychological coercion – DDoS is assuming a more important role.

Since the emotional impact of a DoS attack is powered by the attacker's message, the actor can choose to make a political statement out of any apparently successful attack. Targeting can be highly opportunistic, which greatly exacerbates the technical asymmetry already faced by defenders in cyberspace.

Vulnerabilities and Exploits

In 2023, we tracked renewed interest in Vulnerability Intelligence and prioritization. As defenders are increasingly overwhelmed by waves of new vulnerabilities and exploits, the challenge of patching and mitigation remains as intractable as ever, and attackers have rediscovered the art (and benefit) of exploiting vulnerable systems over the internet.

Vulnerability is getting old

This year we revisit the menacing vulnerability theme with an eye on the ever present and lingering tail of unresolved system weaknesses. We assess over 2.5m vulnerability findings that we reported to our clients, and over 1,500 reports from our professional ethical hackers, to understand the current state of security vulnerabilities and consider their role and effectiveness as a tool for prioritization.

The bulk of unique Findings reported by our scanning teams - 79% - are classified as 'High' or 'Medium', and 18% of all serious findings are 150-days or older. Though these are generally dealt with more swiftly than others, some residual still accumulates over time. While the number of findings we identify are resolved rapidly after 90 days, 35% of all findings we report persist for 120 days and longer. Too many are never addressed at all.

While our scanning results illuminate the persistent problem of unpatched vulnerabilities, our Ethical Hacking teams more frequently encounter newer applications and systems built on contemporary platforms, frameworks and languages.

17.67% of findings our Ethical Hackers reported were rated as 'Serious', but the hackers must work harder today to discover them then they had to in the past.

Hacking getting harder

The Ethical Hacking dataset we examine for this report includes clients from over 10 different countries.

From this data we assess that our hacking teams had to work 13% harder in 2023 than in 2018 to match the level of findings reported per project day.

The average time spent per project to report a serious finding is 10.5 days.

Hacking Intelligently and patching intelligently

Only an estimated 4.1% to 5.5% of all vulnerabilities in 2020 were considered exploitable, and this reality hasn't changed[38][39].

The Exploit Prediction Scoring System (EPSS) by FIRST is a relatively new statistically-derived metric designed to help the vulnerability management process by illuminating vulnerabilities that are more likely to be exploited[40]. EPSS could help focus security teams on vulnerabilities that should be patched first.

In this report we explore the notion that Ethical Hacking, as a form of vulnerability identification and prioritization, also acts as a source of highly contextual vulnerability intelligence.

By scaling EPSS scores so that they can easily be compared with the scores assigned by Ethical Hackers, we note that EPSS and Ethical Hacking scores correlate quite closely, but vary across different target types.

Most importantly, however, a total of 177 (85.92%) CVEs were reported by our testers that have a lower EPSS score. In other words, a skilled attacker matching our Ethical Hacking team's skill would have found 177 potentially serious vulnerabilities that would probably not have been prioritized using EPSS.

Using our own in-house Exploit Database as a reference, we are unable to reproduce the very encouraging conclusions of previous research that used more 'theoretical' frames of reference. This year we thus continue to explore more efficient ways to employ Vulnerability Intelligence in the 'real world'.

CyberSOCs on the Cold Face

As always, we strive to provide a global overview of what we are seeing in our incident data. To facilitate this a broad data set is collected from across our 14 CyberSOCs responsible for supporting clients around the globe. This year we have had a full year's worth of data based on using the VERIS framework to better categorize our incidents.

In total 129,395 incidents were detected and responded to, all of which were investigated by human security analysts in one of our CyberSOCs. These investigations resulted in 25,076 'True Positive' confirmed security incidents being raised with our customers - 19%.

The VERIS 'Hacking' category retains the lion's share of recorded incidents, accounting for almost ~30% of incidents. Historically, 'Malware' has been a top category, but this year it slipped to 4th place. The Misuse category was again 2nd, almost in line with last year's report.

We add a second level of detail to the top level VERIS Threat category, so we can derive a more detailed view of the underlying cause of the incidents. The top three combined incident types are:

- Web Attack - Hacking,
- Unapproved hardware/software/script/workaround – Misuse, and
- Port Scan – Hacking.

Together, these incidents constitute over 45% of all categorized Incidents. All three of these incident types retain their ranking from last year but increased their percentage share of incidents considerably.

Industries under fire

In this report we use our propriety 'Coverage Score' to produce a normalized comparison of the volume of incidents encountered by our clients in different industries. On this normalized basis we assess that our clients in the Manufacturing sector deal with almost 3 times as many incidents as the next most impacted sector – Retail Trade. Within our client base these sectors are followed by 'Professional, Scientific, and Technical Services', 'Finance and Insurance' and 'Accommodation and Food Services'.

Dealing with the noise

Every year since we started the Navigator, we've kept track of the ratio between confirmed 'True Positive' findings, and 'Other' Incidents with statuses like False Positives, Unconfirmed, and others.

The proportion of True Positive (Confirmed) incidents to all Incidents recorded has decreased from 45% in 2020 to 19% of total Incidents this year.

We have a tight definition of a 'Confirmed' True Positive Incident, which requires us to receive specific confirmation from the Client. The higher number of potential incidents impacts our teams and not our clients, as our analysts review each potential incident before it is escalated.

We find that the overall ratio between Confirmed and Other Incidents is actually misleading, as this ratio varies greatly from client to client. We observe this year that the efficiency of mature, established clients can be four times higher than that of new clients who are just starting their onboarding journey with us, and we argue that this client maturity is strongly expressed in the frequency with which we receive feedback on incidents.

We also show that while the 'quantity' of incidents we report to our clients has decreased proportionally over the years, the 'quality' has actually increased. We argue that this is a function of detection tuning, more rigorous analysis, and other service enhancements.

The Threat Detection Maturity Wave

Finally, this year we introduce the 'Threat Detection Maturity Wave', which captures the repeating phases of data ingestion and tuning that ultimately lead to a slope of enlightenment where Confirmed Incidents constitute almost half of all processed events and appear to continue trending gradually upwards from there.

Operating Securely

What made Stuxnet such a watershed moment in Operational Technology (OT) security is the complexity and precision with which it targeted OT specific hardware and software. But the lines of what constitutes a cyberattack on OT have never been well defined. If anything, they have further blurred over time.

Operational technology is the hardware and software that is used to monitor, control, and manage the physical environment in an industrial process. OT is commonly found in sectors such as manufacturing, energy, water treatment, utilities, transport, and healthcare.

From the barrage of reports on cyberattacks affecting OT, it's easy to get the impression they are targeted and sophisticated. But are OT environments really besieged by a constant barrage of complex cyberattacks?

In this year's report we define 5 types of cyberattacks that can affect OT. We then analyze 35 years of OT attacks and assess what kinds of attacks we've really been seeing in the OT space.

From our analysis of the history of OT cyberattacks, we note that the landscape is shifting towards techniques that target IT, and only inadvertently impact OT. This trend provides fortunate breathing room for OT defenders.

The current Cy-X attacks impacting IT systems are proving to be very lucrative for criminals, and the veritable pandemic of ransomware and extortion may get worse before it gets better. But if organizations build up a resilience to contemporary Cy-X attacks, we should expect the criminal modus operandi (MO) to change. Could we see an evolution of Cy-X that impacts OT directly?

Dead Man's PLC

While considering a potential shift to criminals targeting OT, we also consider what shape it might possibly take. We present a novel and pragmatic Cy-X technique specifically targeted against OT devices; in particular, PLCs and their accompanying engineering workstations.

We call it Dead Man's PLC.

Dead Man's PLC works by adding to legitimate, operational PLC code to create a covert monitoring network, whereby all the PLCs remain functional but are constantly polling one another. If the polling network detects any attempt from the victim to respond to the attack, or the victim does not pay their ransom in time, polling will cease, and Dead Man's PLC will trigger a "Dead Man's switch" and detonate.

Detonation involves deactivating the legitimate PLC code, responsible for the control and automation of the operational process, and activation of malicious code that causes physical damage to operational devices.

It has generally been believed that OT-specific Cy-X presents an unlikely risk, due to the requirements placed on criminals from a technical perspective. However, in this report we argue Dead Man's PLC is an effective and pragmatic technique for holding the entire operational process to ransom.

This should act as a starting point for defenders to rethink the risk ransomware and Cy-X could pose to OT, beyond the current surge of IT attacks and the conventional Cy-X we see today.

The power of GRC

How governance, risk and compliance (GRC) can shape the backbone of your security strategy

While many organizations may work with these three elements individually, the true power of GRC principles lies in their ability to synergize with each other and, at the same time, harmoniously align with business objectives and strategic goals.

Together, the GRC principles form a holistic, strategic, and protective ”umbrella” that safeguards critical areas, including OT Security and Mobile Device Security, against a broad spectrum of cyber threats.

Margarita Sallinen, Information Security Consultant, **Orange Cyberdefense**

Adapting to complex cyber threats

Cyber threats range from well-established approaches like phishing attacks to emerging ones like Cyber Extortion, hacktivism and AI-driven attacks by cybercriminals. In addition to providing comprehensive defense, GRC principles offer a strategic framework for mitigating financial and reputational risks while preserving an organization's brand. Achieved through governance, robust risk management, and stringent compliance measures, this approach enables organizations to navigate the complex domain of cyber threats with resilience and confidence.

It's not 'just a tech problem'

Cybersecurity is usually associated with tech, code, firewalls, and encryption algorithms. But equating security with technology is a misconception; and implementing solutions alone can lead to a false sense of protection. Of course deploying the right tools and having the appropriate expertise to respond and recover from cyber security incidents is essential. However, as risks have grown more intricate, and threats more pervasive, technology alone is not sufficient to ensure cyber resilience.

As cyber threats evolve, they introduce new challenges, spanning from Operational Technology (”OT”) risks, encompassing critical infrastructure, to vulnerabilities associated with Mobile Device Security, which impact nearly every employee. Within this evolving threat landscape, organizations now face consequences such as breaches, financial losses, and reputational damage, prompting them to carefully consider where to direct their cybersecurity efforts. Therefore, it has become imperative to zoom out and adopt a broader, and more comprehensive perspective.

The Critical role of the C-suite

Leadership, including the Board and C-suite executives, plays a pivotal role in adopting the GRC framework into the organization's cybersecurity strategy. Cybersecurity resilience should start in the boardroom.

A strong commitment to cybersecurity initiatives drives substantial change and fosters a resilient cybersecurity culture, seamlessly integrating cybersecurity with strategic planning rather than treating it as an afterthought.

C-suite executives must champion GRC principles in cybersecurity, and send a clear message throughout the organization that cybersecurity is not merely a technical concern but a critical aspect of risk management and corporate governance. This mindset should permeate every department, from the boardroom to employees handling sensitive information, ultimately creating a culture of cyber resilience. When the boardroom treats cybersecurity as a strategic business imperative it sets the expected behavior for the rest of the organization.

Redefining the Cybersecurity Strategy

To effectively adapt to and navigate the shifting threat landscape, organizations must transcend the boundaries of traditional IT-focused cybersecurity strategies. Instead of relying solely on reactive measures and asking, "Why would it happen to us?" organizations should embrace a holistic approach grounded in resilience and proactive measures. They should recognize the profound importance of Governance, Risk Management, and Compliance (”GRC”) principles as a foundational framework for cybersecurity.

Understanding GRC Principles

For an organization's cybersecurity strategy to excel, GRC should rightfully claim the spotlight. To gain a comprehensive understanding of this framework and unlock its benefits, it's essential to delve into the individual GRC principles first.

Governance: The Strategic Compass

Governance is the strategic compass for an organization's cybersecurity, aligning the strategy with the given objectives. It sets clear goals, policies, and proactive strategies. For example, in safeguarding customer data, governance establishes policies like encryption, access controls, and incident response plans, aligning cybersecurity with broader business strategies to protect the organization against emerging threats.

Risk Management: The Agile Watchdog

Risk management is like a vigilant cybersecurity watchdog. It entails proactively identifying, assessing and mitigating risks. Anticipating and enabling preventive measures to minimize their impact is also essential. Risk management can entail threat modeling and developing countermeasures, effectively bolstering incident response capabilities.

Compliance: The Steadfast Lighthouse

Compliance, like a dependable lighthouse, ensures organizations navigate the complexities of the cyber domain while upholding legal and ethical standards. It encompasses adherence to laws, regulations, and standards, verified through regular audits. When new regulations arise, compliance involves reviewing processes, updating policies, and conducting audits to maintain legality, ethics, and enhance incident response as per regulatory expectations.

To summarize: governance sets the direction; risk management identifies potential obstacles; and compliance ensures cybersecurity practices remains lawful and ethical.

Five practical GRC implementation tips

While understanding the individual GRC principles is important, practical implementation blending all three is where organizations can be most effective.

1. Define Clear Governance Policies

Establish comprehensive governance policies that clearly define roles, responsibilities, and decision-making processes related to cybersecurity. Ensure alignment with your organization's strategic objectives. Engage key stakeholders, including leadership, IT teams, and legal departments, in policy development.

2. Conduct a Cybersecurity Risk Assessment

Start by identifying your organization's unique cybersecurity risks. Understand the threats you face, the vulnerabilities in your systems, and the potential impact of security incidents. This assessment serves as the foundation for tailored governance, risk management, and compliance strategies.

3. Stay Compliant

Continuously monitor and maintain compliance with relevant laws, regulations, and industry standards. This includes conducting regular audits and assessments to ensure adherence to cybersecurity best practices. Keep abreast of regulatory changes that may impact your organization.

4. Foster a Cybersecurity Culture

Promote a culture of cybersecurity awareness and responsibility throughout the organization. Train employees to recognize and respond to threats effectively. Encourage reporting of security incidents and near misses.

5. Continuously Evaluate and Improve

Cybersecurity is an ongoing journey. Regularly assess the effectiveness of your GRC principles and make adjustments as needed. Conduct post-incident reviews to identify areas for improvement.

Key takeaways

The Power of GRC in cybersecurity is realized when Governance, Risk Management, and Compliance (GRC) principles synergize, while aligning with business objectives. This holistic approach yields multiple benefits, including the minimization of operational inefficiencies, improved communication, and enhanced risk mitigation. GRC principles play a pivotal role in this context, offering a comprehensive framework that bridges technology with strategic goals.

GRC principles not only protect critical areas but also mitigate financial and reputational risks. Leadership's commitment, especially in the boardroom, is crucial to fostering a culture of cyber resilience.

Basic Data analysis

Key data of the year

We collect and analyze two fundamental forms of data for the Security Navigator: data produced by our internal operations – Threat Detection, Security Intelligence, Vulnerability Scanning and Ethical Hacking – and data we collect specifically for research purposes, namely Cyber Extortion victims, (limited) Hacktivism attacks.

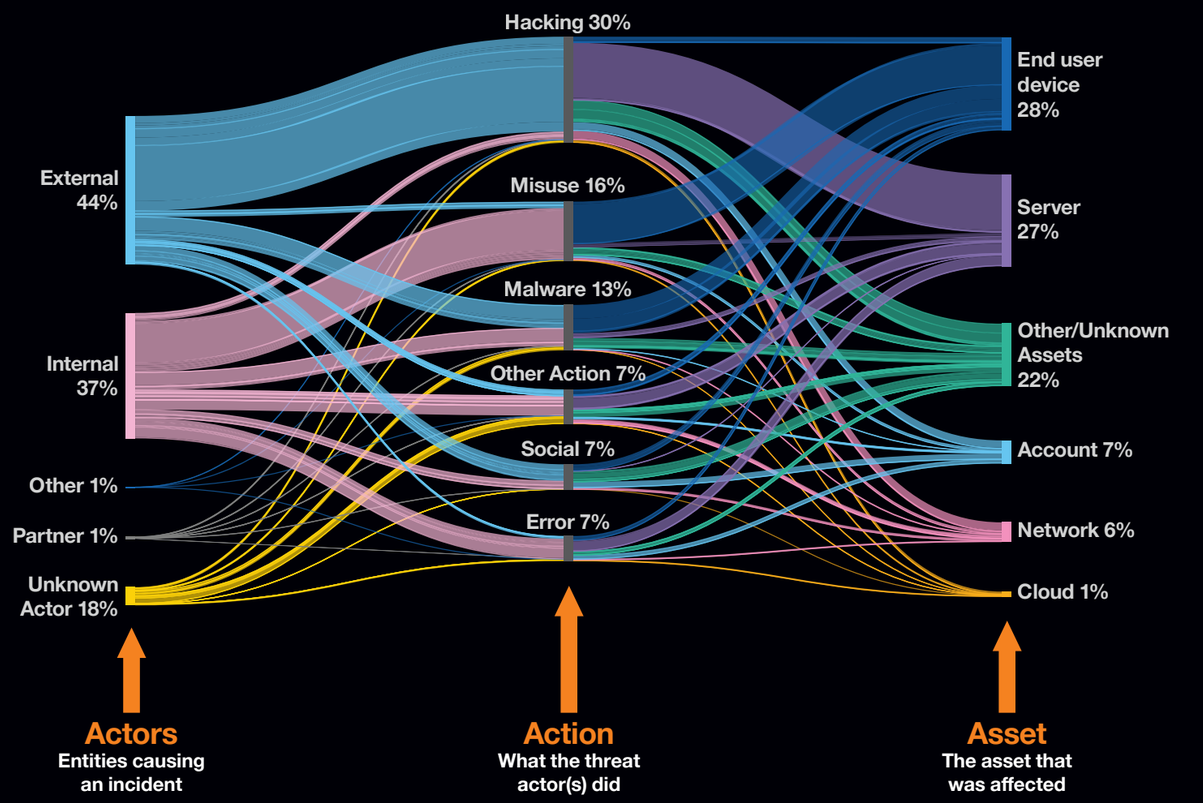
In this chapter we present an analysis of each of these data sources individually, then also apply this data elsewhere in the report to answer specific research questions.

Threat Detection

About the data

- Total of incidents: 129,395 (up from 99,506 in 2022)
- Out of these incidents, 25,076 could be confirmed as True Positive Incidents (19%)
- Period analyzed: October 2022 to September 2023
- Data sources: firewalls, directory services, proxy, endpoint, EDR, IPS, DNS, DHCP, SIEM and our managed threat detection platform

Funnel: Alert to incident → 129,395 Potential incidents → 25,076 Confirmed Incidents



* Overview flow with major categories, for details see following pages

Types of incidents

We announced in our previous report that we were in the process of adopting the industry standard VERIS (Vocabulary for Event Recording and Incident Sharing) framework for incident classification across our SOCs. This has now been rolled out to the majority of our CyberSOCs, meaning most of the data in scope for this report now uses this classification framework, allowing us to provide analysis based solely on VERIS.

4A

Actor	THREAT ACTORS are entities that cause or contribute to an incident.
Action	THREAT ACTION describe what the threat actor(s) did to cause or contribute to the incident.
Asset	ASSET describes the information assets that were compromised during the incident.
Attribute (CIA)	Which security ATTRIBUTES were compromised during the incident?

Threat Actions

The Threat Action categories used in the VERIS framework consist of the following 7 primary categories:

Malware

Malware is any malicious software, script, or code run on a device that alters its state or function without the owner's informed consent. Examples include viruses, worms, spyware, keyloggers, backdoors, etc.

Hacking

Hacking is defined within VERIS as all attempts to intentionally access or harm information assets without (or exceeding) authorization by circumventing or thwarting logical security mechanisms. This includes brute force, SQL injection, cryptanalysis, denial of service attacks, etc.

Social

Social tactics employ deception, manipulation, intimidation, etc to exploit the human element, or users, of information assets. Includes pretexting, phishing, blackmail, threats, scams, etc.

Misuse

Misuse is defined as the use of entrusted organizational resources or privileges for any purpose or manner contrary to that which was intended. Includes administrative abuse, use policy violations, use of non-approved assets, etc. These actions can be malicious or non-malicious in nature. Misuse is exclusive to parties that enjoy a degree of trust from the organization, such as insiders and partners.

Physical

Physical actions encompass deliberate threats that involve proximity, possession, or force. Includes theft, tampering, snooping, sabotage, local device access, assault, etc.

Error

Error broadly encompasses anything done (or left undone) incorrectly or inadvertently. Includes omissions, misconfigurations, programming errors, trips and spills, malfunctions, etc.

Environmental

Environmental not only includes natural events such as earthquakes and floods, but also hazards associated with the immediate environment or infrastructure in which assets are located. The latter encompasses power failures, electrical interference, pipe leaks, and atmospheric conditions.

A global view

As always, we strive to provide a global overview of what we are seeing in our incident data with the aim being to highlight trends that can also be applied to the global threat landscape. To facilitate this, a broad data set is collected from across all of the operational teams within Orange Cyberdefense including our 14 CyberSOCs responsible for supporting customers around the globe.

Following in the same vein as recent Security Navigator reports, we again have the luxury of utilizing a whole years' worth of Managed Threat Detection Services data, 1st October 2022 to 30th September 2023. This year's report however will be the first time we have had a full year's worth of data based on using the VERIS framework to better categorize our incidents.

Events, Incidents, Confirmed Incidents

A note on terminology: we log an event that has met certain conditions and is thus considered an Indicator of Compromise, Attack or Vulnerability. An Incident is when this logged Event, or several Events, are correlated or flagged for investigation by a human – our security analysts.

An Incident is considered 'Confirmed' when, with help of the customer or at the discretion of the analyst, we can determine that security was indeed compromised. We refer to these 'Confirmed' incidents in this report as 'True Positives'.

True Legitimate incidents are those that were raised but, after consultation with the customer, proved to be legitimate activity. Incidents are categorized as 'False Positive' when a false alarm was raised.

Because individual SOCs or clients may have slightly different approaches to defining Incident status, we simplify these categories to 'Confirmed' and 'Other' in parts of this report.

Totals

In total 129,395 incidents were recorded, all of which were investigated by human security analysts in one of our CyberSOCs. These investigations resulted in 25,076 'True Positive' confirmed security incidents being raised with our customers - 19% of all the incidents we investigated. The other incidents comprised of 10% 'True Legitimates' and 58% 'False Positives' with the remaining 13% having inconclusive status.

We are happy to say that our client base has grown from last year with data from 44.5% more clients being included in this report. This relatively large growth in dataset however actually resulted in only 25,076 confirmed incidents, a decrease of 14% in the confirmed incidents from last year's report.

This translated into an average number of 23.6 confirmed incidents per month/customer over the past 12 months. This is a significant decrease from the figure of 42.7 we recorded for the same period last year, primarily due to the configuration of clients in this dataset, and internal operational efficiencies.

Historically we have always seen Malware to be one of the two highest detected true positive incident types, this year though it has slipped to third with just 13%, dropping from 16.5% of VERIS classified incidents seen last year which saw it joint second with Misuse. The Misuse category was again second with 17.28%, almost exactly in line with last year's report.

It's important to remember though that Misuse does not necessarily equate to malicious activity with intent to cause harm or loss, it could equally be an unintentional breach of a policy. With this being the first time we present full year of VERIS data, we reserve speculation on shifts until we have another full year for comparison.

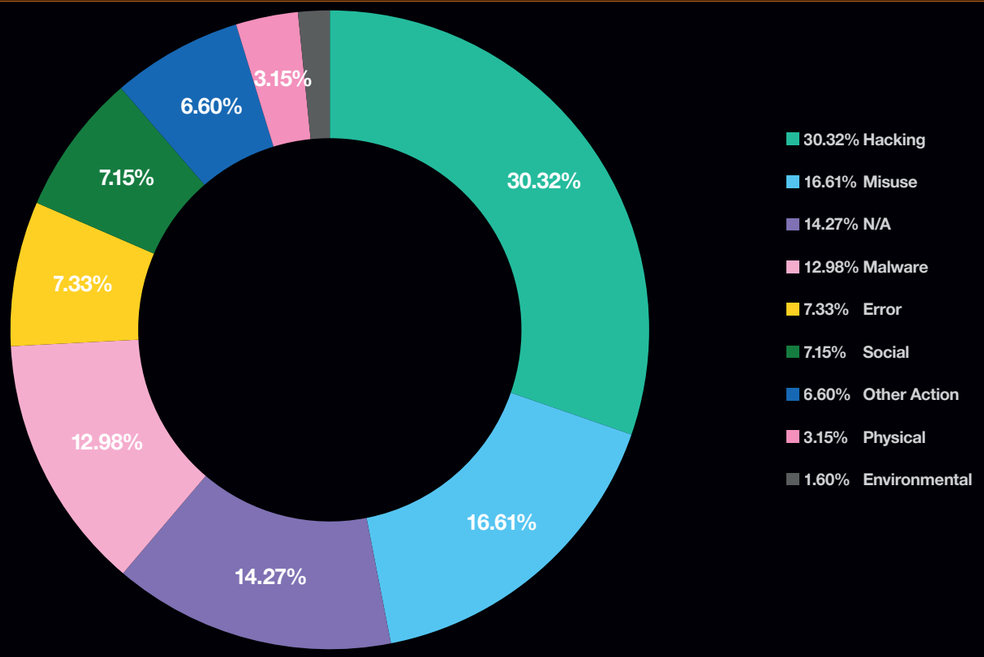
Just as we saw last year, Hacking remains in the top spot, however this year it accounts for almost a third of confirmed incidents with 30.32%, which is a relatively significant increase on the 25% previously seen. Incidents categorized as Error (7.33%) again take fourth place and Social (7.15%) completes the top 5.

Whilst 'Error' does not always imply a security incident it can easily be a precursor to one, especially with the rapid migration to cloud environments and the complexities involved with their configurations for example, whereby a simple misconfiguration could easily leave private data exposed.

The Social category covers any attempt to deceive, manipulate or otherwise abuse employees. The obvious tactic here is any form of phishing or Business Email Compromise (BEC). Social attacks of this kind are difficult to identify in detection data – where we observe the effect rather than the cause of an activity. This threat vector is therefore probably under-represented in this datasource.

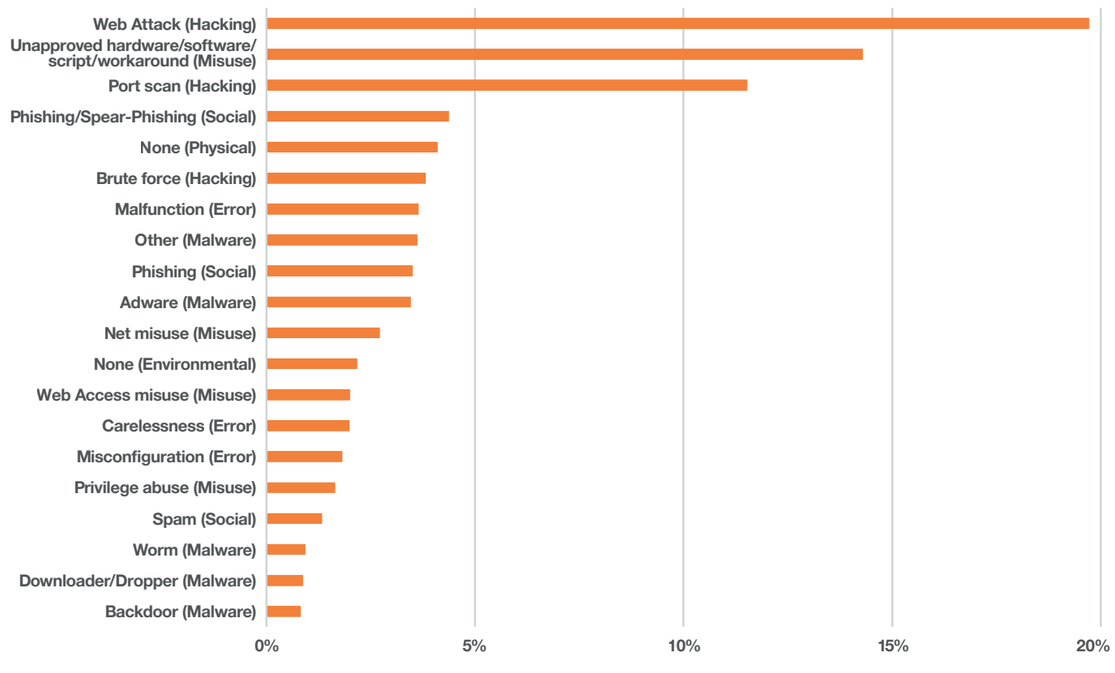
Incidents by Threat Action

Distribution of True Positive incidents by threat action



Threat Action in detail

Top 20 Threat Action and Threat Action Level 2 combined



If we add a second level of detail to the top level VERIS Threat category, we can see a more granular view of the underlying cause of the incidents our analysts have investigated. The top three combined incident types, Web Attack (Hacking), Unapproved hardware/software/script/workaround (Misuse) and Port Scan (Hacking), in the above chart make up over 45% of all categorized Incidents. All three of these combined incident types remain in the same places as in the previous Navigator report, however all three did increase their percentage share of incidents quite considerably.

Web Attacks are where an attacker will try and abuse a weakness or vulnerability in a website or web-based application. These will commonly include SQL injection and Cross-Site Scripting (XSS), as well as Cross-Site Request Forgery (CSRF) attacks.

The sub-action of "Unapproved hardware/software/script/ workaround", which is a form of Misuse, again features in the top 3 combined incident types we detected, with 14%. In our data we saw Misuse incidents which covered activities such as:

- Suspicious PowerShell/CMD command line detected
- Honeytoken activity
- Hacking tool detected
- Proxy Bypass: TOR, anonymization or other
- High volume of data transferred to removable storage
- Malware detected on USB devices
- Connection toward a known suspicious domain/IP address
- Network reconnaissance or host scan detected
- Potential phishing link clicked

It's worth remembering that this combination would also cover so-called shadow IT. This is where employees deploy or use hardware (or software) that has not been approved or provisioned by the organization. The motivation is usually to bypass certain restrictions, hence this is done without the involvement of the IT department who would ensure correct and secure configuration.

External Port Scans are a very common activity and are used by "legitimate" services such as Shodan or Censys for example.

However, they are also a common technique used by threat actors in the reconnaissance phase of an attack.

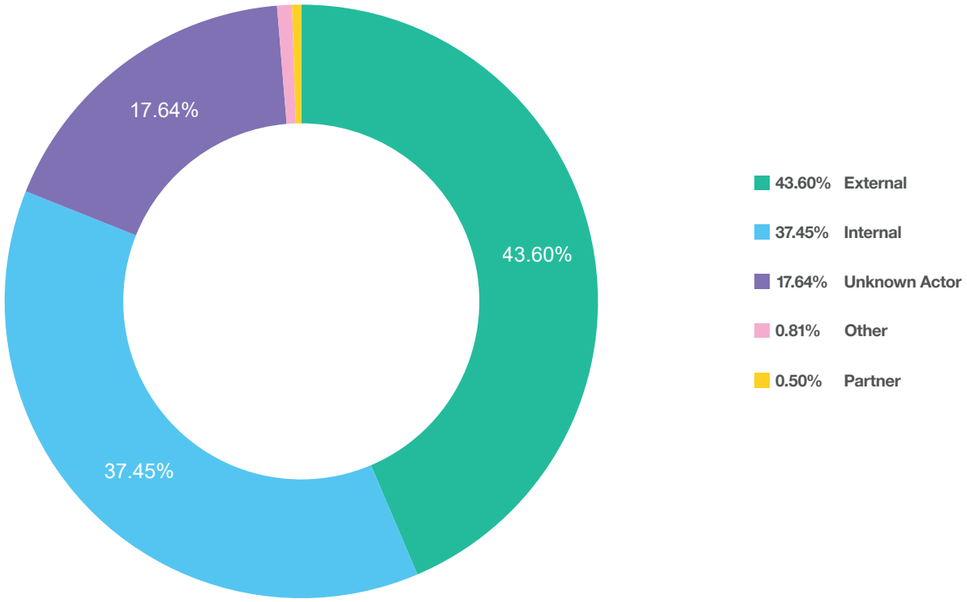
Incident sources and targets

As the flow chart at the start of this chapter illustrates, we see an almost equal proportion of incidents being attributed to Internal and External Actors. This is a notable shift away from last year, when Internal 'actors' featured more prominently. This is a trend worth noting.

End user devices are (predictably) the most common assets impacted. These endpoints remain the cold-face for most contemporary attacks. But Servers also feature prominently, and there is a general sense that attackers are reviving the 'lost' art of exploiting services over the internet.

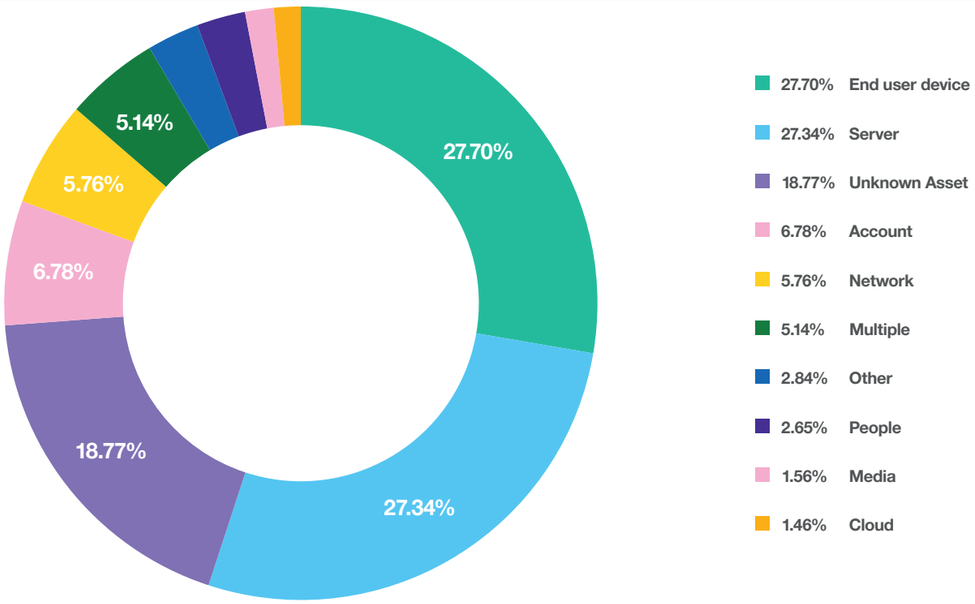
Incident sources

Distribution of incidents by Threat Actor



Incident targets

Distribution of incidents by impacted asset



Other & Unconfirmed Incidents

In addition to classifying Confirmed Incidents, our analysts also document Unconfirmed Incidents using the “4W” framework to the right.

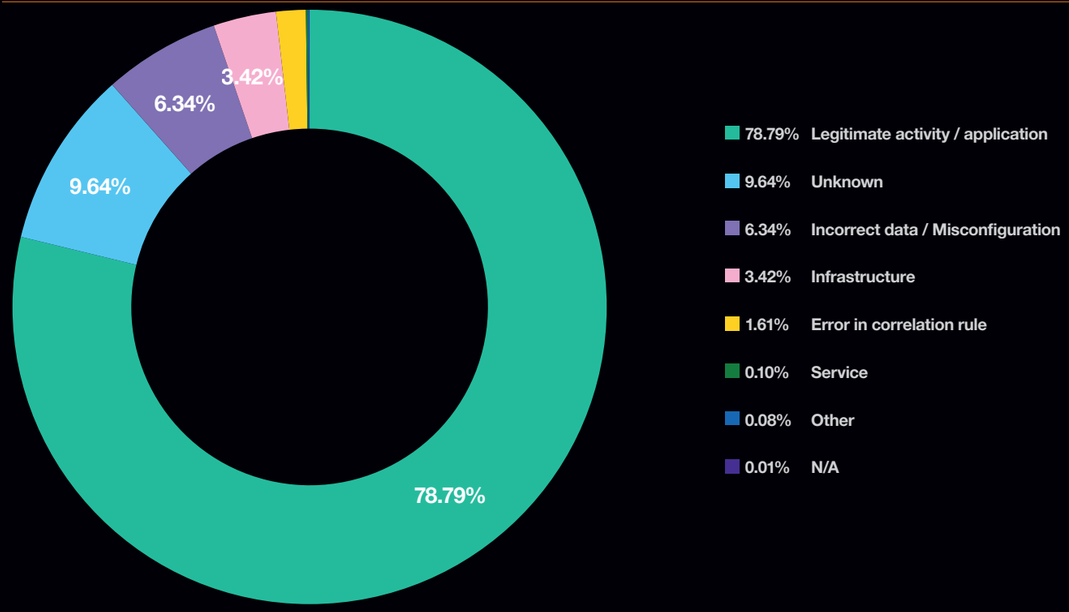
We investigate questions regarding the volume of False Positive alerts our CyberSOCs deal with later in the report in chapter "Fake News and False Positives"

4W

Why?	Why did we get an unexpected result?
Where?	Where is the root cause of the unexpected result located?
Who?	Who was the actor or entity that caused or contributed to this unexpected result?
What?	Which mission of the security incident management chain was impacted?
How?	How was the improvement handled?

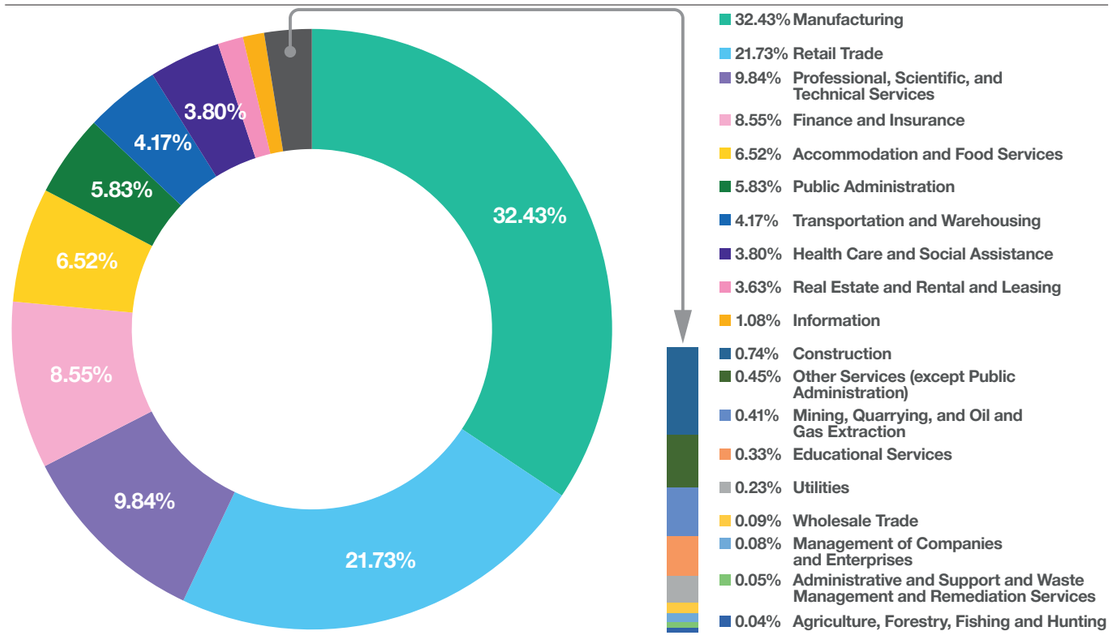
False Positive types

Distribution of incidents that raised an alert but turned out to be harmless



Incidents by industry

Breakdown of incidents analyzed by customer industry



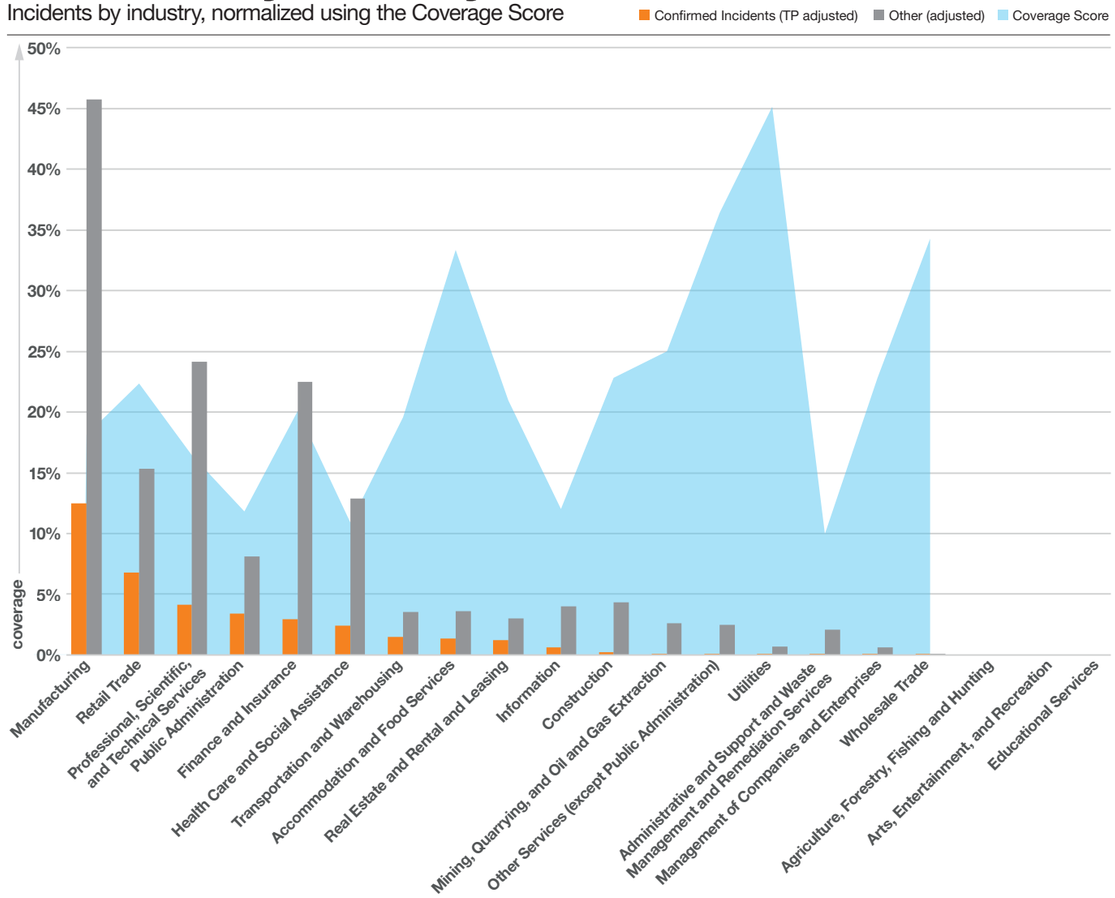
Incidents by Industry

Another key factor we take into consideration is which vertical our customers are operating in. As can be seen above, the Manufacturing sector is by far the largest contributor in terms of Confirmed Incidents our analysts handled, following the same trend as recent years. With Retail Trade & Professional, Scientific and Technological Services completing the top 3, we can easily see that just 3 Industries are responsible for almost two thirds of the Confirmed Incidents we responded to.

Where available, the Assessed Coverage Score can be used to review our comparison of Incident levels across Industries and Business Size.

Incidents by industry

Incidents by industry, normalized using the Coverage Score



We perform a simple modification on the Incident volumes to factor in the relative level of coverage: Divide the incident count by the assessed coverage score and multiply it by the maximum possible score. Put simply, the lower a client's assessed coverage score is, the more this adjustment will 'boost' the number of incidents in this comparison. For a client with the maximum possible level of coverage, we will simply reflect the actual number of incidents we observed.

Using this simple calculation, we can now consider how businesses and industries compare with their relative levels of coverage taken into account.

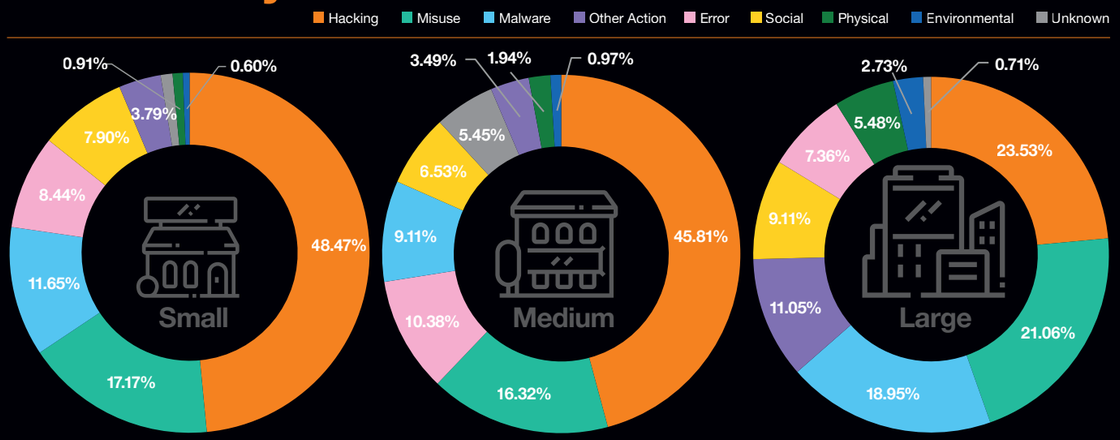
Incidents by business size

We correlate certain demographics of our customers with the incidents we investigate. One of the key demographics we take into account is the Business Size.

We map our detected incidents not only through classifications but also by connecting certain ‘demographics’ of the customer profile to them - one of these is organization size. Based on the OECD business size scale we differentiate between business sizes as in the table to the right.

Business Size	Employee Count
Small	1-49
Medium	50-249
Large	250-10,000+

Incidents by business size



For our clients who are categorized as Small, slightly under 50% of the Confirmed Incidents were as a result of Hacking activity.

Hacking is again the highest cause of Confirmed Incidents for our Medium sized customers, albeit with a slightly reduced proportion. When combined, the Misuse & Malware threat actions were responsible for just over 25% of incidents for this category of organization, which is still considerably lower than those categorized as Hacking.

With our large customers the pattern remains similar in terms of the threat actions making up the top 3. However there has been a fairly significant shift in the proportions. The threat actions of Misuse (21.06%) and Malware (18.95%) now make up over 40% of confirmed incidents between them, whereas Hacking has now dropped to 23.53%.

Vulnerability Scanning

To be effective at vulnerability management one must be able to address those items that may have the biggest impact on the business in a meaningful way. This requires timely threat intelligence that is accurate and concise, combined with efficient vulnerability scanning results in a capability that empowers teams responsible for managing exposure and associated risks.

The Orange Cyberdefense Vulnerability Operations Center (VOC) monitors our customers' exposure to current threats and how open their environment is to potential risks.

This year we revisit the menacing vulnerability theme with an eye on the ever present and lingering tail of unresolved system weaknesses. The waves of newly discovered serious issues joust for our attention with existing unresolved issues, seeming like a hydra that keeps on growing new snaking heads as soon as you dispatch others.

Assessing whether a system is adequately protected is a challenge that requires skill and expertise and can take a lot of time. But we want to learn of any weaknesses beforehand rather than having to deal with the fallout of an unplanned "free pentest" by a random Cy-X group.

The role of the Ethical Hacker is to conduct Penetration Tests – to emulate a malicious attacker and assess a system, application, device, or even people for vulnerabilities that could be used to gain access or deny access to IT resources.

Penetration Testing is generally considered a component of Vulnerability Management, but could also be seen as a form of Threat Intelligence that businesses should leverage as part of their proactive defense strategy.

A capable Ethical Hacker demonstrates value through clear communication with actionable feedback that empowers the client and instills trust.

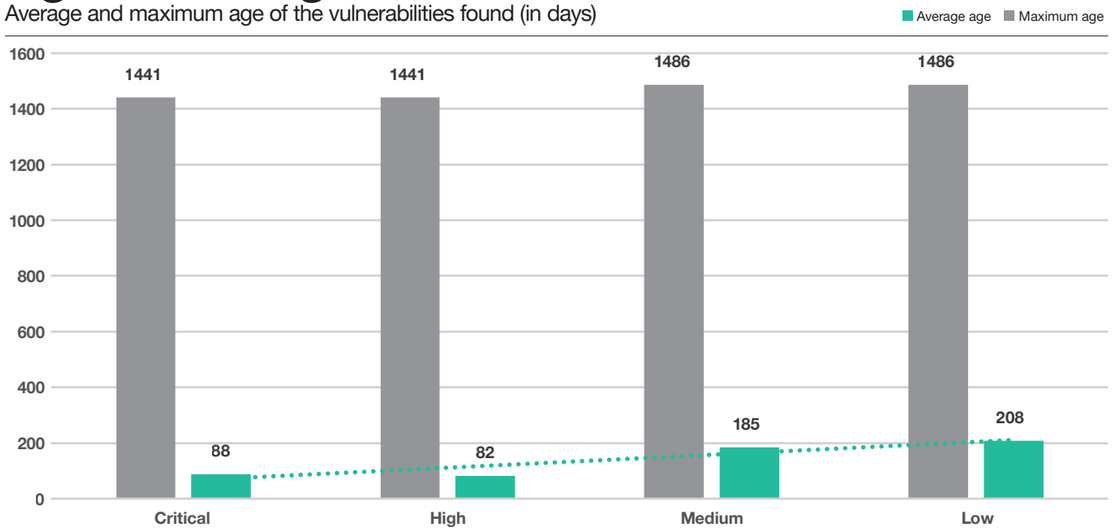
Vulnerability Scanning Findings by Severity

The chart on the bottom of the next page shows the long tail of unresolved real findings. Examining the severity rating share per unique Finding we see that the bulk of unique Findings, 79%, are classified as 'High' or 'Medium'. However, it is also worth noting that half, 50.4%, of unique Findings are considered 'Critical' or 'High'.

The average number of 'Critical' or 'High' Findings has decreased by 52.17% and 43.83% respectively compared to our previous published results. An improvement can also be observed for Findings with severity ratings 'Medium' and 'Low' being down 29.92% and 28.76%. As this report uses a slightly different sample of clients to last year, a YoY comparison has limited value, but we believe clients are responding to the findings we report.

Age of findings

Average and maximum age of the vulnerabilities found (in days)



The majority, 78%, of Findings rated 'Critical' or 'High' are 30 days or younger (when looking at a 120-day window). Conversely, 18% of all findings rated 'Critical' or 'High' are 150-days or older. From prioritization perspective 'Critical' or 'High' real findings seem to be dealt with swiftly, but some residual still accumulates over time.

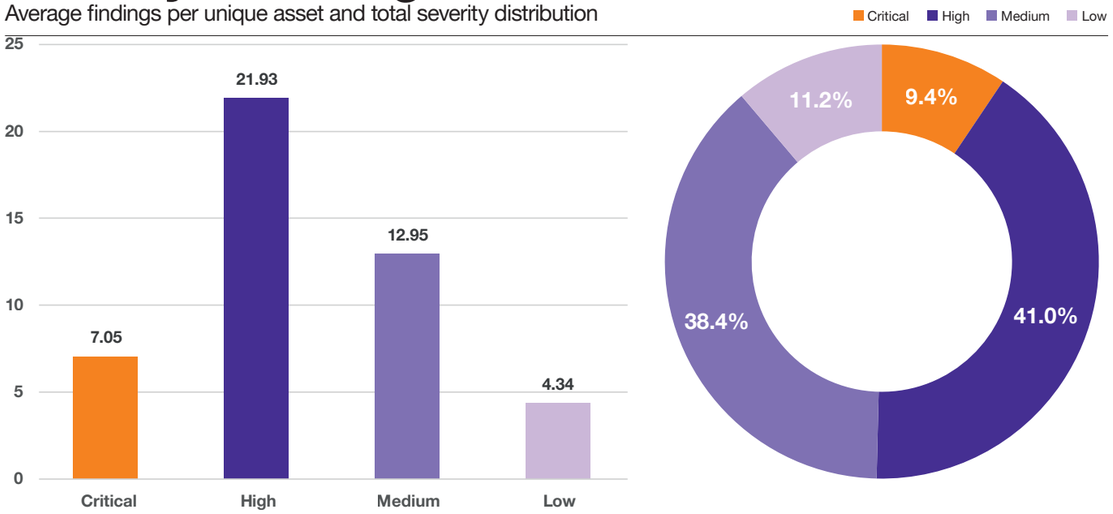
But should this be a concern when only 0.71% of critical findings are 660 days or older?

Overall, Critical findings constitute only 0.37% of all real findings.

We see therefore that unresolved Findings continue to grow older. Indeed, ~35% of all unique CVEs are from findings 120 days old, and older.

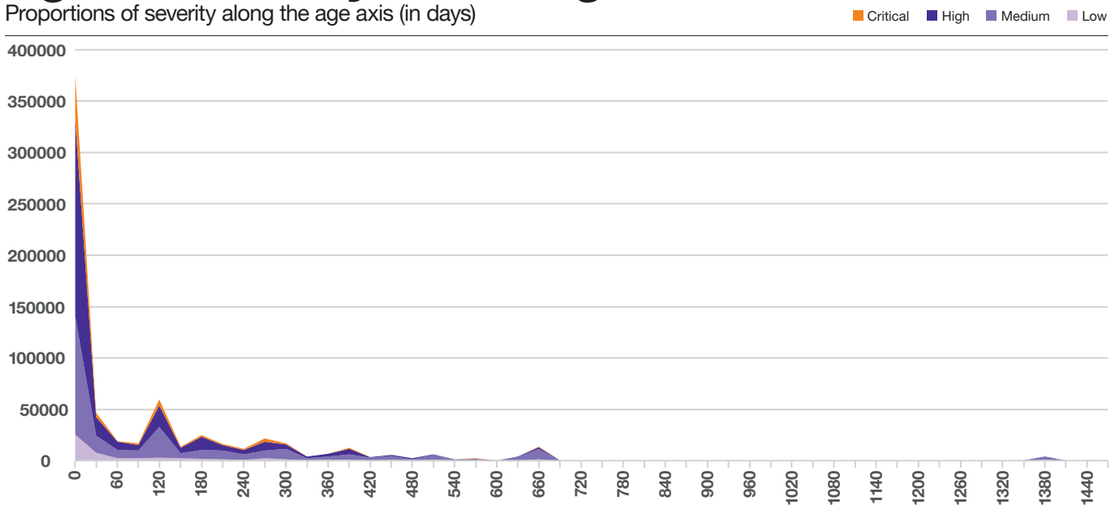
Severity of findings

Average findings per unique asset and total severity distribution



Age vs. Severity of findings

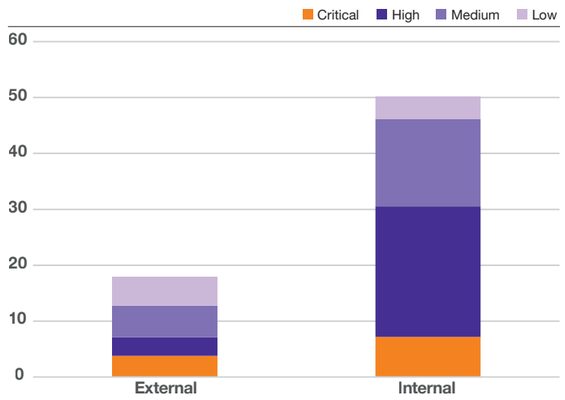
Proportions of severity along the age axis (in days)



Findings by Asset Exposure

We can also examine the average severity rating of Findings per unique Asset which are classified as External or Internal to an organization. Both Internal and External assets have a similar number of Medium findings at approximate 31%. Internal Assets have on average 23.38 Findings rated 'High', and 15.6 findings rated Medium. Although External assets only have 3.77 Unique Findings rated 'Critical', it is proportionally much higher than the 'High' severity for External Assets (18.7%). Internal assets have 7.18 average Findings for unique assets rated 'Critical', this is very close to the overall average.

Finding Severity by target exposure

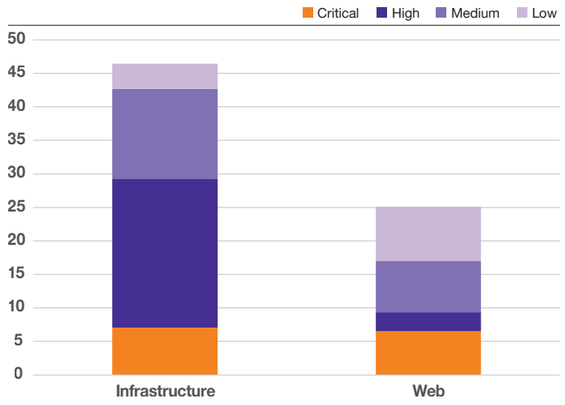


Findings by Asset Type

Another approach is to consider the scanning engine used to distinguish between assets classes. We can create two groups, namely ‘Web’ and ‘Infrastructure’. The group classified as Infrastructure yield average scores per severity rating nearly identical to the overall average. Assets classified as Web have proportionally, much lower severity rating of ‘High’ on average.

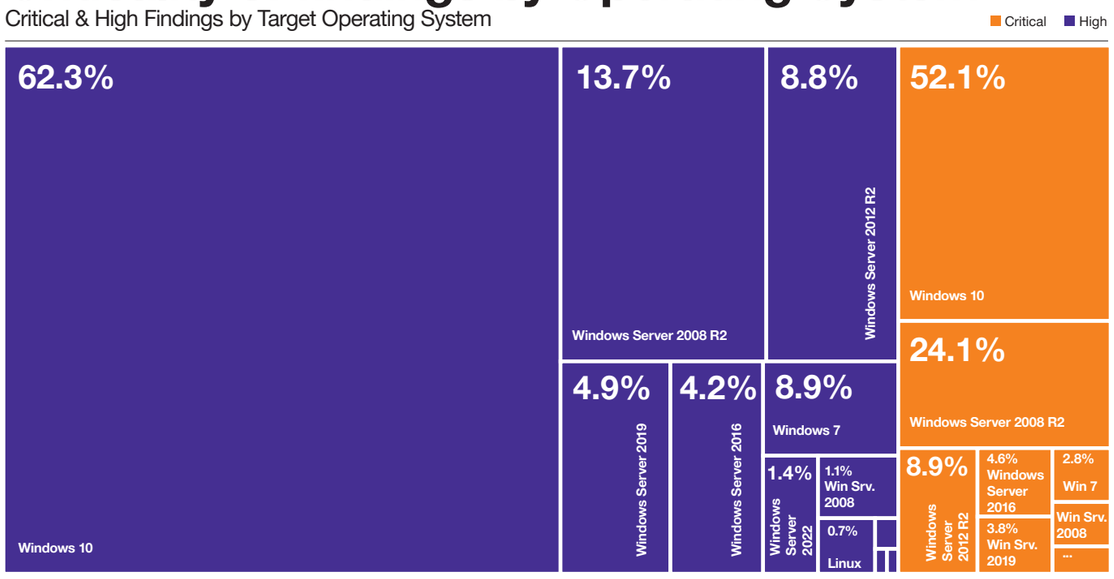
Assets classified as External and Web do seem to have fewer impactful Findings on average compared with assets falling in the Internal and Infrastructure groups, especially for Findings with a Severity rating of 'High'. This would suggest that External and Web assets are enjoying priority when getting Findings resolved.

Finding Severity by target type



Criticality of findings by Operating System

Critical & High Findings by Target Operating System



Industry perspective

The high average numbers of ‘Critical’ and ‘High’ findings are largely influenced by assets running Microsoft Windows or Microsoft Windows Server operating systems. Assets running operating systems other than Microsoft such as Linux based OS are present, but these are reported proportionally far less.

We should note, however, that the ‘Critical’ or ‘High’ findings associated with assets running Windows are not necessarily vulnerabilities in the operating system but can also be related to applications running on the asset.

It is perhaps understandable that unsupported Microsoft Windows and Windows Server versions are prominent here, but it is surprising to find more recent versions of these operating systems with severities rated as ‘Critical’ or ‘High’.

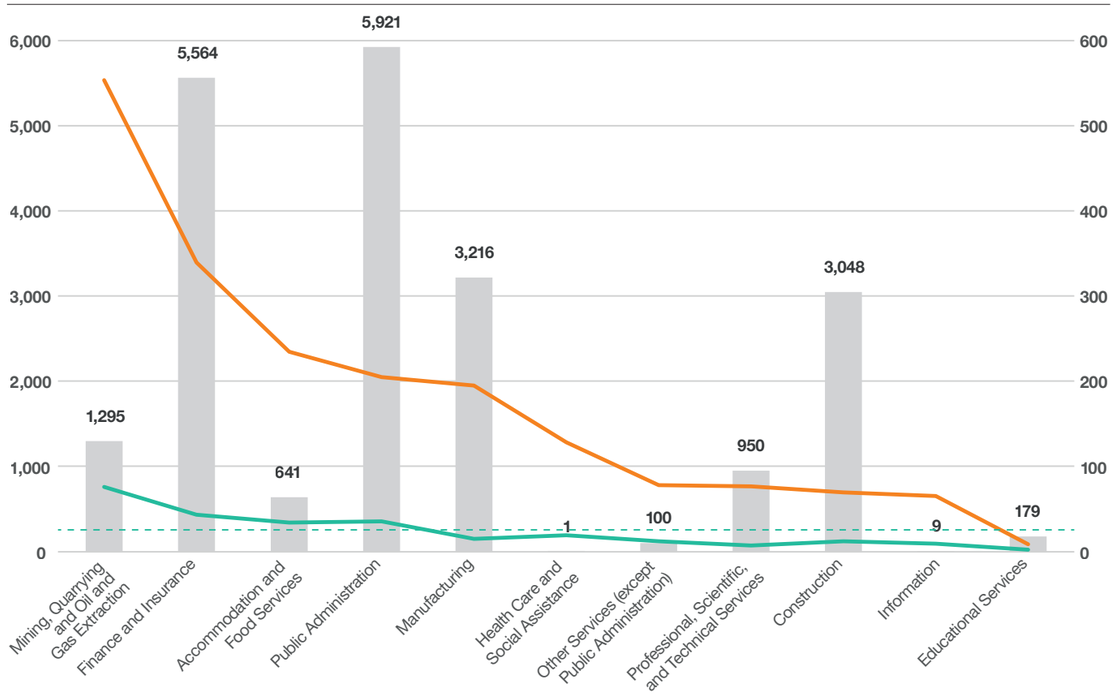
The results here only consider Findings based on scans of hosts rather than services such as web applications. The average unique real finding per unique asset is 31.74 for all organizations, denoted by the dashed horizontal line in the chart below.

Our clients in the Construction industry appear to be performing exceptionally well compared to clients in other industries, with an average of 12.12 Findings per Asset. At the opposite end of the spectrum, we have the Mining, Quarrying, and Oil and Gas industry, where we report an average of 76.25 unique findings per asset. Clients in Public Administration surprised us by outperforming Finance and Insurance with an average of 35.3 Findings per Asset, compared with 43.27, despite the larger number of Assets. Of course, these values derived from the set of clients present in our sample, and may not represent the universal reality.

By comparing the ratio of Total CVSS3 Base Score per Asset to the total number of Assets for a given Industry, we observe that our clients in the Construction Industry are performing the best. In second place is Public Administration, followed by Manufacturing that just pipped third place from Finance and Insurance. Mining and Quarrying and Oil and Gas along with Accommodation and Food Services have ratios of between 6 to 7 times higher than Manufacturing. Industries with Unique Assets below 500 may not yield meaningful results.

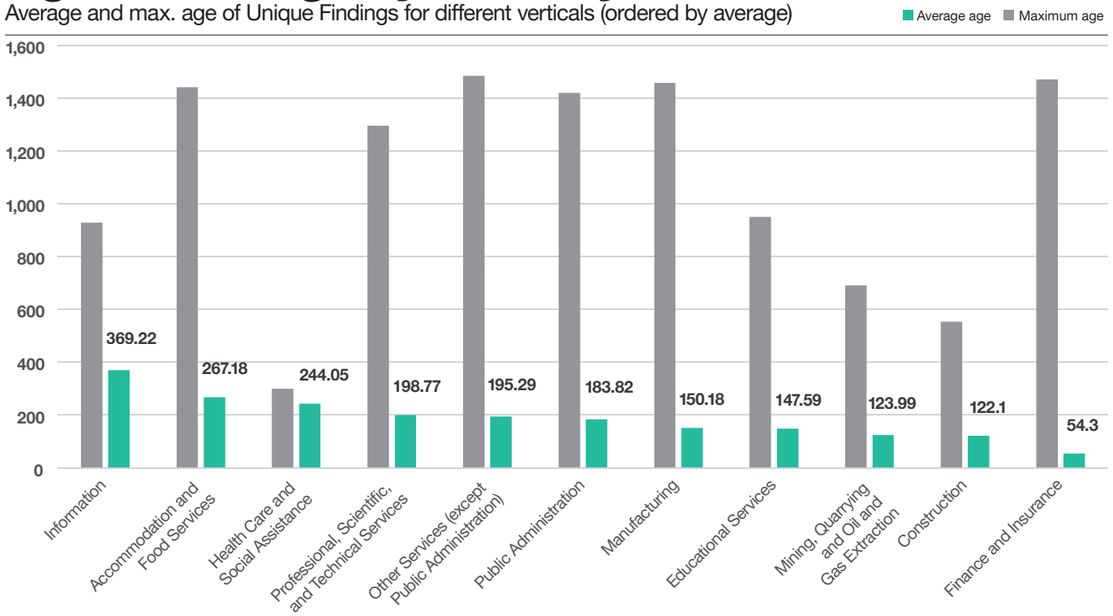
Findings per asset by industry

Average Unique Findings per Unique Asset by Industry



Age of findings by industry

Average and max. age of Unique Findings for different verticals (ordered by average)



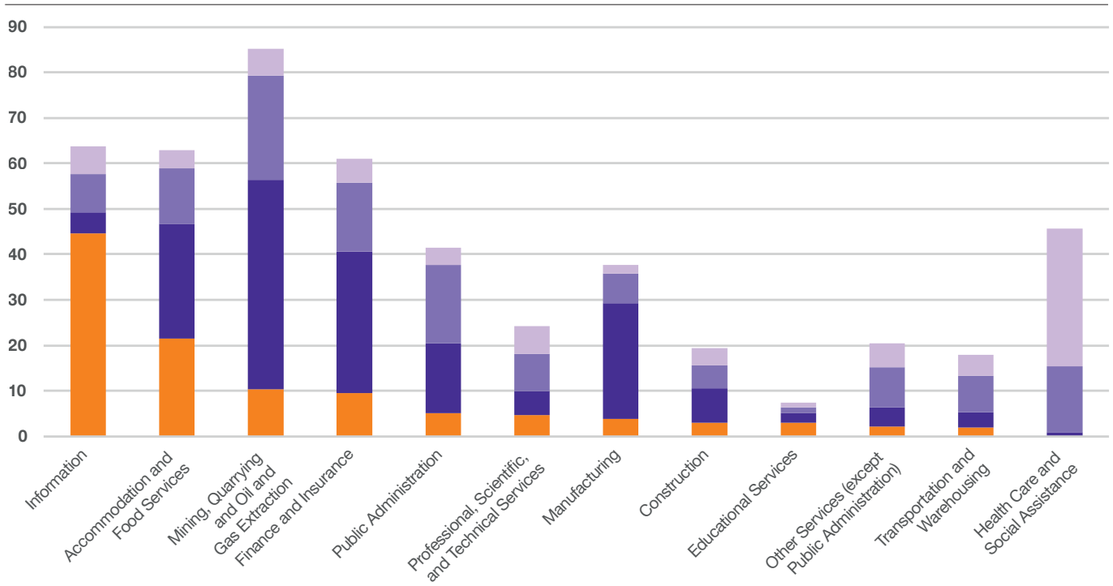
When comparing the average severity per unique asset per Industry we see a mixed picture. We can ignore Health Care and Social Assistance and Information, with a relatively small unique asset count, that results in averages that are disproportionate in relation to other Industries.

Our overall Industry average for Severity rating High is 21.93 and by that number Mining, Quarrying and Oil and Gas Extraction has more than double that average.

Similarly, Finance and Insurance with Accommodation and Food Services also overshot the overall average by 10.2 and 3.4 findings per unique asset respectively. The same three Industries exceeded the overall average for findings rated Critical, with Accommodation and Food Servers doing so by almost a factor of 3.

Criticality of findings by industry

Average Severity per Unique Asset per Industry (ordered by most critical)



Research Question:

Can we reproduce the findings of other researchers on the effectiveness of EPSS, but on the vulnerabilities reported to our own clients?

We are unable to reproduce the findings of other researchers using our own vulnerability and EPSS datasets, which shows how context-sensitive vulnerability intelligence is. However, EPSS has been shown to be a more effective alternative to CVSS when making remediation decisions, especially in terms of Coverage

EPSSolutely Vulnerable

An estimated 4.1 to 5.5% of all vulnerabilities in 2020 were found to be exploitable[41][42]. Given that fewer than 10% of reported vulnerabilities are likely to ever be exploited by an attacker in the wild, and given that most enterprises are never able to patch more than ~15%[43] of the vulnerabilities on their networks, determining what vulnerabilities to prioritize becomes an essential facet of Vulnerability Management.

The Exploit Prediction Scoring System (EPSS)[44] was presented by the FIRST organization at the BlackHat conference in 2019[45], and seeks to provide clear, accurate predictions on whether vulnerabilities are likely to be exploited. EPSS promises to become an invaluable source of intelligence that can inform defenders' decisions, by illuminating vulnerabilities that are more likely to be exploited within 30 days of a given date[46].

EPSS scores are calculated by a complex algorithm using real-time intelligence from multiple sources to help defenders strike the optimal balance between coverage and efficiency. A judicious application of the EPSS predictions should result in no exploitable vulnerabilities getting missed, while avoiding the 'wasted effort' of patching or mitigating issues that aren't ever exploited.

Predicting Hacking

EPSS provides a metric that can be used to inform prioritization strategies. Each of the 212,443 available CVE is assigned an EPSS score from between 0 and 1 daily, based on fresh data and intelligence. For example, only 6,838 CVS have an EPSS score greater than or equal to 0.4, which is approximately 3.2% of all CVE. Choosing an EPSS score threshold can determine which CVEs are mitigated or left, depending on the use case.

Ethical Hacking, as a form of vulnerability identification and prioritization, can also be thought of as a source of highly contextual vulnerability intelligence. So how do these two sources of intelligence compare?

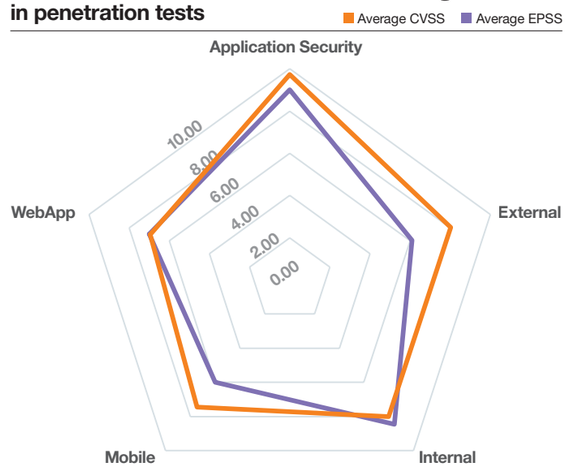
The chart to the right shows a mix of project types with 29 CVEs reported that have an EPSS score of 0.4 or higher, grouped by project type. The CVSS scores vary from as low as 3 to a max of 10.

Perhaps most importantly, a total of 177 (85.92%) CVEs were reported by our testers but have an EPSS score of less than 0.4, and so are not present in this chart.

Included in this group are 34 CVEs that have an CVSS score of 8, and some with scores as high as 9.8. In other words, a skilled attacker matching our Penetration Testing team's skill would have found 177 potentially serious vulnerabilities that would probably not have been prioritized using EPSS.

CVSS vs EPSS of CVE Findings

in penetration tests



This serves as a reminder that EPSS is a general model with certain limitations in terms of context. Penetration Tests, on the other hand, can look deeper into an environment to produce findings that may not be considered in the algorithm that produces EPSS scores.

Leveraging additional capabilities such EPSS can assist vulnerability management teams to focus on what is likely to be exploited. An effective vulnerability management process should also use the intelligence produced by Penetration Testing to augment other vulnerability management data.

Science comes to Vulnerability Management

In a seminal paper titled 'Enhancing Vulnerability Prioritization: Data-Driven Exploit Predictions with Community-Driven Insights'[47], Jacobs et al. consider how EPSS can be used to derive and evaluate patching strategies by using Effort, Coverage, and Efficiency as metrics[48].

How much time (Effort) must be invested to get all relevant vulnerabilities patched (Coverage) while ensuring that we do not waste resources on patching less impactful vulnerabilities (Efficiency)?

The paper by Jacobs et al. is a rare example of the application of real science and data to a problem in our industry. The depth and breadth of the work exceeds anything we could hope to present here, but it outlines some concepts and conclusions that are incredibly far-reaching and offer a base from which we can endeavor to build further.

In a section titled 'Simple Remediation Strategies' the paper's authors endeavor to 'compare the amount of effort required (as measured by the number of vulnerabilities needing to be remediated) for differing remediation strategies… [and highlight] the performance of 6 simple (but practical) vulnerability prioritization strategies based on [their] test data'.

They posit that patching only vulnerabilities with an EPSS score of 0.022 (2.2% probability) or above, would require only 15.3% of all vulnerabilities to be patched (aligning with the pragmatic real-world observation mentioned above) and result in 90.4% of exploitable vulnerabilities being mitigated, at an efficiency level of 24.1%.

This intelligent and encouraging finding required the researchers to define some concepts and parameters:

- First, they needed a 'population' of existing vulnerabilities that represents the combination of everything that could and should be patched. Jacobs et al. used the entire CVE set at the time of writing as their population.
- Next, they need a 'target' exploit group, which reflects all the vulnerabilities that are known to be exploited in the wild. There is no single definitive list like this at any given time, however, and the Jacobs team don't disclose what list they use in their evaluation.
- Finally, they define the concepts 'Coverage', 'Efficiency' and 'Effort' as the metrics that need to be balanced to evaluate the quality of a given patching strategy.

Standing on the shoulders of giants

In an effort to apply the concepts presented by Jacobs et al. in the context of our own clients, and with our own intelligence about what's being exploited, we derive the following definitions:

Vulnerability population (n = 24,177) is the collection of all vulnerabilities that require consideration. Jacobs et al. used the entire CVE dataset. For our purposes we use all the CVEs present in the dataset of unpatched client vulnerability findings we reported on in this Security Navigator.

Target exploit group is the collection of vulnerabilities that is believed to be exploited and must therefore be patched. This is a subset of the total vulnerability population. We derive this subset by matching our client's vulnerabilities with either:

- our own internal 'VulnWatch' Exploit Database (EDB) (n = 439)
- A list of CVE reported by our Ethihical Hackers on clients' estates (n = 482), or
- The CISA Known Exploited Vulnerabilities list (KEV) (n = 465).

Remediation group is the collection of vulnerabilities that must be patched according to the selected strategy. This is a subset of the vulnerability population and can overlap with the target exploit group.

EPSS score is the temporal score calculated by the EPSSv3 Machine Learning model that predicts the likelihood of the vulnerability being exploited within the next 30 days.

Strategy is how we select the vulnerabilities to be included in the remediation group. In our case this will be done by using the Common Vulnerability Scoring System (CVSS) version 3 score or the EPSS score.

Coverage is the percentage of remediated vulnerabilities that were that is also present in the target exploit group. For example, if 15 vulnerabilities are present in the target exploit group and the strategy led to 5 being remediated, then Coverage is 33.3%.

Efficiency is the number of remediated vulnerabilities from the target exploit group as a proportion of the total remediation group. If we patch 100 vulnerabilities in total but only 5 are considered exploitable, then our efficiency is 5%.

Effort is expressed as the number of vulnerabilities in the remediation group that will be patched as a percentage of the vulnerability population. If the total number of vulnerabilities in consideration is the entire CVE pool of 212,443 and our strategy requires us to patch 21,245 vulnerabilities, then the Effort is 10%.

The EPSS paper provides quantitative examples of evaluating Efficiency, Coverage, and Effort for a strategy based on either CVSS or EPSS scores. In their experiment they use the entire CVE pool as their vulnerability population. The target exploit group in their paper is a set of vulnerabilities they collected from various sources.

We emulate this experiment with our own vulnerability datasets. Our vulnerability population is comprised of CVE identified on client networks by our VOC scanning service. We chose three separate target exploit groups: two are based on proprietary vulnerability intelligence sources, namely our own 'Vulnerability Watch' Exploit Database (EDB) and a Pentest EDB that is a collection of CVE identified by our ethical hacking teams on client assignments. The third target exploit group is the CISA Known Exploited Vulnerability list (KEV), which we label the KEV EDB.

All three target exploit groups are trimmed down to intersect with our vulnerability population, as some of the 'exploited' vulnerabilities do not occur in our client environments and would thus be of no interest to us.

The chart below illustrates the outcomes of our efforts to replicate the Jacobs et al. analysis, using the more 'local' perspective provided by our own data. Their data and paper serve as the benchmark against which our replicated tests can be compared. These are labelled 'First CVSS' and 'First EPSS' respectively.

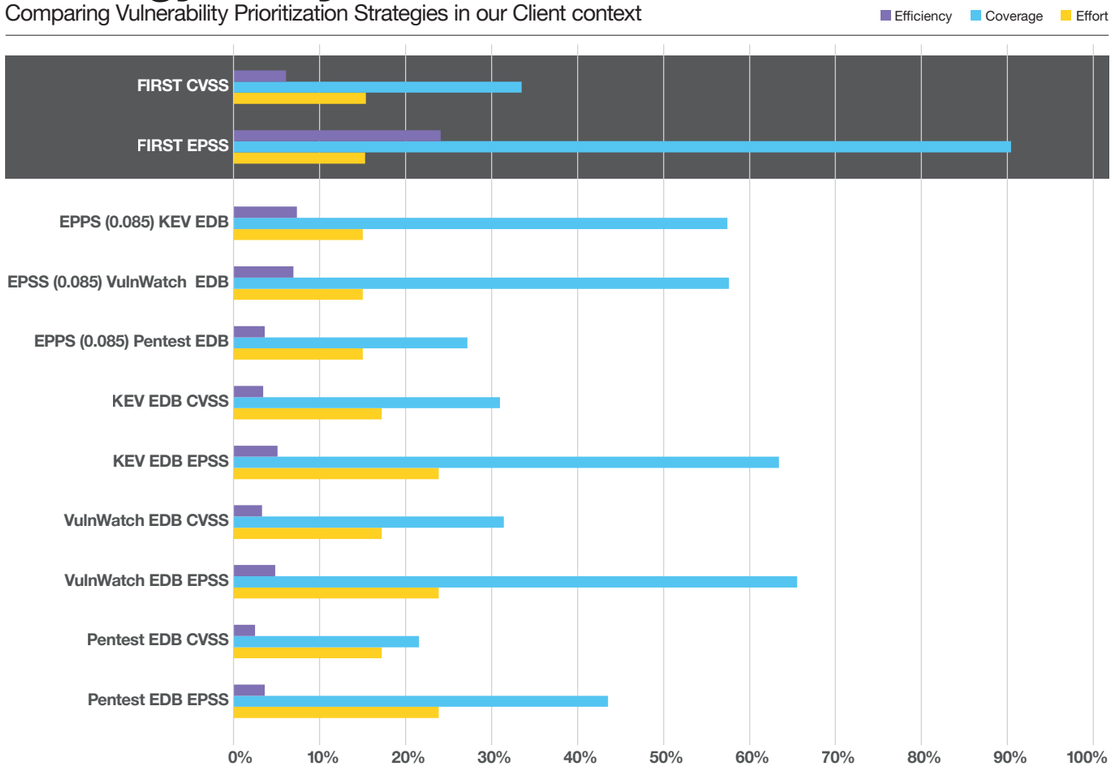
The First CVSS and the First EPSS Analysis assess the Effort, Coverage, and Effort for strategies involving vulnerabilities with a CVSS score of 9.1 or higher (First CVSS), and an EPSS score of 0.022 or higher (First EPSS).

These two thresholds were selected by aiming for an Effort of approximately 15%, which other research shows is a pragmatic level for most organizations.

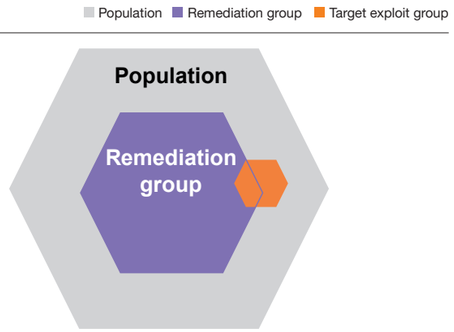
Notice that for the same level of Effort, the First EPSS strategy achieves Coverage of 90% and Efficiency of 24.1%, far better than the CVSS strategy, which only achieves 33.5% and 6.1% respectively.

Strategy Analysis

Comparing Vulnerability Prioritization Strategies in our Client context



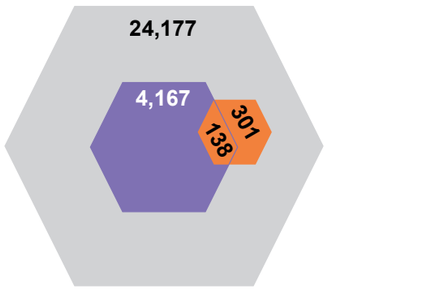
FIRST example strategies



Strategy: **CVSS v3.x**
Threshold: 9.1+ CVSS score
Effort: 15.1% of CVEs
Coverage: 33.5%
Efficiency: 6.1%

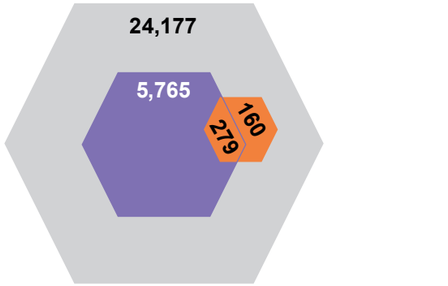
Strategy: **EPSS v3**
Threshold: 0.022+ EPSS score
Effort: 15.3% of CVEs
Coverage: 90.4%
Efficiency: 24.1%

Strategy: Patch all CVSS >= 9.1



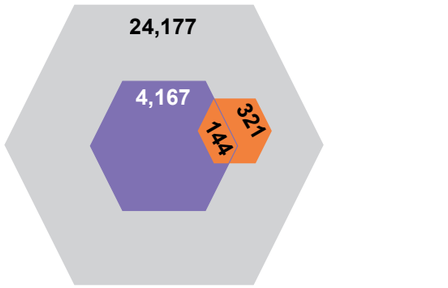
Population: All CVE in VOC results (24,177)
Known Exploited: All CVE from VulnWatch EDB Finding
Threshold: 9.1+ CVSS score
Effort: 17.24% of reported CVEs
Coverage: 31.44% of ‘exploited’ CVEs
Efficiency: 3.31% of vulnerabilities patched were exploitable

Patch all EPSS >= 0.022



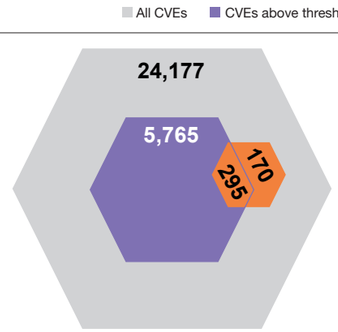
Population: All CVE in VOC results (24,177)
Known Exploited: All CVE from VulnWatch EDB Finding
Threshold: 0.022+ EPSSv3 score
Effort: 23.84% of reported CVEs
Coverage: 63.55% of ‘exploited’ CVEs
Efficiency: 4,83% of vulnerabilities patched were exploitable

Patch all CVSS >= 9.1



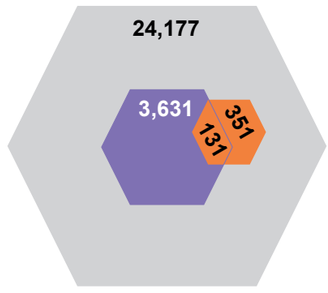
Population: All CVE in VOC results (24,177)
Known Exploited: All CVE from KEV EDB
Threshold: 9.1+ CVSS score
Effort: 17.24% of reported CVEs
Coverage: 30.97% of ‘exploited’ CVEs
Efficiency: 3.46% of vulnerabilities patched were exploitable

Patch all EPSS >= 0.022



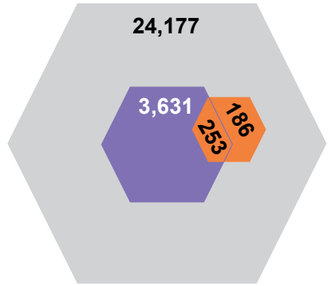
Population: All CVE in VOC results (24,177)
Known Exploited: All CVE from KEV EDB
Threshold: 0.022+ EPSSv3 score
Effort: 23.84% of reported CVEs
Coverage: 63.44% of ‘exploited’ CVEs
Efficiency: 5.11% of vulnerabilities patched were exploitable

Effort 15% with EPSS >= 0.085



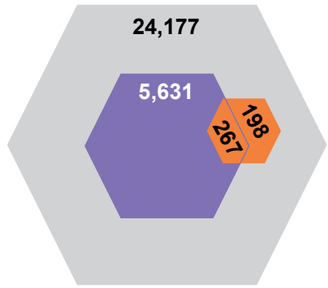
Population: All CVE in VOC results (24,177)
Known Exploited: All CVE from Pentest EDB
Threshold: 0.085+ EPSSv3 score
Effort: 15.02% of reported CVEs
Coverage: 27.18% of ‘exploited’ CVEs
Efficiency: 3.61% of vulnerabilities patched were exploitable

Effort 15% with EPSS >= 0.085



Population: All CVE in VOC results (24,177)
Known Exploited: All CVE from VulnWatch EDB
Threshold: 0.085+ EPSSv3 score
Effort: 15.02% of reported CVEs
Coverage: 57.63% of ‘exploited’ CVEs
Efficiency: 6.97% of vulnerabilities patched were exploitable

Effort 15% with EPSS >= 0.085



Population: All CVE in VOC results (24,177)
Known Exploited: All CVE from KEV EDB
Threshold: 0.085+ EPSSv3 score
Effort: 15.02% of reported CVEs
Coverage: 57.42% of ‘exploited’ CVEs
Efficiency: 7.35% of vulnerabilities patched were exploitable

1. Most notable in these experiments is that we do not report Coverage above 57.63% for any strategy, or Efficiency of above 5.1%, against any of our EDB.
2. Back-to-back for any dataset, EPSS out-performs CVSS in terms of Coverage, but of course Effort and Efficiency then tend to vary accordingly.
3. The FIRST EPSS Strategy of patching EPSS >= 0.022 requires an Effort of > 23% on our client vulnerability population, which is far higher than the 15.2% established by Jacobs et al.
4. Using the KEV EDB and the VulnWatch EDB tend to yield similar results for both strategies.
5. A CVSS strategy fairs particularly poorly against the Pentest EDB, achieving 50% lower Coverage compared to the EPSS strategy while requiring 7 percentage points more Effort.
6. In repeating the experiments from the Jacobs paper, we overshot the target Effort level of 15%. Our EPSS strategy generally required more Effort than the CVSS strategy, but of course with correspondingly better results.
7. To align with the Effort level in line with the 15% target Jacobs et al. set, we derive an EPSS strategy with a score of 0.085 as a threshold. Once again, the KEV EDB and VulnWatch EDB Coverage were remarkably similar, but none of the scenarios achieved more than 57.63% coverage or 7.35% Efficiency.
8. Another point to note is that these two EDBs do not intersect fully and represent different vulnerabilities. Aiming for a 15% Efficiency when dealing with the Pentest EDB yielded a much lower Coverage and Efficiency score.

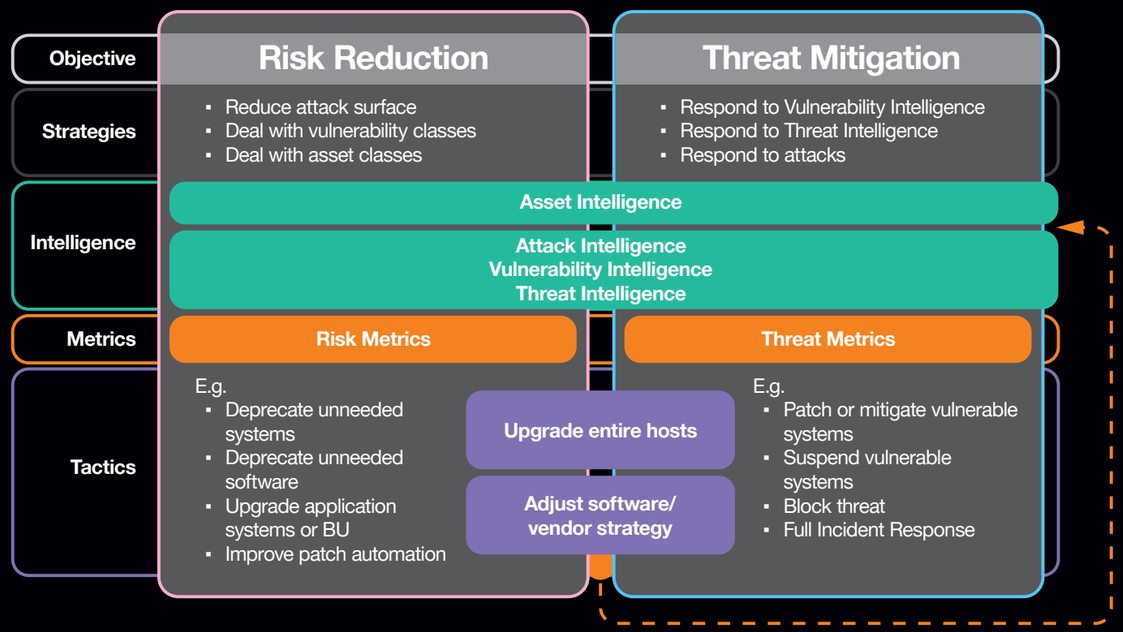
Summary

The difference in the size and nature of datasets represent different perspectives of what the 'threat' (the list of exploitable vulnerabilities) is. This needs to be decided, then weighed up against the 'challenge' (the total population of vulnerabilities), and the available budget and skill, before a strategy can be selected.

EPSS provides an invaluable input into this decision-making process, but its usefulness at any given threshold can only be determined once the respective factors are selected.

EPSS has been shown to be a more Effective alternative to CVSS when making remediation decisions, especially in terms of Coverage. But our Pentest EDB dataset still poses a challenge for both the CVSS and EPSS strategies.

Ethical Hacking can be thought of as a source of vulnerability intelligence that is unique in that it can provide much better context to a specific environment.



VOC Scanning Research Notes

About the data

- 2,555,515 unique findings
- 0.02% of unique findings classified as False Positives
- 23,690 unique assets
- Average number of unique findings per unique asset is 31.74 for all organizations
- Oldest findings are 1,486 days
- Average finding age is 125.81 days
- 0.37% of all unique findings are rated 'Critical'

The dataset is representative of a subset of clients that subscribe to our vulnerability scanning services. Assets scanned include those reachable across the Internet, as well as those present on internal networks. The data include findings for network equipment, desktops, web servers, database servers, and even the odd document printer or scanning device.

The number of organizations in this dataset is smaller (3 less) than the previous dataset used in Security Navigator 2023 and some organizations were replaced by new additions. With the change of organizations comes a different mix of assets which leaves comparing the previous results in the Security Navigator 2023 akin to comparing apples to oranges (we might be biased), but it still worth noting similar patterns where possible.

The term unique finding is used to describe an identifier that is specific to an asset linked to a to an organization. A unique finding is a composition of the following attributes:

- Client Identifier
- Asset Name
- IP Address
- Host Type
- Finding Name

This dataset contains 2,555,515 unique findings, which is a 22.9% increase in size compared with the number of unique findings in the previous Security Navigator, even though we have fewer client organization present this year. It is important to note that the total unique findings mentioned here includes False Positives. This year we reported a drop in the number of False Positives to approximately 0.02% of unique findings, compared with 1% unique findings in Security Navigator 2023.

Terminology

Findings are assigned a severity rating that can be either 'Informational', 'Low', 'Medium', 'High', or 'Critical'. The 'Informational' severity rating can be relevant in some cases, but this is excluded from our analysis due to its volume in relation to other severity rating types.

Real findings are those findings that exclude duplicates and false positives, while having a severity rating of either 'Critical', 'High', 'Medium' or 'Low.

Clients and Assets sampled

Industry	%
Finance and Insurance	31.20%
Public Administration	25.18%
Manufacturing	13.71%
Construction	12.87%
Professional, Scientific, and Technical Services	5.63%
Mining, Quarrying and Oil and Gas Extraction	5.47%
Accommodation and Food Services	2.71%
Other Services (except Public Administration)	1.78%
Educational Services	0.76%
Transportation and Warehousing	0.57%
Information	0.11%
Health Care and Social Assistance	0.02%

Business size	%
1-100	15.91%
101-500	9.31%
501-1000	5.15%
1001-5000	9.75%
5001-10000	16.14%
10001-50000	39.45%
100001-200000	4.30%

Penetration Testing

A Penetration Test is a contracted exercise in which a team of skilled and highly-trained 'Ethical Hackers' is tasked with emulating the activities of a real attacker in order to assess the security of a system, identify vulnerabilities, and derive opportunities to improve its security posture.

Like Vulnerability Scanning, this exercise involves finding and reporting Vulnerabilities in the target systems, and has a similar goal. But the process is very different. The tester will also seek to identify known vulnerabilities (often those with CVE numbers assigned to them) but will then also attempt to leverage those vulnerabilities to gain access to a target system, identify valuable resources that could be compromised or pivot from there to attack other systems in range.

Penetration Testing is usually very targeted, performed within a set of constraints agreed with the client that will include the targets in scope, the time available, the location and privileges of the attacker, and sometimes specific goals or 'objectives' the tester should seek to achieve. Each test is performed by one or more specific Ethical Hackers who then also writes up a report by hand explaining what was done, what was achieved, what that implies and what could be done to improve security posture.

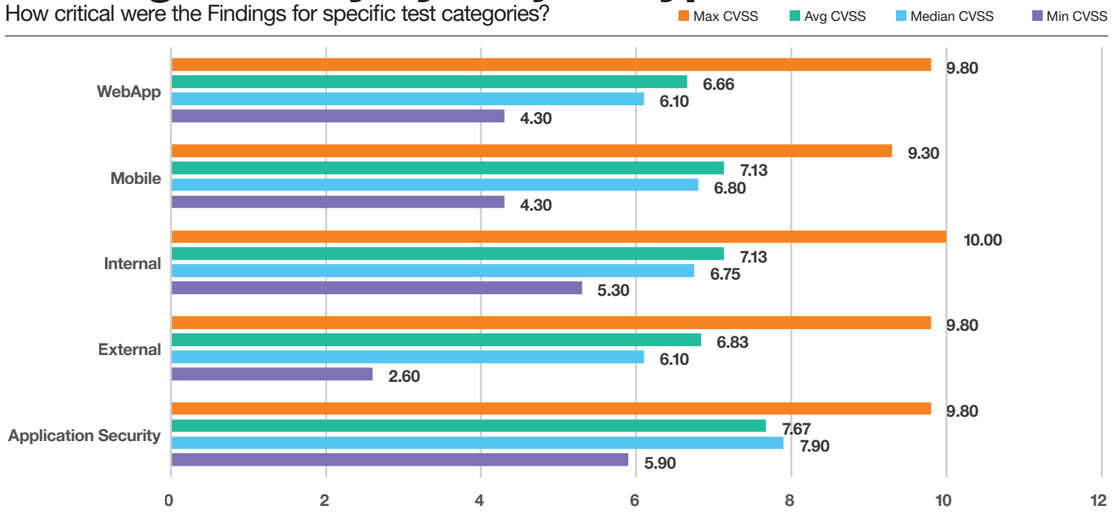
The 'findings' of a Penetration Test report are therefore only a small element of the overall output, but they contain elements similar to the findings of a vulnerability scan and can be analyzed in a similar way, and even compared to some extent.

As reports are a boutique product – hand-written by the tester and customized to meet the client's specific requirement - they do not lend themselves readily to quantitative analysis.

This year's Penetration Testing dataset was expanded from last year to include reports from two teams, one being a new addition. We reviewed 296 anonymized Penetration Testing reports for the period October 2022 through September 2023. Assessments are typically focused on specific customer requirements and scopes within the bounds of certain project types such as Internal, External, Web Application, Mobile Application Security, Red Teaming, API assessment, Configuration Review, and more. These can vary in complexity and time allocation and may require multiple Ethical Hackers to perform. For the most part the Client determines the scope and extent of testing required.

Finding Severity by Project Type

How critical were the Findings for specific test categories?



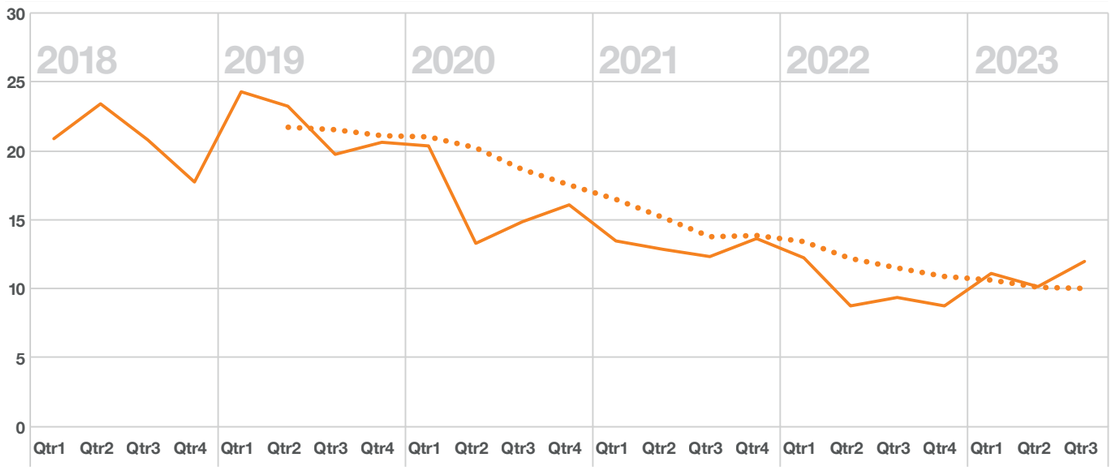
In last year's Navigator we reported that our Penetration Testing teams had to work 10% harder in the year 2022 than in 2018, requiring 8 hours and 47 minutes to achieve a comparable outcome. Here we see the same pattern emerging. The testing teams had to work 13% harder in 2023 than in 2018 to match the same total CVSS score per project day – needing to work 9h 3m per project day. Our testers would have to work 9h 3m to achieve the same results they would have managed in 8 hours at the start of 2018, which is 16 minutes more than for 2022.

The average number of project days required to report a Serious (Critical or High) finding has increased by 2.5% to 7.9, up from 7.7 previously reported in 2022. Comparatively the average length of a project in which we report a serious finding, is 10.5 days.

We've thus speculated previously that Penetration Tests have been revealing fewer serious security flaws over time, requiring our Penetration Testing teams to work harder to uncover weaknesses that may impact a business. The good news for our clients is that this still holds true for our 2023 data, and no significant regression has been observed. However, issues are still regularly discovered that could negatively impact a business if left unattended.

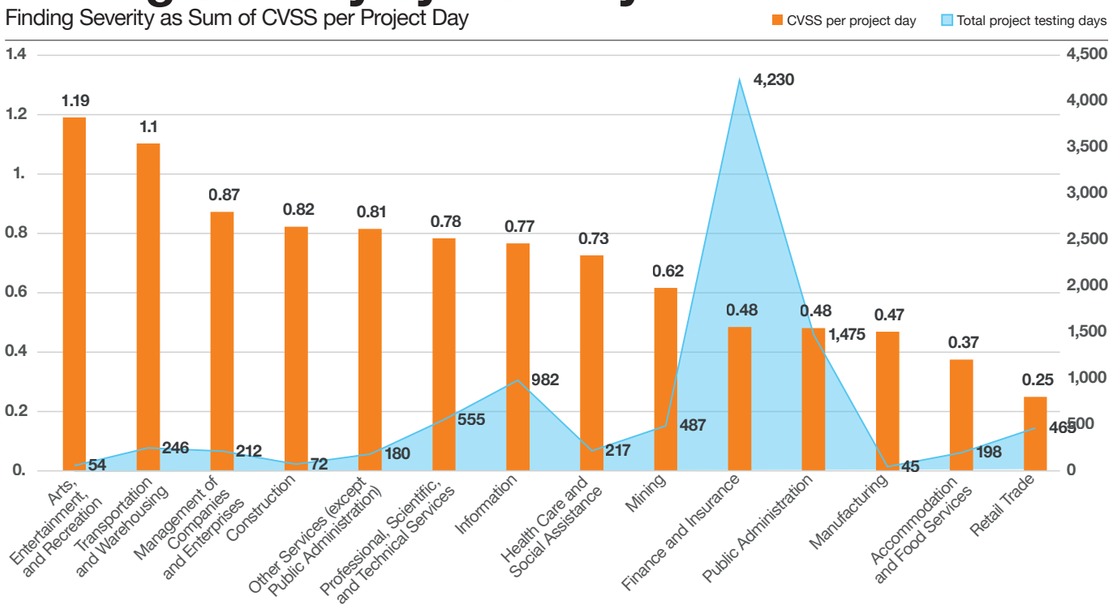
Finding Severity over time

Finding Severity as Sum of CVSS per Project Day



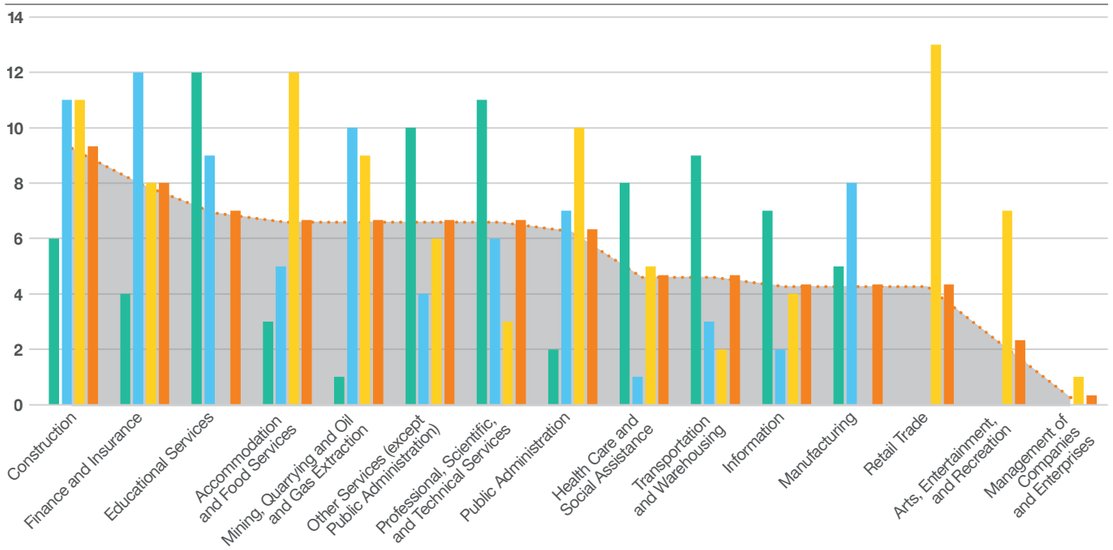
Finding Severity by industry

Finding Severity as Sum of CVSS per Project Day



Key metrics by industry

Key metrics for the over-all vulnerability of different verticals



Research Notes

About the data

- 296 new Penetration Tests reports in scope
- Period reviewed October 2022 to September 2023, making a total dataset of 1,799 reports
- Average CVSS score for CVEs report is 6.93
- Average number of findings per project 7.71
- 17.67% of findings are rated ‘Serious’

This dataset includes Clients from over 10 different countries. The selection of project types in this chart above is a subset of project types compromised of WebApp, Internal, External, Mobile, and Application Security. The type of projects our penetration testers engage in are for the most part determined by our Clients. Our clients in this dataset have contracted us for over 930 hours of WebApp testing from Q4 2022 through Q3 2023. This is the same amount of time allocated to External, Internal, Mobile and Application Security projects combined.

Clients sampled

A subset of our Clients was classified per Industry and business based on employee count. Where comparisons are made based on Industry and employee count, bear in mind that the data set is smaller. The distribution of projects per Industry varies and only provides a metric that is useful when combined with observations such as the Vulnerability Operations Center (VOC) scan results.

Having said that, we can assert that our clients in the Finance and Insurance and Public Administration industries rank high in both Penetration Testing and VOC Industry datasets, suggesting that these businesses are investing in improving cyber security postures.

Types of tests

Project type	%	
Application Security	6.5%	Application Security involves evaluating discrete application that runs natively on an OS
External	21.12%	A simulated attack from outside the test scope. Typically, from across the Internet.
Internal	10.78%	Simulating a breached network and attacking assets on the private network of a client.
Mobile	11.63%	An assessment of an application running on a mobile OS like Apple iOS or Android.
WebApp	50%	Attacking an application that is typically accessed via a web browser.

Average Time per Project type

Pentesting
Dataset demographics

Industry	%
Finance and Insurance	35.68%
Information	14.05%
Public Administration	13.51%
Professional, Scientific, and Technical Services	11.35%
Management of Companies and Enterprises	5.41%
Transportation and Warehousing	4.86%
Health Care and Social Assistance	4.32%
Other Services (except Public Administration)	3.78%
Mining	3.24%
Accommodation and Food Services	1.08%
Retail Trade	1.08%
Arts, Entertainment, and Recreation	0.54%
Construction	0.54%
Manufacturing	0.54%

The distribution of projects assessed per business size shows us that Small to Large businesses are engaging in penetration testing services.

Dataset caveat

For operational reasons, not all clients can be categorized by Size and Industry, so the data included here is not a complete representation.

World Watch

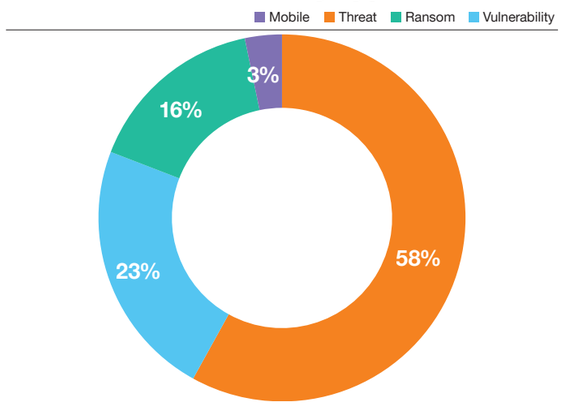
Our World Watch service published 491 advisories for the period October 2022 through September 2023 averaging over 40 advisories per month – a combination of new and updates on previously covered topics. At a high-level World Watch covers vulnerabilities and threats. We have split out two other categories, Mobile and Ransom, to monitor. Rather than being the only themes that emerge in our advisories, these are specific contexts we have chosen to monitor from a research perspective.

The advisories are also classified according to one of five urgency levels - Informational, Low, Medium, High, and Critical. Fortunately, we did not see the need to use the Critical urgency, which is reserved for exceptionally bad situations. The bulk of our advisories this year were assigned an urgency of Medium or Low.

About the data:

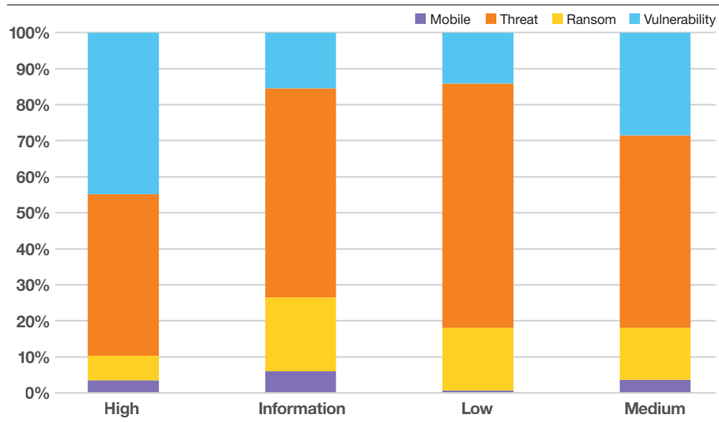
- Number of advisories: 491
- Average number of advisories per month: Over 40
- Period analyzed: October 2022 to September 2023
- Themes: Threat, Vulnerability, Ransom, Mobile
- Distribution of advisories per theme: 58% Threat, 23% Vulnerability, 16% Ransom, 3% Mobile
- Distribution of Urgency: 33% Medium, 31% Low, 24% Information, 12% High
- No Advisories with Urgency Critical was issued for the period.
- 202 distinct CVEs were mentioned in World Watch Advisories

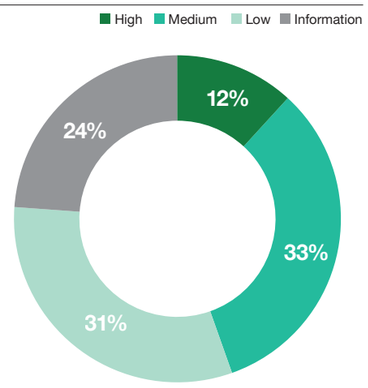
World Watch advisory types



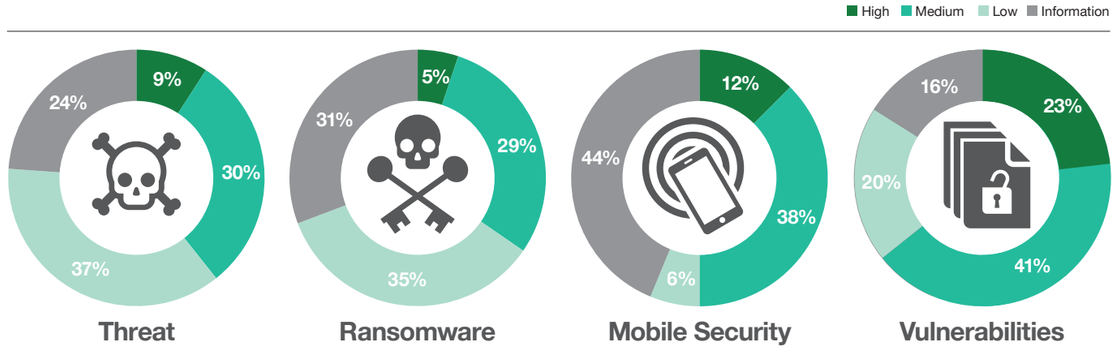
Urgency

Security Advisory types by Urgency



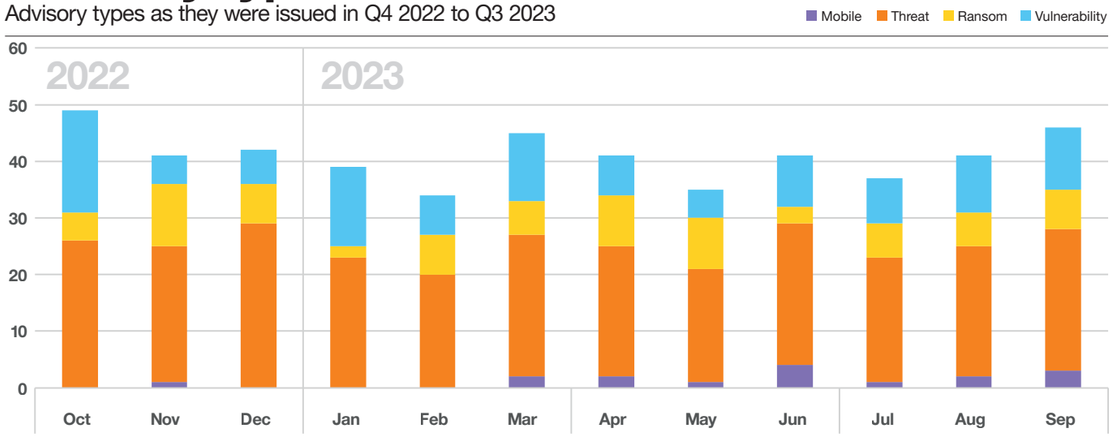


Urgency of advisory types



Advisory types over time

Advisory types as they were issued in Q4 2022 to Q3 2023



Urgency

No advisories with urgency Critical were issued for the period. This is somewhat astonishing given the almost overwhelming scale and frequency of security 'drama' that occupied our minds over the past 12 months. The fact that we didn't have to raise any of these incidents to a Critical level is a tribute to the resilience of our security systems and the level-headedness of our CERT team. Yet the CISOs we speak to universally wear a kind of "thousand yard" stare and report being nearly overwhelmed by the verocity of the security news cycle.

Threats

The World Watch team published 285 advisories describing Threats, this constitutes 58% of all advisories published for the period – made up from a combination of 111 new advisories and 174 updates on existing advisories.

The high proportion of Advisory updates illustrates just how important it is for defenders to have a way to track threats as they develop. This is a somewhat under-examined challenge: Threats and Vulnerabilities are not one-time events. Rather they evolve and our understanding of them develops. Our response needs also needs to adapt as the threat evolves or new insights emerge.

Threats & Technologies

Technlogies or Vendors mentioned in World Watch Advisories relating to threats

Note: In the chart above we omit Google and Microsoft because these two vendors skew the chart considerably.

There are some familiar names in the remaining list of vendors mentioned in our Threat Advisories that remain. It is also notable that we continue to encounter major security vendors in this list.

We also note the emergence of LastPass and Okta – two names that as we write are rapidly and dramatically earning a place in our Advisories, our data, and next year's report.

Ransomware

The cybercrime ecosystem is not shrinking, and as our Cy-X research has shown, ransomware and its associated extortion activities have regained momentum off the back of a slow 2022. Several groups are active, some more than others, and the better resourced groups are evolving their wares.

In November 2022, Orange Cyberdefense published analysis on new features present in the Play ransomware. These features are aimed at hiding the nature of the malware and to make it difficult for others to learn how it functions. The analysis we did proved useful when our Computer Security Incident Response Team (CSIRT) were called in the following month to deal with an incident involving Play.

In February 2023, alarm bells rang as a wave of cyberattacks were observed hitting VMware ESXi server. Malware dubbed ESXiArgs ransomware was used by attackers that compromised ESXi Servers by exploiting a vulnerability in OpenSLP. The panic was somewhat misplaced, as most of the victims were out of date self-hosted ESXi servers on popular cloud hosting service providers. The attackers had also evolved the malware to improve the encryption speed, and it was later discovered that encrypted data could be recovered due to the partial encryption approach used to improve speed.

These events seemed serious in isolation, but nothing could compare with the sheer scale of what Cl0p did to Fortra's GoAnywhere MFT and Progress' MOVEit Managed File Transfer (MFT) solutions. Using a 0-day vulnerability, Cl0p and other groups exploited hundreds if not thousands of internet-facing systems, downloading large volumes of data and later using Cyber Extortion techniques to put pressure on victims. This involved not only businesses who ran the vulnerable software, but also business partners and other 3rd parties whose data was being processed on them. In July 2023, the situation reached such a level that the U.S. State Department offered a reward of up to $10 million for information linking Cl0p to attacks targeting U.S. critical infrastructure.

Mobile

Orange Cyberdefense is part of Orange, a major telecommunications player. As such, we find the threat of attacks against mobile devices warrants special attention. This is why we track it as a separate theme from the general topics of Threats and Vulnerabilities. We believe that attacks against mobile devices will become more important as adoption continues to grow and this technology becomes more essential to personal, businesses and cybersecurity technology.

For example, the threat of espionage gives governments sleepless nights, and the threat of surveillance by some governments on ordinary people is equally scary. But these types of threats require a level of sophistication that is not yet generally accessible.

In last year's report we raised concerns about the challenges of managing vulnerabilities in enterprise mobile phone estates, and postulated that, as mobile phones assume a critical role in the enterprise security stack, criminals would begin to adopt more sophisticated hacking techniques to exploit phones and thus bypass controls like Multi Factor Authentication.

We have yet to see this threat emerging in any significant way.

However, the issue of mobile phone security has continued to grow and has featured prominently in our security advisories this year. For example:

- By July 2023, Apple had already issued patches to address 11 0-day vulnerabilities in several of Apple's operating systems, including iOS. By September 2023 the tally rose to 16 0-days for the year. Once again, the Israeli surveillance firm NSO Group and its Pegasus mobile malware made headlines through research published by the non-profit research group CitizenLab.
- We reported on examples of mobile surveillance by actors other than NSO Group. Google Threat Analysis Group (TAG), with assistance from Amnesty International, published findings on another surveillance activity possibly related to a surveillance vendor called Cytrox. Shortly thereafter, we highlighted work by CitizenLab and Microsoft that pointed to possible surveillance malware called 'Reign', attributed to the Israeli vendor QuaDream.

In last year's report, we examined the relative pros and cons of the Apple and Android environments. This year we see these attributes continuing to shape the threat landscape in different ways.

Apple iOS features frequently in reports as the targeted device, but surveillance vendors such as Cytrox have a complete solution for Android devices also. For attackers and malware writers, iOS platforms have the benefit of being homogenous. In other words, the code base is stable across many versions of the operating systems and runs on many hardware platforms. This allows one 0-day to work on many Apple handsets running a range of iOS version in a predictable manner.

Android has one inadvertent advantage in the numerous device vendors and flavours of the operating system, so attackers cannot rely on just one exploit chain to exploit a wide range of devices or operating systems. This, however, can also make asset and vulnerability management more challenging.

Apple has managed to develop a "privacy halo" that shines on their mobile products, giving it an aura of trustworthiness, so people valuing privacy may tend to gravitate towards Apple. Thus Apple may be more commonly used by the very people surveillance operations are targeting.

Another reason why we appear to observe more sophisticated attacks against iOS then against Android is that Android presents attackers with simpler options.

A feature of Android that iOS lacks is the ability to sideload applications. Sideloading allows users to install mobile applications without having to use the official Google Play Store. Anyone can install a compatible Android application on their handset. This is particularly useful for malware known as trojans.

For example, malware with traces of code linked to the Bahamut campaign was reported on toward the end of 2022. The Android trojan masquerades as the "SecureVPN" mobile application that then proceeds to steal information from the phone itself, as well as installed applications.

This technique is quite common. Another Android application with a strong Chinese user base, Pinduoduo, was found to contain three exploits that target 2 Samsung vulnerabilities and 1 Android vulnerability. Pinduoduo is supposedly a legitimate ecommerce application for mobiles, and the software vendor denies the presence of any exploits. The question of how the exploits ended up in the mobile application remains unanswered and raises the suspicion of either a supply chain compromise or coercion by an outside authority.

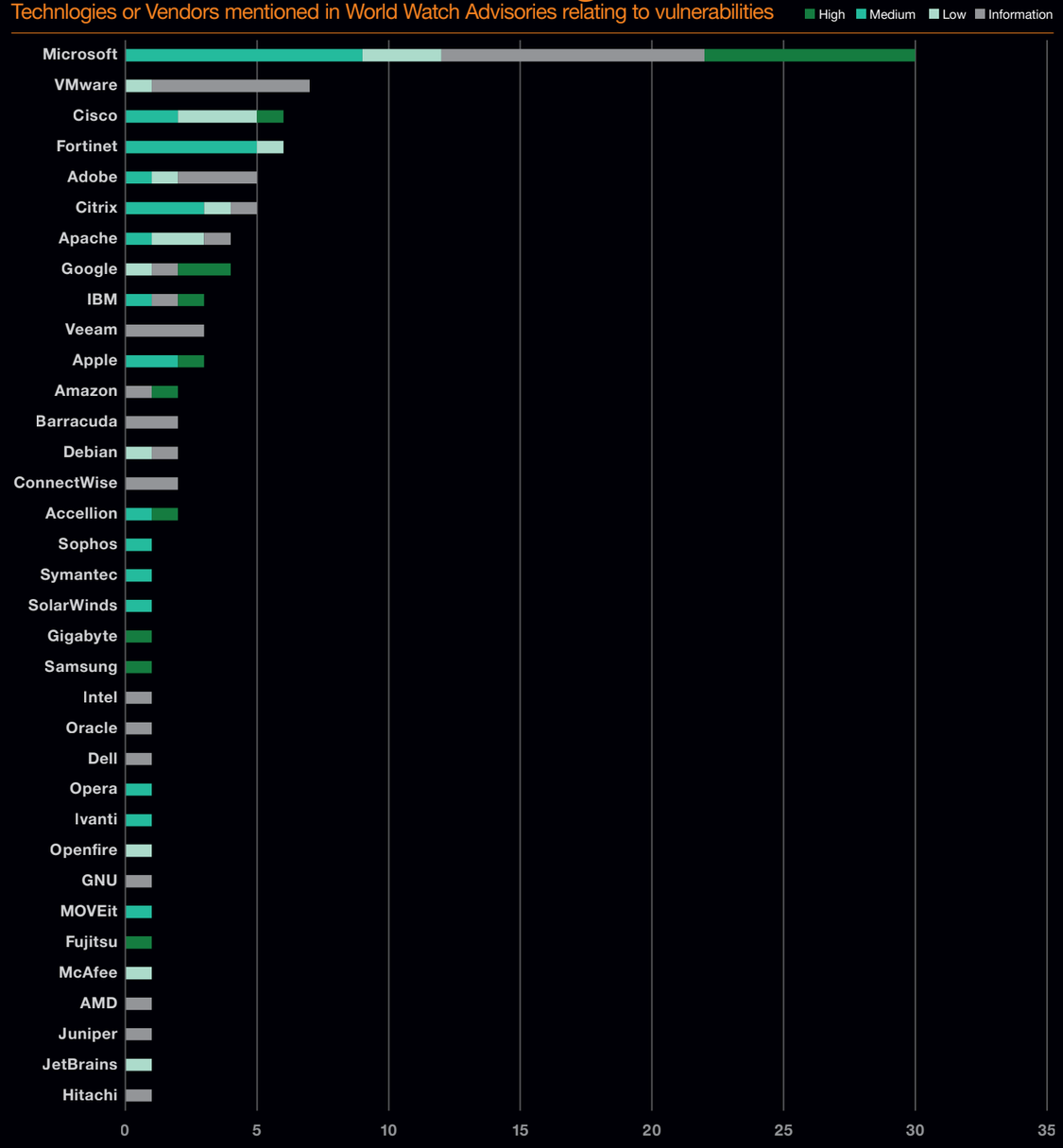
Newer versions of Android spyware called WyrmSpy and DragonEgg were reported on in July 2023 by Lookout Threat Intelligence. The Android spyware has been linked to APT41, a Chinese state-backed hacking group. According to Lookout, the spyware is not in common circulation, and victims are likely be compromised using social engineering techniques.

A trojan can thus be a cheap trick to get surveillance software on a victim's phone in the absence of more sophisticated exploits. Although currently only a real option on Android, cyber criminals will probably start to adopt this approach for iOS also when Apple starts to allow sideloading of applications to comply with requirements from the European Union. Sideloading of iOS application, which will possibly be a feature only available to users in the EU from iOS 17, is earmarked for 2024.

Although the issue of mobile phone security has not yet reached its zenith, and the story is still being written. We continue to caution our clients that the challenge of mobile vulnerability management is emerging and must be considered in medium-term security strategy considerations.

Vulnerabilities & Technologies

Technlogies or Vendors mentioned in World Watch Advisories relating to vulnerabilities



Research Question:

Is EPSS a possible way to prioritize Security Intelligence?

EPSS predicts the likelihood that a given vulnerability will be exploited. We note with interest that prioritizing Advisories that contain CVE with high EPSS scores surfaces an entirely different view on what intelligence to prioritize.

Choosing between left and right

The Exploit Prediction Scoring System (EPSS) is an initiative by the Forum of Incident Response and Security Teams (FIRST)[49]. EPSS provides a score, ranging from 0 to 1, for each registered vulnerability that has an assigned CVE code. The EPSS score indicates the likelihood of possible exploitation of a vulnerability within the next 30 days. The EPSS score can be used as part of a triage process when deciding whether and when to patch a given vulnerability. EPSS has been shown to be an accurate predictor and is rapidly becoming a valuable tool for vulnerability managers.

Along with each EPSS score is another value called the 'percentile' that provides a relative rank for the score assigned to a CVE. At the end of September 2023, there were 203,161 (94.73%) CVEs below the 95th EPSS percentile. Leaving 10,694 (5.26%) CVEs in the top 5% of vulnerabilities most likely to be exploited. If we were only concerned with CVEs, then we could focus our attention on CVEs in this pool.

World Watch Advisories split on CVEs at the 95th percentile of EPSS

Which Intelligence Advisories would be prioritized if we focused on the top 5% of CVE according to EPSS?

One way to explore the potential value of EPSS as a source of Vulnerability Intelligence is to apply it retrospectively. We could look back at past intelligence reports that reference a CVE. Some of our World Watch advisories meet this criterion. We can create two groupings named 'Prioritize' and the other 'Evaluate'. The former, Prioritize, represents the World Watch Advisories we might need to examine closely and reassess. The Evaluate group should not be discarded but should be revisited at a later stage.

Of course, this distinction is made for the purpose of this experiment only. Advisories with a high level of urgency should always be read carefully to determine if this impacts the business.

The chart to the left illustrates how one would view our World Watch Advisories if we apply a simple heuristic using EPSS. This is a simple experiment on using EPSS, but it demonstrates the potential value of the EPSS metric in triage.

If we prioritize advisories with CVEs in 95th EPSS percentile, we reduce the overall intelligence load to 27% of the total. As the chart shows, this grouping is surprisingly diverse, though most Advisories would still address Threats and Vulnerabilities.

The diversity of priority levels is more surprising, with 45% of these prioritized Advisories being categorized as 'Low Priority' by our CERT.

The Priority classification assigned to Advisories is a complex and context-aware process, and should not be ignored by defenders. EPSS predicts the likelihood that a given vulnerability will be exploited. We note with interest that prioritizing Advisories that contain CVE with high EPSS scores surfaces an entirely different view on what intelligence to prioritize. By highlighting specific CVE, this perspective also has the advantage that it identifies specific technical vulnerabilities that can be searched for and addressed!

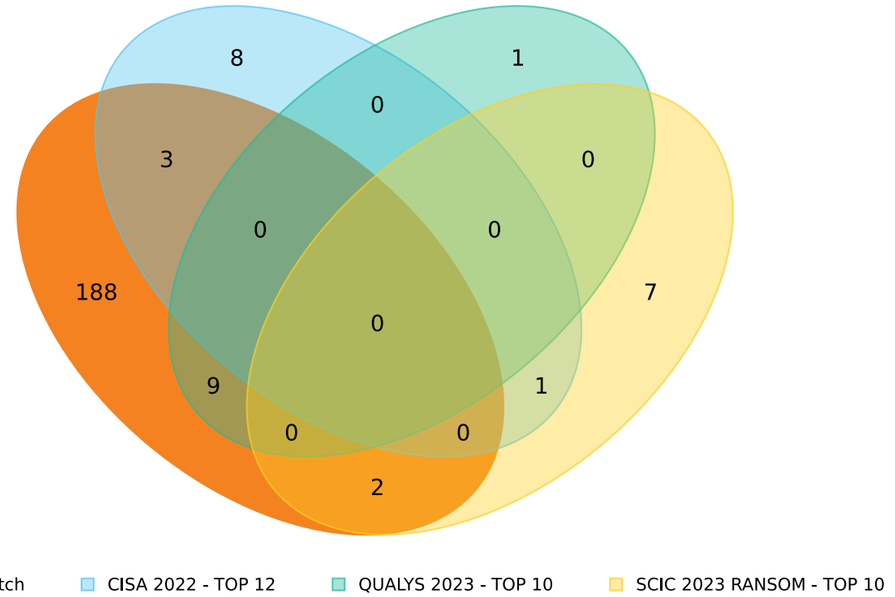
Research Question:

How much does our vulnerability intelligence overlap with other common sources?

We find that the overlap across popular vulnerability intelligence is small, but the vulnerabilities that do overlap are absolutely worth paying attention to.

The common bad

Overlap between World Watch and other popular Vulnerability Intelligence sources



Overlapping Vulnerability

The number of CVEs published in 2022 was 24.4% higher than in 2021. The number CVEs published in the first three quarters of 2023 was 12% higher than the same period in 2022. If this projection is linear then we can predict that in 2023 we will record over 28,000 new CVEs.

World Watch highlighted 202 distinct CVEs across all themes and a 121 distinct CVEs were raised in the context of Vulnerabilities.

To get a sense of the overlap between vulnerability intelligence sources, we evaluated these World Watch CVEs against the CISA 2022 Top Routinely Exploited Vulnerabilities, Qualys 2023 Top 10, and the jointly published Securin, CSW, Ivanti, and Cyware Ransomware Report for 2023. The World Watch CVE pool is as much as 20x larger than the other lists.

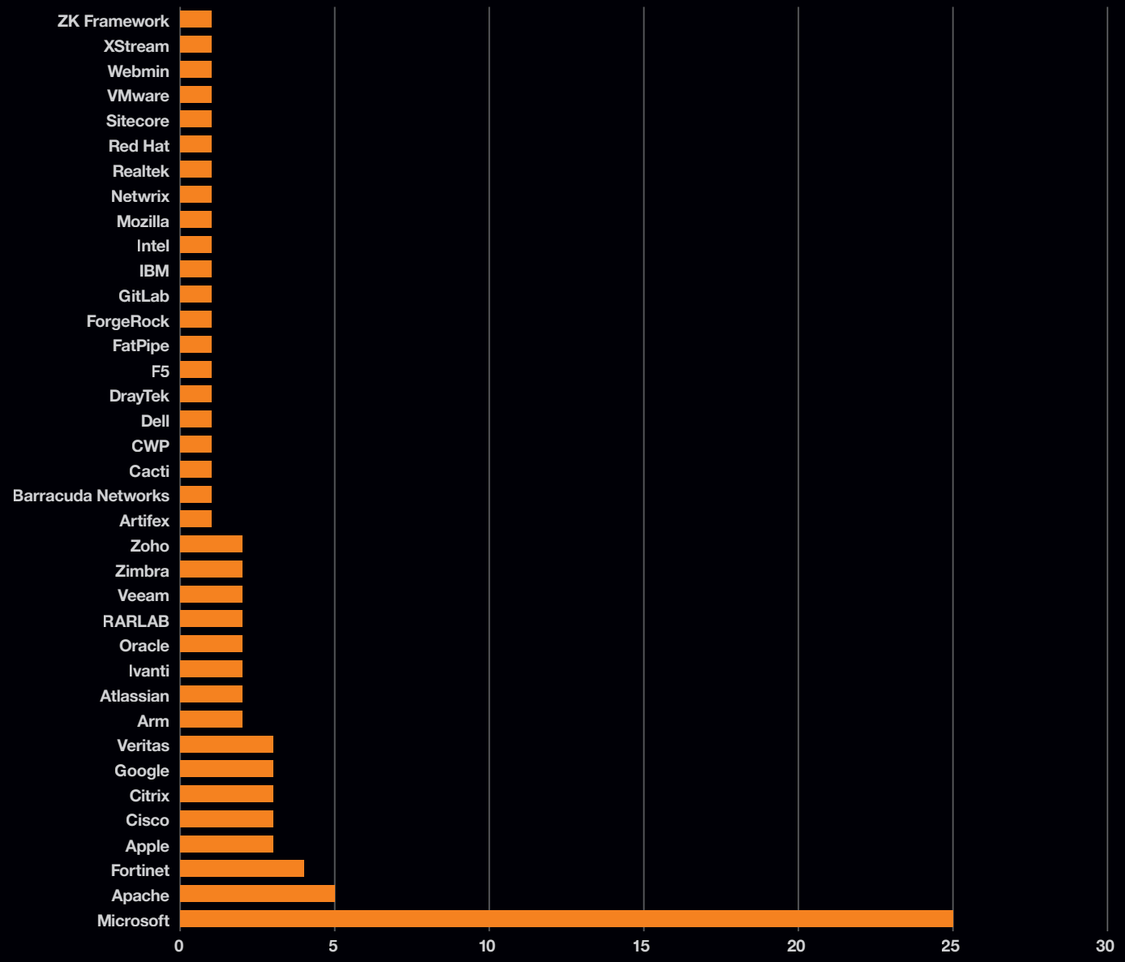
It is striking how small the overlap is between the four CVE groups. The exception is the Qualys list, from which 90% of CVE also appeared in World Watch.

Given the low level of commonality between these lists, identifying the most serious and important vulnerabilities from across all of them is somewhat tricky. Ranked Top X-lists are good at highlighting the tip of the iceberg when it comes to exploited vulnerabilities, but these might not even be applicable to your environment.

CVE	CVSS	Description
CVE-2018-13379	9.8	Fortinet FortiOS SSL VPN Path Traversal Vulnerability
CVE-2020-1472	10	Microsoft Netlogon Privilege Escalation Vulnerability
CVE-2021-45046	9	Apache Log4j2 Deserialization of Untrusted Data Vulnerability
CVE-2022-1388	9.8	F5 BIG-IP Missing Authentication Vulnerability
CVE-2022-22954	9.8	VMware Workspace ONE Access and Identity Manager Server-Side Template Injection Vulnerability*
CVE-2022-26134	9.8	Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability
CVE-2023-0669	7.2	Fortra GoAnywhere MFT Remote Code Execution Vulnerability
CVE-2023-20887	9.8	Vmware Aria Operations for Networks Command Injection Vulnerability
CVE-2023-23397	9.8	Microsoft Office Outlook Privilege Escalation Vulnerability
CVE-2023-24880	4.4	Microsoft Windows SmartScreen Security Feature Bypass Vulnerability
CVE-2023-27350	9.8	PaperCut MF/NG Improper Access Control Vulnerability
CVE-2023-28252	7.8	Microsoft Windows Common Log File System (CLFS) Driver Privilege Escalation Vulnerability
CVE-2023-2868	9.8	Barracuda Networks ESG Appliance Improper Input Validation Vulnerability
CVE-2023-29059	7.8	3CX DesktopApp
CVE-2023-34362	9.8	Progress MOVEit Transfer SQL Injection Vulnerability

Overlap in Vulnerabilities

Vendors in the CISA KEV CVE that overlapped with CVE highlighted in World Watch this year



The vulnerabilities in the table above mostly have satisfyingly high CVSS scores, but that there are some exceptions: the “Microsoft Windows SmartScreen Security Feature Bypass Vulnerability”, has CVSS score of only 4.4 and yet appears in all these lists.

It’s also somewhat sobering to note (again) the prominence of security vendor products in this consensus list about which vulnerabilities really matter.

The CISA Known Exploited Vulnerabilities (KEV) list is another intelligence source worth tracking. It may be very U.S. Government specific, but it is still a valuable source, given that many of the CVEs it lists impact popular vendors.

Placing the two lists side by side, we note that almost 10% of the 1,014 CVEs in the KEV correspond to 48% of the World Watch CVEs mentioned in advisories.

Even bearing in mind that World Watch is an Advisory service, not a ‘top-x’ list, we are surprised to find how little overlap there is between these intelligence sources. Where there is overlap, however, it is clearly a powerful signal that vulnerabilities need to be focused on!

Cyber Extortion

Since January 2020, we recorded 8,948 victims of Cyber Extortion that have been publicly listed on a 'leak site' on the dark web. Cyber Extortion, or 'Cy-X' is a form of computer crime in which the security of a corporate digital asset (Confidentiality, Integrity or Availability) is compromised and exploited in a threat of some form to extort a payment.

While this number of almost 9,000 victims seems high, we know that this is just a partial view on the whole problem of Cyber Extortion. This is obviously true because we note that the victims have been exposed on leak sites. This means they have already reached the end of the Cyber Extortion attack chain and threat actors have determined there is some value in making the purported compromise public. We are very aware that there is a high dark number of victims that we simply don't know of.

Overall trends in victimology

The year 2023 has seen the highest count of victims we have ever recorded, with the amount of Threat Actors participating in this criminal ecosystem and maintaining a leak site also returning to the (previous high) levels we saw in 2021. There are two concerning observations to be made here. First of all, the victim count for 2023 only includes the first three quarters. Secondly, it shows us that roughly the same number of actors can cause much more damage than they did 2 years ago (we don't believe this year's actors are the same actors as 2021).

The Cl0p-Effect

One important factor influencing the record numbers in 2023 is the Threat Actor Cl0p. Cl0p is one of the oldest Cyber Extortion operations we monitor. In 2023, they displayed advanced capabilities by exploiting 0-day vulnerabilities (in GoAnywhere and MOVEit), which resulted in several hundreds of victims being exposed on their leak site.

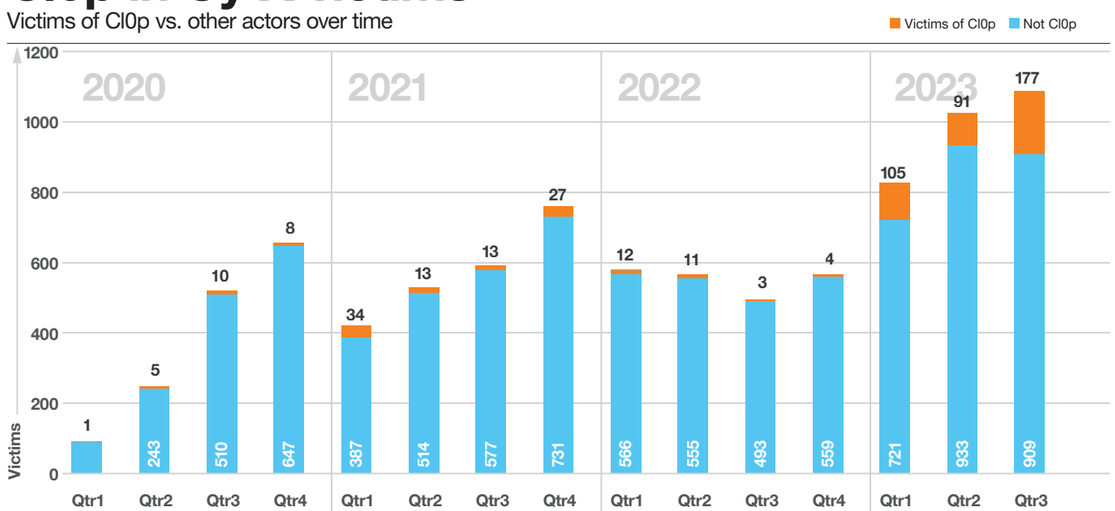
Even without the Cl0p victims, our overall observations still hold true, as we can see in the chart on the next page. We have never seen as many victims in any year as we have collected in 2023. Cl0p accounts for 373 victims in 2023, leaving a victim count excluding them of 2563 for the first three quarters alone.

In the past 12 months, since our last Security Navigator, we documented 3,502 victim of Cyber Extortion. This is an increase of 46% on the year before.

But who are the victims?

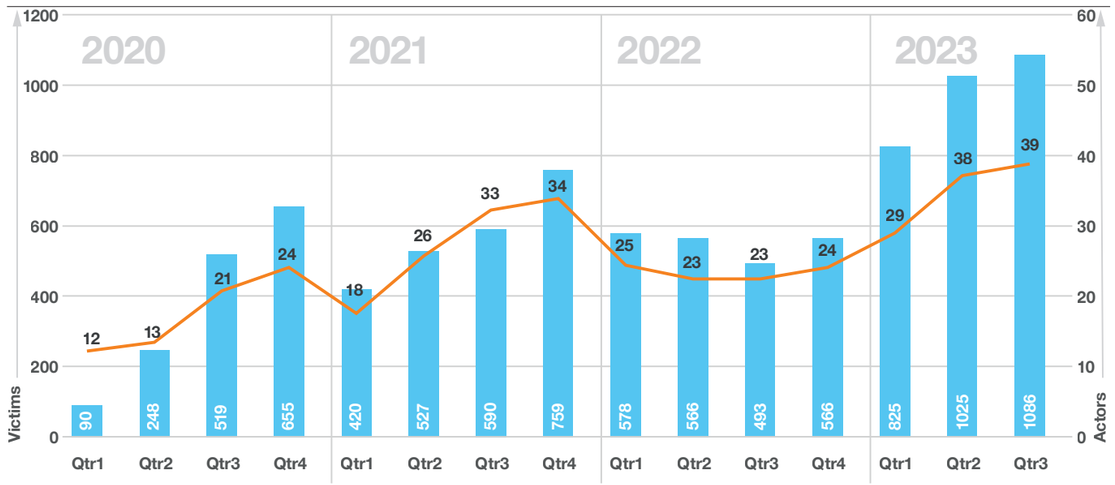
Cl0p in Cy-X victims

Victims of Cl0p vs. other actors over time



Cy-X over time

Victims and actors count observed on double-extortion leak sites over time

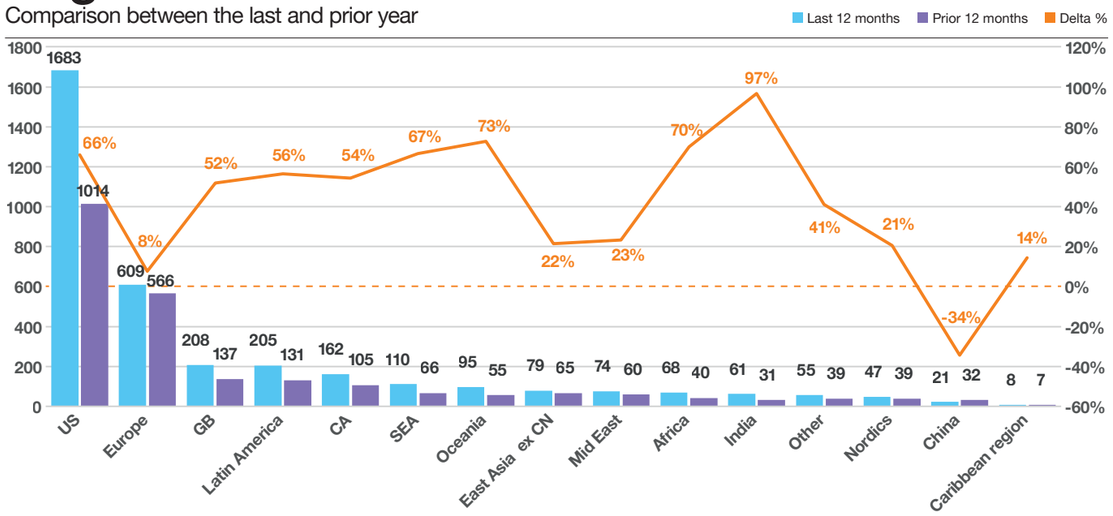


In the past 12 months, since our last Security Navigator Report, we documented 3,502 organizations that fell victim to Cyber Extortion.
This is an increase of 46% on the year before.

But who are the victims?

Regional shift in victim count

Comparison between the last and prior year



Country distribution / Geography

We observe that North America is the most impacted region. In fact, 53% of all victims for the past 12 months were headquartered in the United States (ranked 1st). This is followed by other English-speaking countries such as the United Kingdom (2nd, 6%) and Canada (3rd, 5%). We offer two potential explanations for this. First, as noted in previous reports, we believe that the size of the economy plays a role in why victim countries are impacted by Threat Actors. In our first annual Cy-X report, published in June 2023[50], we considered whether the number of businesses registered in a country could explain the geographical distribution in Cy-X victims. In that analysis, we noticed that the top 7 victim countries were also the countries with the most registered businesses. A large economy and number of businesses serve to predict the number of suitable victims.

India developing

There are other factors that play an important role in shaping the observed victimology, namely language and culture. Obviously, the email and website lures often used to achieve initial access require an actor to be fluent in the victim's language and have insight into their culture and business practices. Moreover, if stolen data is used to pressure and extort victim organizations, Threat Actors need to understand what they have compromised and what it's worth to the victim.

We believe that regional language and culture might act as a 'barrier to entry' to actors outside those regions, and thus served to help shape the victimology. But for a variety of reasons, this has recently started changing. Although English-speaking countries this year continue to account for the highest numbers of victims, we are seeing a shift to other regions.

For example, India has seen the biggest increase in victims over the past 12 months.

Given rapid economic growth in the country, this could be expected. According to the World Bank[51], India is one of the world's fastest-growing economies.
On the other hand, India's victim count is growing from a relatively low base, which we believe may be due to the barriers imposed by language and business culture. Cyber Extortion is a form of bullying in which victims must be coerced into paying for something that was already theirs. Depending on values, culture, and other contextual factors, businesses in different countries are likely to be more or less approachable to the actor and responsive to the coercion. Like China and Japan, India may be unfamiliar territory for most Cy-X threat actors. And, at the risk of grossly generalizing, we suspect that business culture in India may not respond well to the form of ransom negotiation that makes Cy-X function.

These two barriers appear to have been slowly eroding over the past 12 months, causing victim counts to move closer to where the size of the economy predicts. Despite this subtle change, the Indian numbers remain low in comparison with other similarly-sized economies.

Europe still in the cross hairs

Other countries that have been more heavily impacted over the past 12 months are the European countries. Here we see, Germany (4th), France (5th), Italy (6th) and Spain (10th) accounting for the most victims.

Oceania takes the lead

Australia (7th) and Oceania overall has seen an increase of 73%. This is interesting since Australia is the leader of the international taskforce to fight ransomware[52], but this effort does not seem to have had a deterrent effect on actors targeting the country. Instead, Oceania is the region with the second-largest relative growth over the last 12 months.

The South Arises

Latin America continues to feature prominently when we track changes in victimology over time. Here we mostly see Brazil (8th) and Mexico (12th). Victims in this region have been consistently increasing more quickly than elsewhere over time. We see almost every country in South and Central America impacted at least once by Cyber Extortion and clearly remember the attack by Conti against Costa Rica in 2022, "affecting the backbone of the functioning of the state"[53], which led the country to declare a state of national emergency.

The South East Asian Tigers

As we've noted already in June 2023, in our CyXplorer report, we observe above-average victim growth in South East Asia also, where LockBit is responsible for many of the cases. This is interesting if we believe that culture and language may have previously acted as a barrier to Cyber Extortionists. It looks like Threat Actors are overcoming the barrier of language and culture and increasingly impacting organizations in regions where they previously might have had issues understanding, communicating and negotiating. In the South East Asia region we see Thailand, Malaysia and Singapore impacted the most.

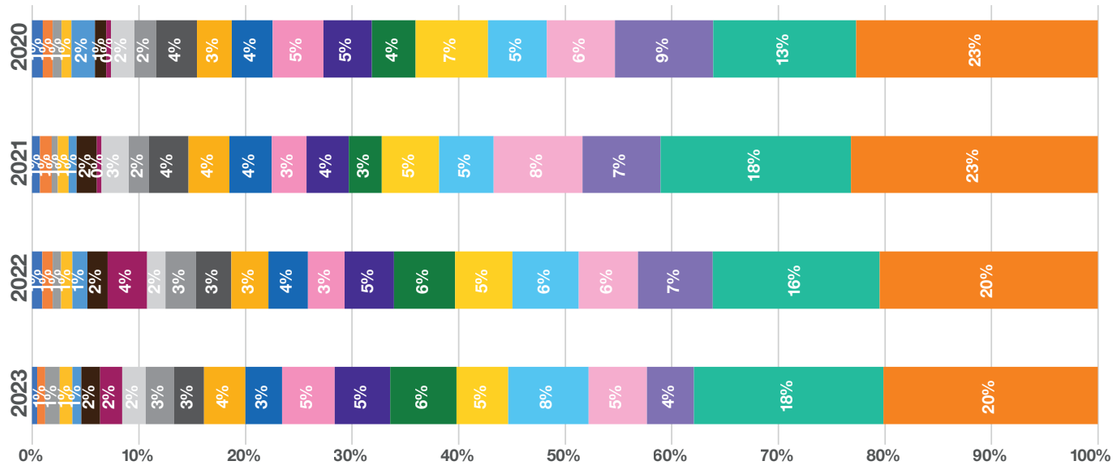
Industry distribution

In the past years, we have seen a rather equal distribution across several industry groups in our victim data. This is especially true when looking at the top 3 impacted industries. As can be seen below, Manufacturing has remained the most impacted sector over the 3.5 years we've been collecting this data. We have investigated the question of why Manufacturing features so prominently in our victim data, in last year's Navigator and elsewhere, and remain perplexed by the topic. To date we have been unable to find an explanation that contradicts our consistent hypothesis: The primary factor influencing victim demographics is the size of the target population.

Bigger economies and bigger industries will in general tend to be impacted more. Where we see deviations from this general pattern, as in the case of Manufacturing, these emerge primarily from attributes of the victims rather than deliberate choices made by the Threat Actor. In the case of Manufacturing, we currently still believe that vulnerability is the primary factor that determines which businesses get compromised and extorted. As our analysis of Industry patterns elsewhere in this report suggests, business in the Manufacturing sector may have less mature security postures and therefore find themselves more vulnerable to opportunistic attacks.

Victims by Industry

Distribution shift among verticals we saw affected by Extortion in different years



Big Business

The second most impacted sector, namely Professional Services is very diverse and includes the sub-industries Engineering, Accounting, Research, Business Services, and Legal Services. It is therefore also a very large industry. The Retail sector has remained somewhere within the top 3 or 4 impacted, except in 2023; where it has moved a few positions down to position 9.

Financing Cl0p

The Finance sector has seen an increase in 2023. This is largely due to a spike in June 2023, where the Threat Actor Cl0p exploited the MOVEit vulnerability and uploaded hundreds of victims to their leak site. Amongst the victims were many businesses from the Financial sector.

Extorting Education

Another observation we are making is that over the last two years the Educational Sector has started featuring significantly in our victim dataset. In fact, from 2022 to 2023 we saw a 115% increase in victims from this sector. Here we see universities, colleges, elementary and secondary schools, as can be seen in our Sub-Industry breakdown.

Extorting Information

Over the past two years, we note that the Information Sector has seen a significant increase of 129% in victims. We see Computing Infrastructure Providers, Data Processing, Web Hosting and Related Services, Telecommunications, Publishing Industry (including Software providers) and Broadcasting and Content Providers (such as radio, television, and media streaming services as well as social networks), to mention a few examples.

The sector was particularly impacted between March and August 2023, where we saw an average of 9. Threat Actors per month extorting victims. We have not previously witnessed this kind of high level of monthly Threat Actor activity for the Information sector. By comparison, February and August 22 we saw an average of 4 Threat Actors in action per month. In 2021, the average was 5. In the past 12 months, Cl0p, LockBit3, ALPHV (BlackCat), Play and BianLian impacted this sector the most.

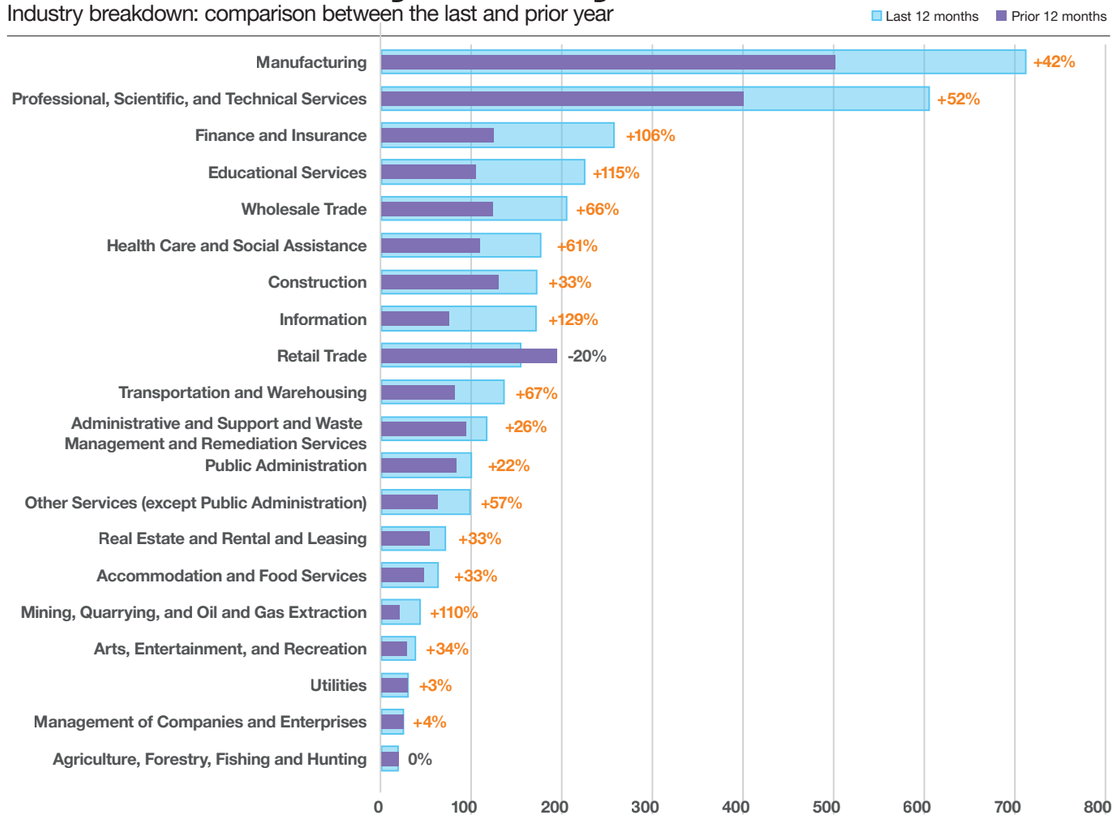
Extorting Transportation

Transportation and Warehousing also caught our attention. In the past 12 months, we noted a significant increase in victims from this sector, making it the 5th fastest growing industry. This sector has sub-classifications that include essential services in society, which makes it particularly interesting to us. For example, 13% of the victims were in Water Transportation, 11% in Air Transportation, 11% in Transit and Ground Passenger Transportation, 2% in Rail Transportation and 2% in Pipeline Transportation.

Pipeline transportation covers for transportation of oils or natural gases for example. The biggest sub-industry within this sector was Support Activities for Transportation. Those would the cover activities such as Air Traffic Control, Air Operations, Freight Transportation support[54].

Shift in victims by industry

Industry breakdown: comparison between the last and prior year



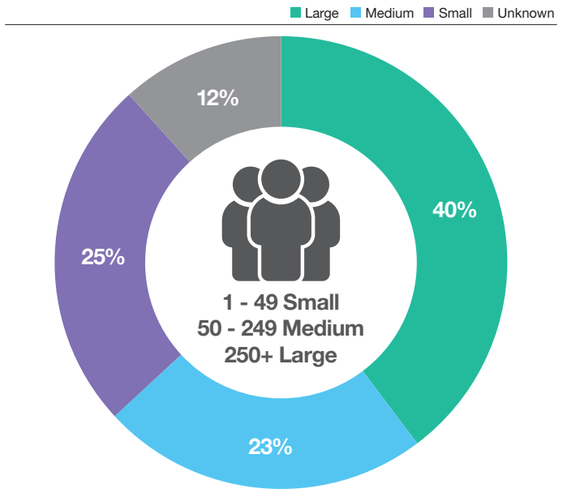
Business sizes

We've already established that organizations from different sectors around the world are being impacted by this form of cybercrime. Businesses of every size are also impacted. We observe Large Enterprises being impacted the most in real numbers. They are followed by Small organizations, which make up a quarter of all the victims and Medium-sized businesses, with a share of 23%. This is similar to the distribution we reported in our CyXplorer report in June 2023.

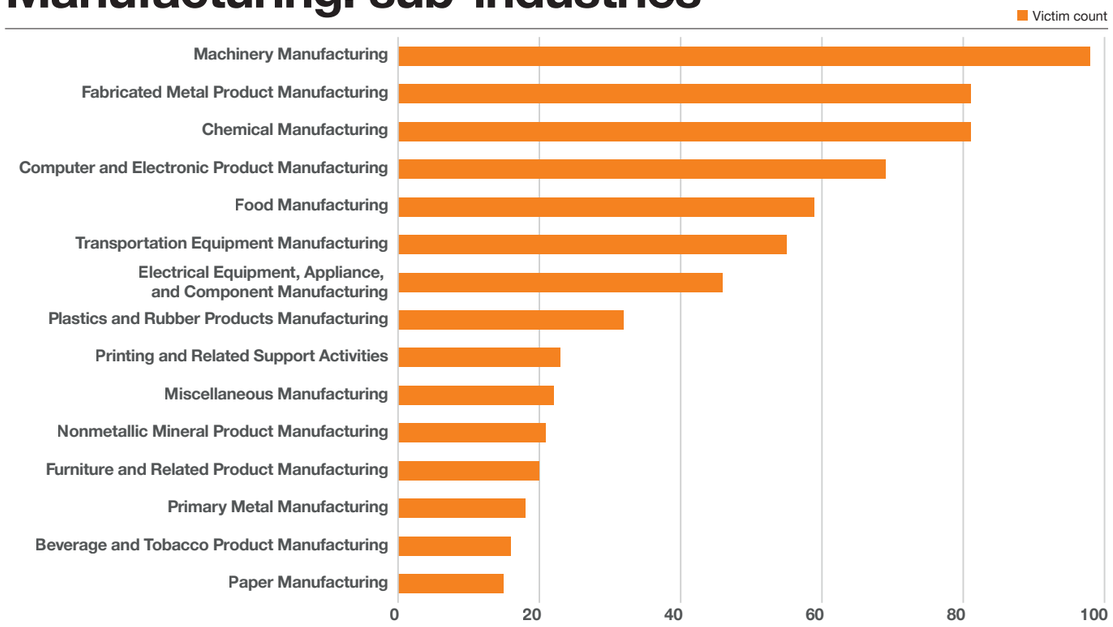
Noteworthy is that we see Large organizations being impacted more over the past 12 months, especially in August, when we saw victims with employee count of 1,000 to 9,999 peaking. This seems to be a collective contribution – including victims from LockBit, 8Base, ALPHV (BlackCat), NoEscape, Akira, and others – and thus not connected to a single event or single Threat Actor.

Victims with 10,000+ employees have seen a steady increase in 2023, most notably with peaks in March, June and July. This can be largely attributed to a single threat actor, namely Cl0p. They exploited two major vulnerabilities in 2023 and uploaded data from hundreds of victims during those months, many from the Large business category.

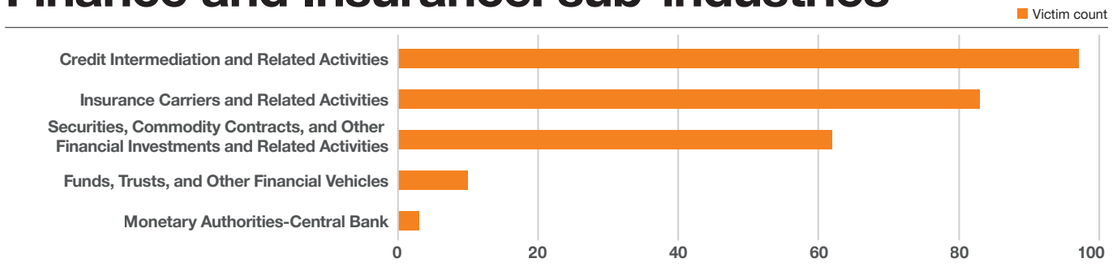
Cy-X victims by business size



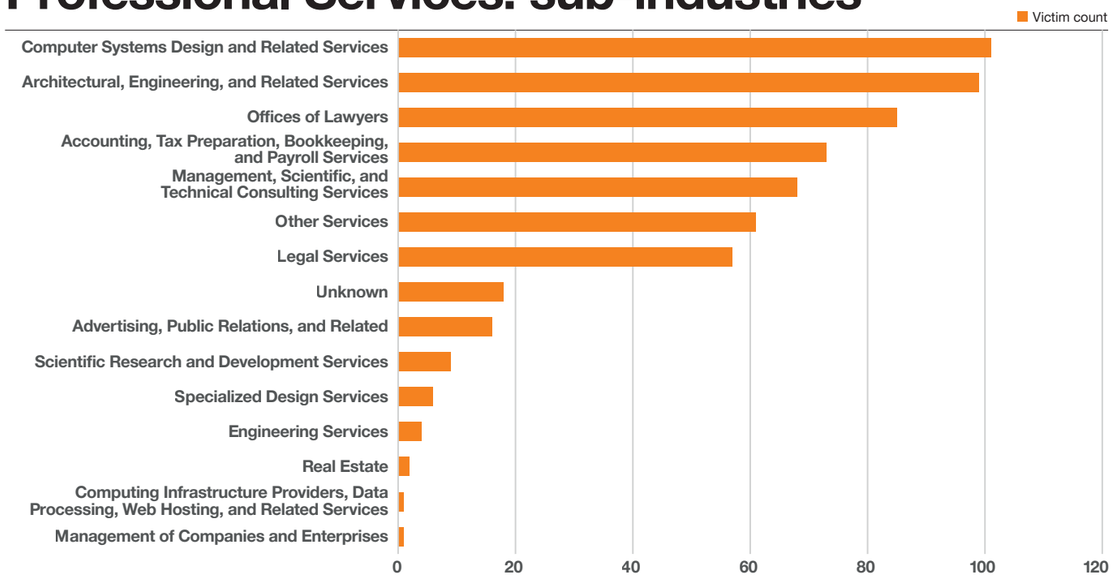
Manufacturing: sub-industries



Finance and Insurance: sub-industries

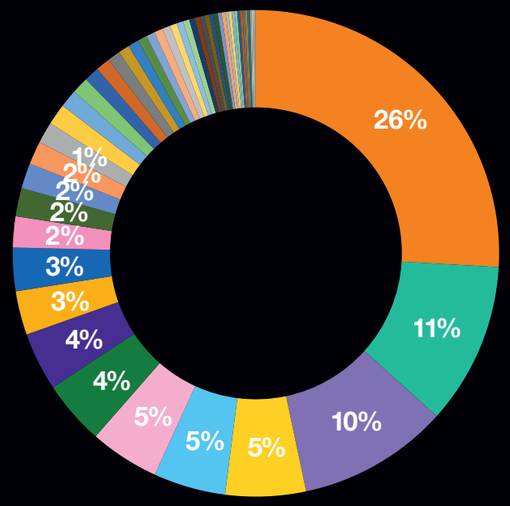


Professional Services: sub-industries



Threat Actors

Extortion groups observed in the past 12 months



- 26% LockBit3
- 11% Clop
- 10% ALPHV (BlackCat)
- 5% Play
- 5% Royal
- 5% 8Base
- 4% BianLian
- 4% Black Basta
- 3% Akira
- 3% Medusa
- 2% ViceSociety
- 2% BlackByte
- 2% Snatch
- 2% noescape
- 1% losttrust
- 1% Karakurt
- 1% Rhysida
- 1% cactus
- 1% Qilin
- 1% RagnarLocker
- 1% HiveLeaks

1% or less:

- cloak
- AvosLocker
- Abyss
- Mallox
- Cuba
- RA Group
- MONTI
- LV
- Everest
- metaencryptor
- incransom
- knight (cyclops)
- Lorenz
- Dunghill Leak
- Ransomhouse
- ransomedvc
- Darkrace
- ciphbit
- Money Message
- Trigona
- threeam

Threat Actors & the Cy-X ecosystem

The Cyber Extortion ecosystem has been highly active over the past 12 months but even more so since February 2023. This is an interesting observation, given the fact this also marks one year since Russias war against Ukraine broke out and we reported notable disruptions in Cyber Extortion operations. So, what has changed in the ecosystem to cause such an increase? To shed light on this, we explore which Actors are responsible for the compromises we are seeing.

Multiple personalities

If we're to believe the self-portrayals of Threat Actors, we are dealing with "honest and simple pentesters" that call their victims "customers" and offer "loyal" conditions in pursuit of the return their hostages – namely the stolen data – to the victims after payment has been received.

In reality, we are dealing with individuals or groups of individuals that conduct criminal activities by extorting organizations to receive a ransom payment.

Evolving tactics

Threat actors continue evolving their tactics, especially their extortion techniques. As previously observed, attacks no longer just involve encryption. But, especially in 2023, we have seen a larger proportion of attacks extorting money only based on stolen data, which we record as Data Extortion. Besides Data Extortion and the classic ransomware, we also observed a small amount of DDoS threats made by the Threat Actor group NoEscape. This is interesting since we last saw threats to DDoS from a long-gone group called Avaddon.

There are indications that NoEscape might actually be the first re-brand we have seen of Avaddon since they closed operations in June 2021, the main clue being that NoEscape's and Avaddon's encryptors are almost identical[55].

The major players

Who were the major Threat Actor groups over the past 12 months? In total, we recorded 54 Cyber Extortion operations with leak sites on the dark web. This is an increase in Threat Actors of 12.5% over 2022. As previously mentioned, the number of victims increased 46% over the same period. This disproportionality suggests how effective this criminal ecosystem has become.

Threat Actors observed during this report period are shown below. LockBit3 has remained the most prolific actor site since approx. 1.5 years ago when Conti was still active and claimed the top position. In line with the general trend, we saw a steady increase in LockBit3's activity during the past 12 months. In June 2023, the German BSI and the US CISA agency published a warning regarding LockBit, calling them the most dangerous ransomware group[56][57]. However, other Threat Actors have also been busy, and proportionally, we've actually been seeing less LockBit3. Another group that sticks out is Cl0p, who we have mentioned on several occasions already. Cl0p is closely followed by Play, who is responsible for 10% of all victims over the past 12 months.

The frequent changes in and between Threat Actor groups can make the ecosystem seem bigger than it really is. Our analysis shows a growth of 'only' 12.5% in active groups but the victim count is growing more rapidly. We examine Threat Actor movements in a dedicated analysis later in this report that might shed some more light to this.

Cyber Threat Intelligence

Accurate and timely Cyber Threat Intelligence (CTI) can help defenders better identify and mitigate vulnerabilities and attacks. CTI can also measure the credibility of possible attacks to reduce the number of security alerts IT teams face, so that they are freed to mitigate genuine attacks.

The Orange Cyberdefense Datalake was developed to deliver an integrated "Threat Intelligence Platform" (TIP) that allows allows our analysts and customer organizations to see what is being detected by threat intelligence sources around the world. It presents relevant information in a format that eases the analysis of Indicators of Compromise (IoC), providing risk scores given by our security experts to facilitate decision making.

The datalake collects, normalizes, enriches and offers up standard CTI Indicators of Compromise (IoC) like domains, FQDN, IP and URLs, but also other types of data such as emails, pasties, hash files, malware signature, registry keys, data related to finance, such as IBAN numbers, and so forth.

The original threat data (called "Events") include Orange's tier-1 telco operator Internet backbone feeds, Orange Cyberdefense feeds, open-source threat intelligence feeds, customers and partners.

Threat data is being generated at an astronomical rate. The chart below illustrates just how much data the datalake ingested this year.

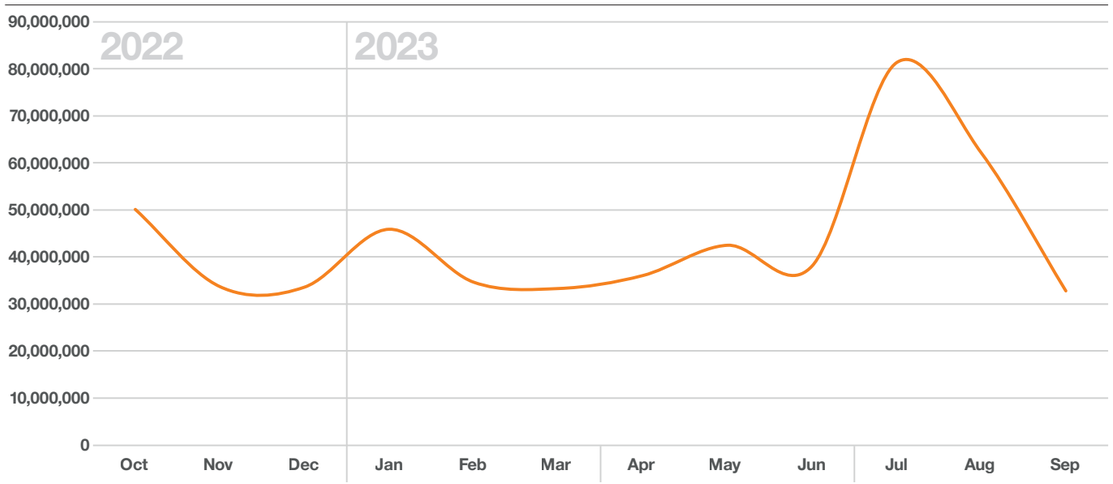
The datalake continuously ingests security data from nearly 500 distinct sources. From these sources, we processed over 500 million distinct inputs during this reporting period.

About the data

- **Period:** 01 October 2022 – 30 September 2023
- **Number of Data Sources:** 473
- **Ingested Events:** 526,582,280
- **Unique Indicators:** 246,113,573
- **Data sample:** 2,245,430 Unique IP indicators
- **Sampled between:** 01 April 2023 & 30 September 2023

Processed IoC data

Datalake Indicators ingested over time

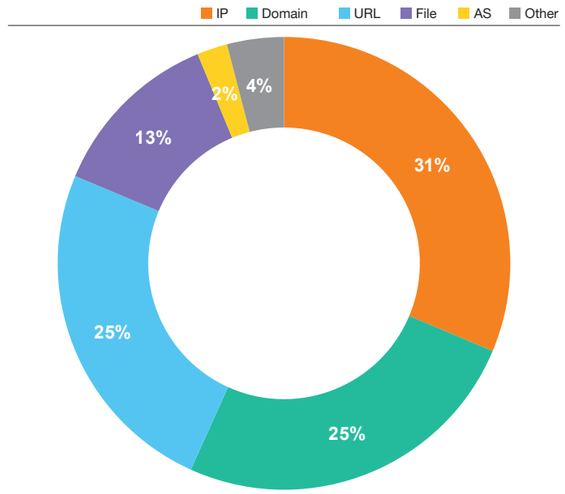


We collect a variety of IoC types, as depicted by the chart to the right.

The majority of the IoC we collect are IPs and Domains, which together constitute over 50% of the data we collect.

As we collect IoC we remove duplicates. About 53% of the Indicators are unique. We also use a proprietary algorithm to assign each indicator a 'Risk Score' between 0 and 100. This scores serves as an indicator of how trustworthy we believe an indicator to be. The Risk Scores can be manually adjusted by our Threat Analysts as they investigate Incidents, but are also algorithmically adjusted using variables like Sightings, the fundamental trust we assign to the source and how many unique sources report the same indicator.

Datalake IoC collected by Type



Uniqueness

Our CERT team has conducted internal research into the relative "uniqueness" of the intelligence we produce. With CTI, a key question is always "how much do we need", and "how much value does additional intelligence add"? To assess this question, the team investigates how much of the intelligence we can offer that isn't already available in other data sources.

Every CTI product must have unique properties to be competitive in the market, and for us one differentiating feature is the internal intelligence we collect, from Orange as a mobile operator, and from our own in-house capabilities. Some examples of these bespoke sources can be found below.

Orange Cyberdefense uniqueness rate

48%

Mean > 48% exclusive intelligence

C2 Monitoring

- Active C2 tracker, with ~0% false-positives, tracking 43 malware families, including Cobalt Strike, Sliver, PoshC2, Quakbot, Bumblebee and more.
- Over 10,000 active C2 trackers in database.

38%

Mean > 38% exclusive intelligence

Phishing Initiative

- https://phishing-initiative.eu/
- Backed by Orange Cyberdefense CERT experts
- All intelligence is a result of manual analysis

42%

Mean > 42% exclusive intelligence

Detect DNS

- Based in DNS Telemetry to identify phishing and malicious domains
- Backed by CERT Threat Intelligence experts

42%

Mean > 44% exclusive intelligence

P2A Sandbox

- Proprietary in-house sandbox developed by Orange Cyberdefense
- Automatic malware identification and configuration extraction

There are other internal sources also, e.g. IoC noted in incidents and registered by our CyberSOC and CSIRT teams, but for confidentiality reasons they are not reflected in the chart on the previous page.

As some of our intelligence is boutique and sourced internally, that begs the question how "unique" our data is compared with other sources available to defenders.

Given that there will also be data in those other sources that are not present in our datalake, it is clear that our clients enjoy increased visibility when additional intelligence is added. Whether the additional intelligence warrants the additional cost, and what that tipping point is, remains open for debate.

The great intelligence dilemma

The effectiveness of any kind of security intelligence lies on an asymptotic curve – no matter how good it is, it will always be missing something. And since we can't know how much there is to know, we can never know how much we're missing.

That begs the question of whether improving the effectiveness of any security intelligence makes any sense at all. No matter how much we know, there will always be unknowns.

All forms of intelligence-led security suffer from the same tension between three factors – False Positives, Limited Resources & the infamous Unknown Unknowns.

At what levels do these come into balance and, given that we will never know the Unknown Unknowns, is there any real logic in pursuing them?

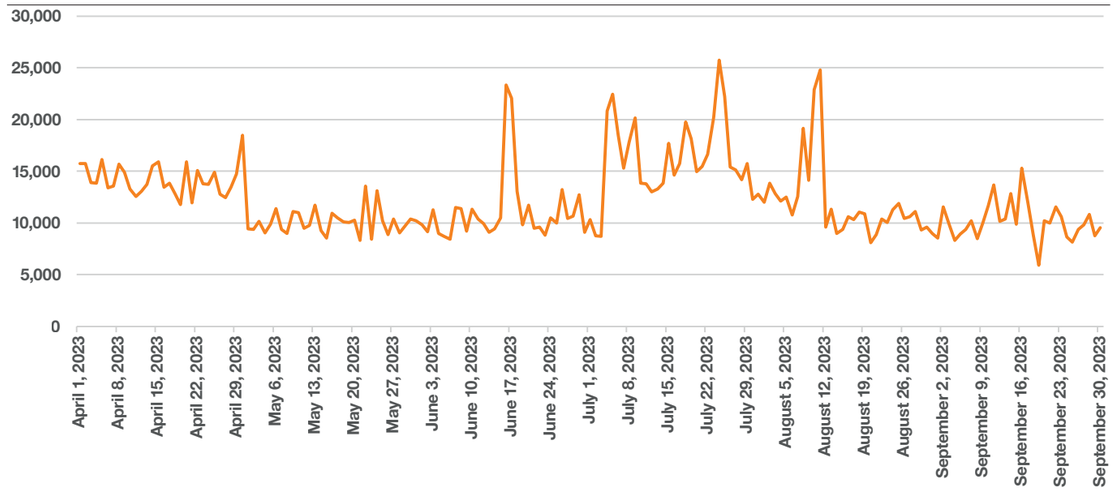
Would our limited resources not be better spent in proactively engineering robust systems?

This dilemma holds not only for Threat Intelligence, but also for Threat Detection, Bug Hunting, Vulnerability Scanning and other domains.

We hope to bring some data and transparency to this debate through reports like this one, and we hope other vendors will join us in providing objective insights that defenders can apply to do the difficult decisions they have to make.

Malicious IPs

IP IoC collected for this sample over time



Data sample

For the purpose of this first public exploration of our IoC data, we extracted a sample of all the unique IP address indicators recorded in the Datalake between 01 April and 30 September 2023. This sample represents just under 2.5 million datapoints, which is a paltry sample of the full dataset. While this is therefore just a humble introduction to this remarkable dataset, we believe that there are interesting questions to be raised, and anticipate expanding on this research with bigger samples in future research.

What we see

Although limited, the sample dataset provides insights into the volumes, effectiveness and diversity of the IoC we produce.

The source of all wisdom

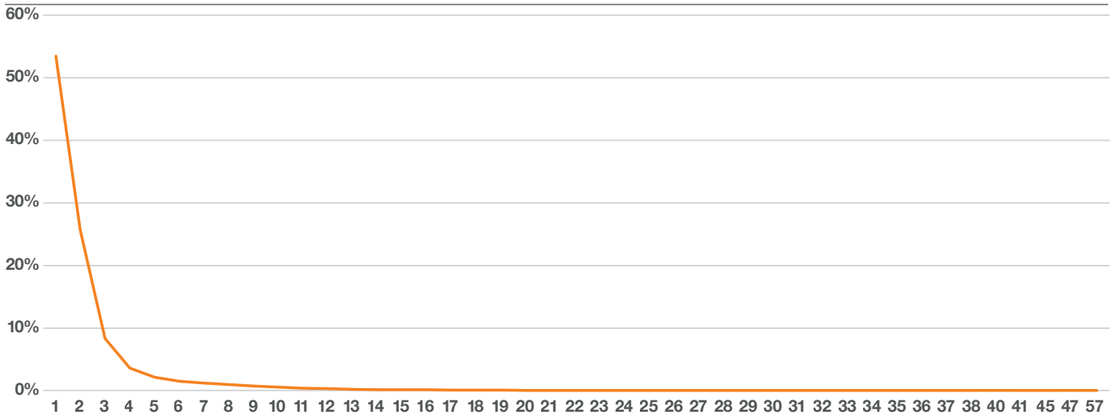
We ingest nearly 500 CTI sources, including internal, commercial and open source offerings. So how much value do we get from each source?

We note that 50% of all IoC are contributed by just 5 CTI data sources. The most prolific source alone contributes 16%. The 'long tail' of ROI starts at the 20th data source. From here on each data source contributes less than 1% of all the IoC.

On average, each unique IoC is contributed by 2.2 sources. But once again, the distribution is highly skewed:

Sources across IoCs

Distribution of the number of distinct Sources across IoC



As the chart above illustrates, 53% of IoC are contributed by just one Source, while a further 26% are contributed by two different Sources. And although some IoC are reported by more than 50 sources, more than 98% of all IoC are reported by 10 sources or less.

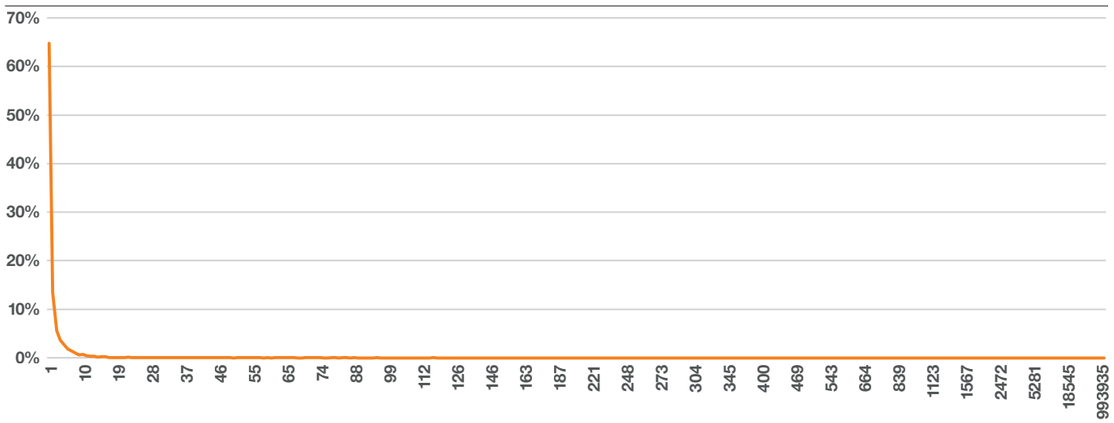
Correlation

Every time an IoC is submitted to the datalake we update an event counter. So analyzing the Events Count can give us a sense of how many times a given IoC has been submitted and re-submitted by all our diverse sources.

The Average Event count is 15.5.

Confirmed IoCs

Distribution of IoC confirmations - 10 or less



Just under 68% of all IoC are only submitted once and 96% are submitted 10 or fewer times.

A Risky Business

Each IoC is assigned a risk score, initially derived from the value of the source, but adjusted manually over time by intervention, correlation, sightings, etc.

The Risk Score gives defenders a means of focusing on IoC that are likely to be better predictors of malicious activity, because they come from a reliable source, have been reported by multiple sources or have been associated with Incidents somewhere in our operations.

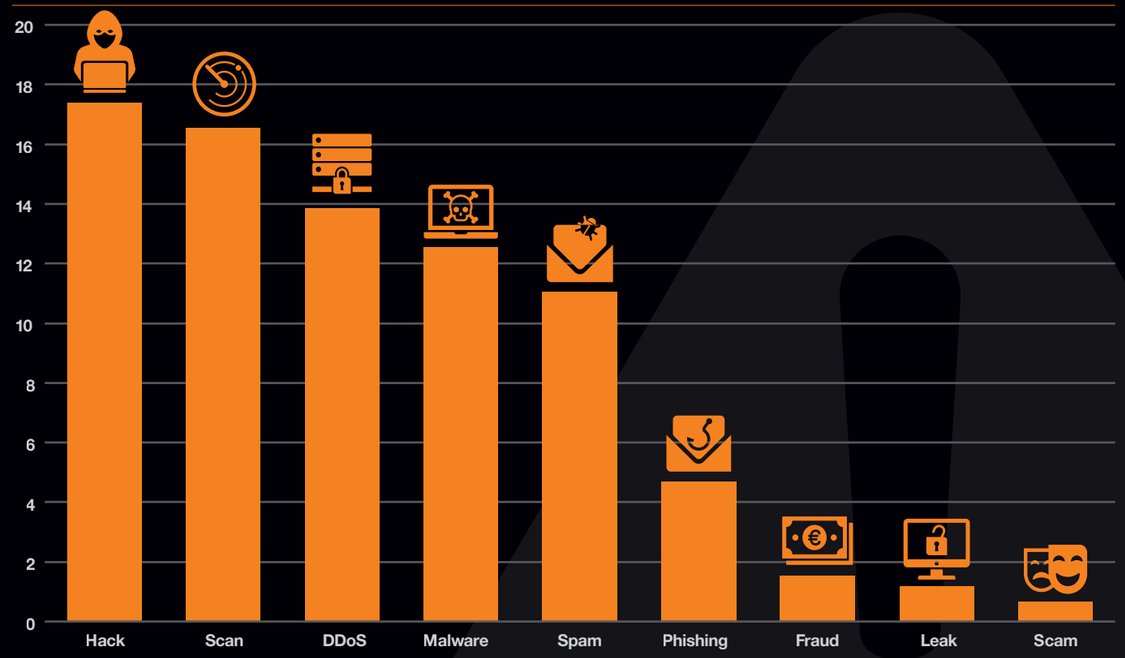
The shape of this distribution is intriguing: 33% of all IoC have a risk score of 20, and 98% have a risk score of 20 or less. 0.12% of IoC have a Risk Score of 100.

This characteristic is more easily understood when we consider that each IoC is assigned a risk score between 0 and 20 in any of nine categories: Hack, Scan, DDoS, Malware, Spam, Phishing, Fraud, Leak and Scam.

The average Score (on a scale of 0-100) assigned for each of these Risk types is as follows:

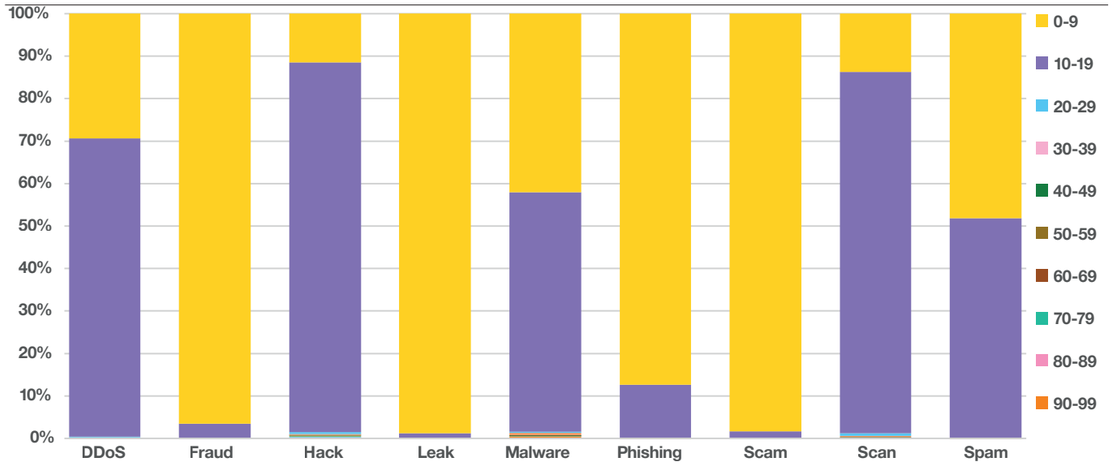
Risk Score per type

Average Risk Score by Risk Type



Risk Score per type

Average Risk Score by Risk Type



The distribution of Trust Scores across the different Threat Types is quite diverse. It's clear to see that vast majority of IoC have a Risk Score below 20 across all Threat Types.

Some Tender Loving Care

After being ingested, an IoC needs to be enriched and its Risk Score needs to be updated as more sources submit it, its seen in the wild, or an analyst manually reviews it.

How often does this happen?

To answer this question we consider the 'Last Updated' field of an IoC. If this is more than a day later than the 'First Seen' date on which the IoC was first catalogued in the Datalake, then we consider the IoC to have been 'Updated' in some way.

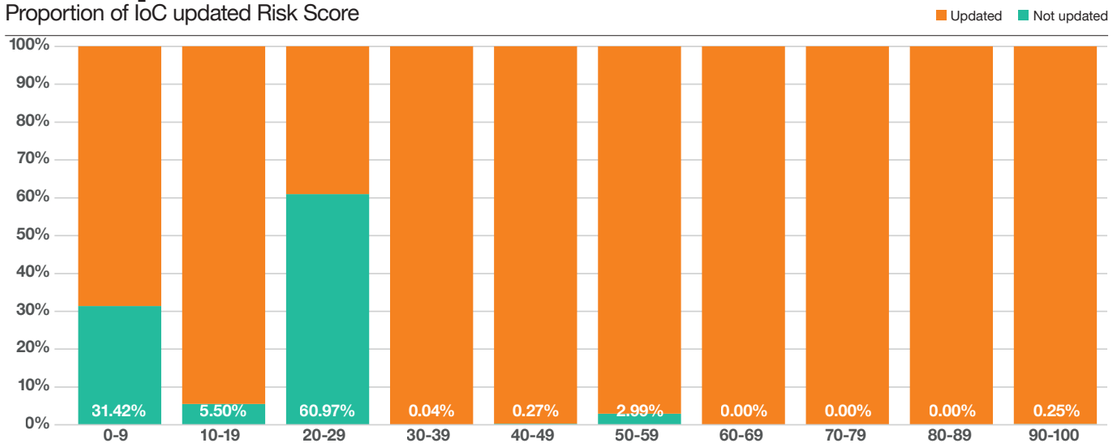
One in three of all IoC are updated a day or more after being ingested into the platform.

Perhaps unsurprisingly given our observations above, most IoC that are updated end up with a Risk Score under 20. The only other Risk Score common with updated IoC is between 50 and 60. ~3% of IoC that were updated ended up with a Risk Score in this range.

The average lag between an IoC first being seen, and last being updated, is 17 days.

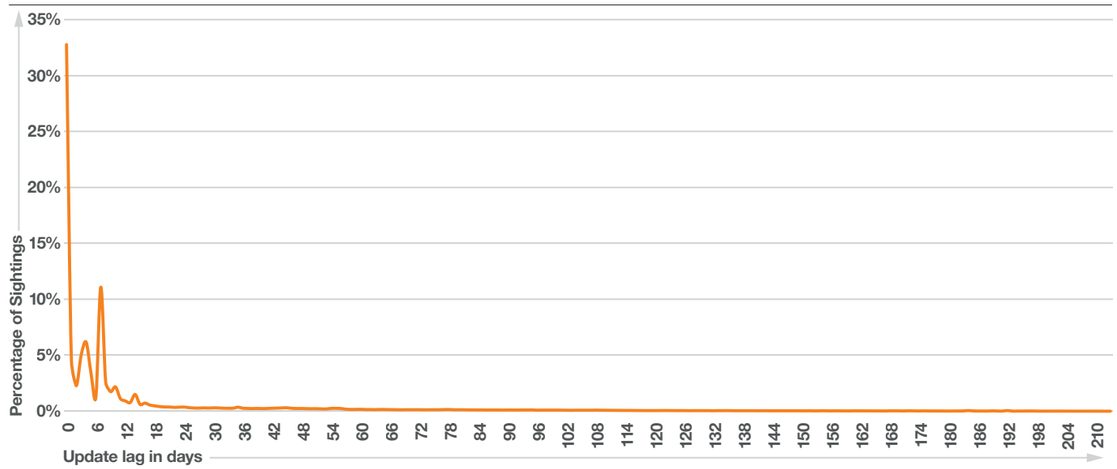
IoC Updates and Risk Score

Proportion of IoC updated Risk Score



Update Lag

Distribution across Update Lag Time in days



The chart above visualizes how the maximum update 'lag' is distributed across all the IoC in this dataset. Almost a third (33%) are updated on the same day, while 84% aren't updated again after 30 days. Only 5% of IoC in the dataset are updated after 90 days.

In the world of the blind

The truly meaningful question to ask about CTI is of course whether it ever produces any results. Are the IoC we collect and distribute from the Datalake ever actually observed in 'action' by our clients or security operations? Like good advice, good CTI is not necessarily heeded. Since we don't always know if, when, or how the CTI we distribute is put to use, this can be a very difficult question to answer objectively.

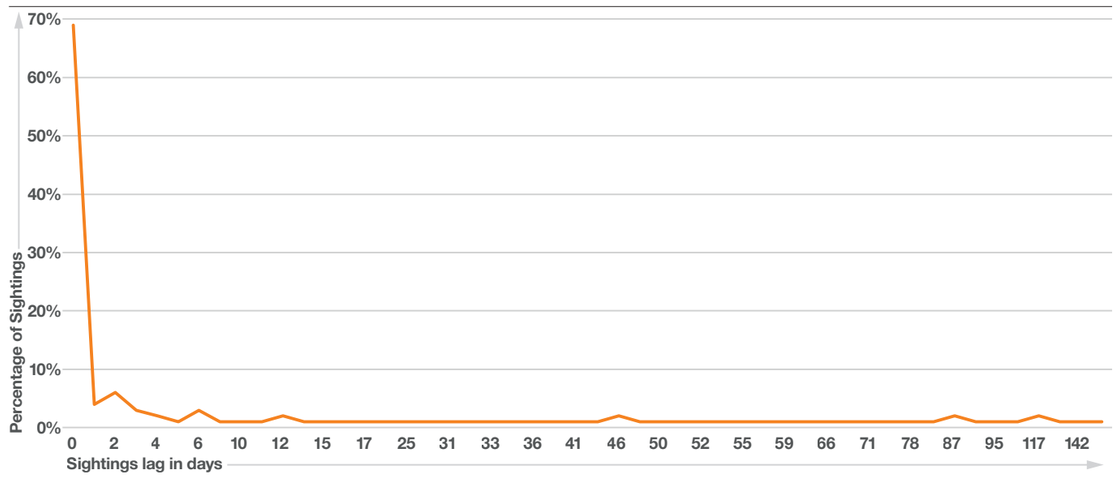
Nevertheless, for our own Cyber Security Services we do have feedback mechanisms in place that records when and where IoC are discovered by our operations in the wild. We call this a 'Positive Sighting'.

Less than 1% of the IoC in this dataset were updated with a confirmed 'Positive Sighting'. However, whether or not that information is fed back to our Datalake, and how much additional information accompanies that feedback, is an operational question. So we can't glean much insight into the effectiveness of the CTI itself. We focus therefore on the 1% of IoC that were positively identified in the wild and reported to the Datalake.

First we examine how the 'lag' between the IoC being recorded in the Datalake and being observed in the wild. This distribution is illustrated below:

Sightings Lag

Positive Sightings Time Lag - distribution in days



We note that 51% of all the confirmed Positive Sightings are not recorded in the wild after the 1st day. The average time between recording the IoC in the Datalake and a confirmed Positive Sighting in the wild is ~ 20 days. Two thirds (67%) of all IoC are not reported in the wild after ~10 days.

If we consider Sightings that were reported but not 'confirmed' as Positive (we call these 'Neutral Sightings'), the sample 'grows' to 2.15% of this dataset. The 'oldest' Sighting also increases slightly from 155 to 202 days, the average time to sight an IoC grows to 31 days, and we note that 67% of IoC are sighted within the first 10 days before 'disappearing'.

The Mean Risk score across all types is 14 for IoC with confirmed Positive Sightings, compared to just 5 for 'Neutral' Sightings. 40% of Positive Sightings have a Risk Score between 20 and 30. Interestingly, there is a small spike in IoC with a 'perfect' Risk Score of 100 within the Positive Sightings – almost 2% - compared to 0.6% for Neutral Sightings.

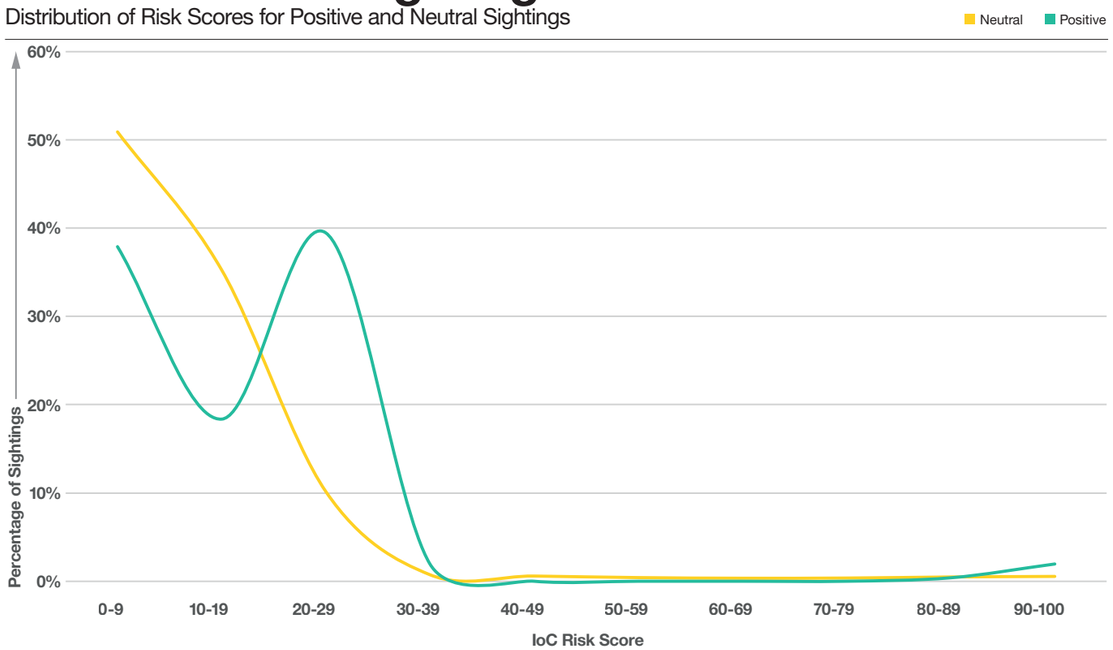
We therefore see some evidence that a higher Risk Score correlates with a higher probably of Sighting in the wild, but a more extensive analysis would be required to confirm this.

Risk Scores for IoC Sighted in Operations

Sighting	Min Score	Average Score	Max Score	Median Score
None	0	14,51	100	
Neutral	0	9,47	100	5
Positive	0	15,95	100	14

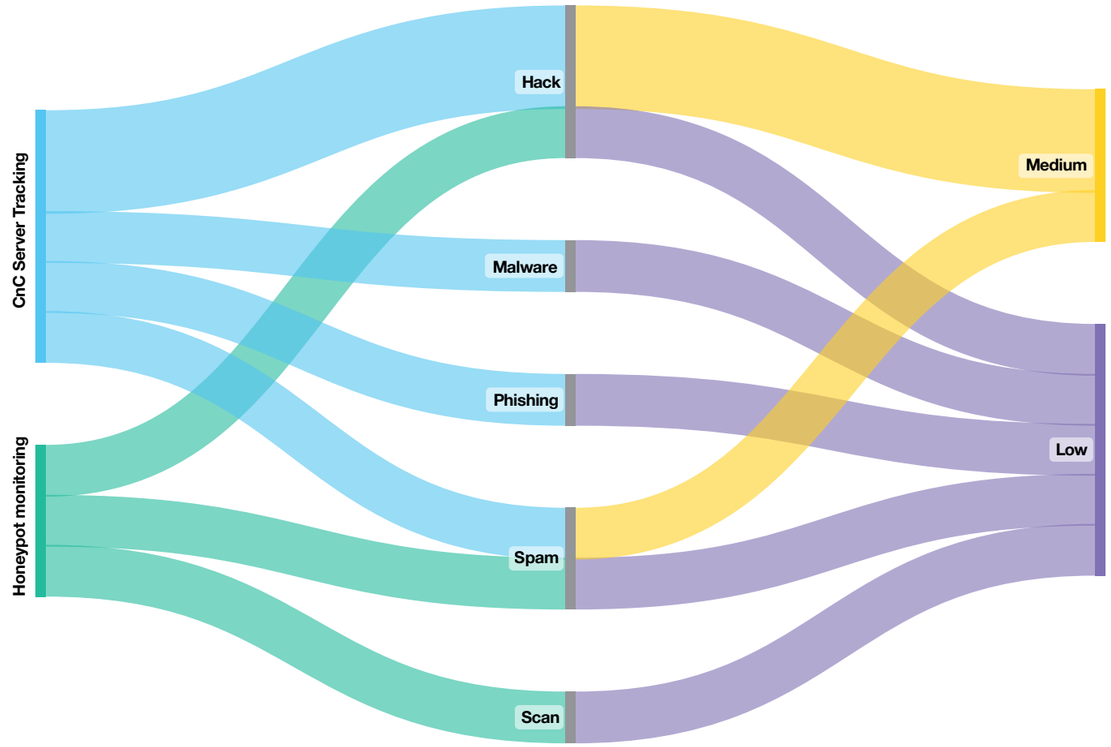
Risk scores of Sightings

Distribution of Risk Scores for Positive and Neutral Sightings



Sightings Flow

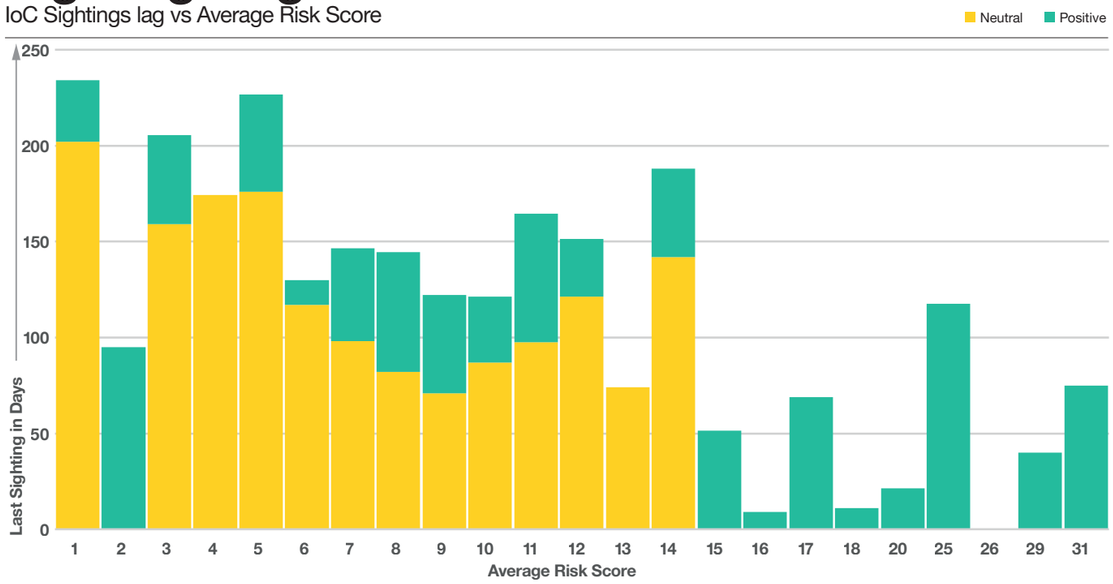
Confirmed Sightings for two Orange Cyberdefense internal data sources



The relationship between Sources and Risk Scores for confirmed positive Sightings is shown above, limited to two internal IoC data sources that were sighted. The flow visualizes the data source, the Threat Type and Risk Score for that Threat Type for each IoC in a confirmed Positive Sighting:

Sightings lag and Risk Score

IoC Sightings lag vs Average Risk Score



The average Risk Score assigned across all IoC is 14.39.

Although this dataset is arguably too small to draw definitive conclusions from, we note with interest that as the Risk Score increases (shown on the X-axis from 1 to 31), the Sightings lag (shown in days on the Y-axis) appears to decrease. Bearing in mind that this refers to the last sighting, it would seem to suggest that the more highly rated the IoC (the ones we have more confidence in) persist in the wild for a shorter time. This may in turn suggest that this high-confidence is indeed more accurate, but that the attacker infrastructure being identified is being recycled quickly.

IoC with a Risk Score above 20 were never Sighted after more than ~100 days had lapsed.

A tale of curvy distributions

This humble analysis of our CTI data surfaces several inconclusive findings: The volume of data in play is overwhelming, and that's just from a researcher's perspective. Defenders have to deal with a plethora of data sets that differ but also overlap significantly.

A dynamic Risk Score provides clients with a means to prioritize indicators, but on a scale of 1-100, the average Risk Score assigned is only 14.39. Furthermore, 98% of IoC have a risk score of 20 or less and only 0.12% of IoC have a Risk Score of 100.

It's very hard to select the best CTI 'Sources' also: 50% of all IoC in our Datalake are contributed by just 5 CTI data sources. The most prolific source alone contributes 16%. But there's a 'long tail' of contributors that starts at the 20th data source. From here on each data source contributes less than 1% of all the IoC. How many data sources are enough?

Like so many things in security, the 'effectiveness' of IoC is also a large blind spot: Since CTI tends to flow in one direction, it's hard to know what CTI is effective, and how long it remains effective.

From the limited insight we have, we assess that the average time between recording the IoC in the Datalake and a confirmed Positive Sighting in the wild is ~ 20 days. However, the majority of IoC that we do observe are not seen again after 5 days, and really 2 days seems to be the expiry time for most CTI. So any process that consumes CTI needs to be highly agile.

The challenge for defenders is therefore to determine how much CTI they need, and what CTI matters.

Wherever we examine any attribute that might help inform that question, we see the same dramatic 'reverse L' distribution emerging. The bulk of IoC tend to share the same attributes (source, Risk Score, Updates, etc), but that is always followed by a 'long tail' of IoC that have diverse attributes. This pattern is so consistent across the distributions we visualize in the study above that the charts can be hard to tell apart!

This kind of distribution beautifully captures the 'intelligence dilemma' we discuss above, which is classic 'Pareto Principle'[58]: The majority of the apparent value we get from CTI is highly concentrated in a few sources, with an average Risk Score and will persist for around 2 days. At the same time, however, there is a lot of value distributed across other sources, with diverse Risk Scores. Ignoring those indicators means taking the risk of missing crucial intelligence, though the probabilities become even lower. We need both 'depth' and 'breadth' in the CTI we consider. At the same time, even that is not *all* the intelligence there is, so one is inclined to add even more data. But IoC are duplicated across multiple sources, so the relative ROI decreases even more, although the security value is still there.

A few key elements ensure positive security outcomes from CTI:

1. The correct balance between quality and quantity of data;
2. Data context to facilitate effective triage;
3. Minimum 'friction' to reduce the cost of applying and acting on CTI;
4. Feedback loops that allows one to assess the relative value of sources and indicators;
5. Data transparency that facilitates informed decision making by security buyers.

We hope that the data provided in this report sheds some light on the intelligence dilemma and contributes in some small way to the effective procurement and application of CTI by defenders.

Region Scorecard

Europe Region

Cy-X region ranking

Europe, including UK, had the second highest number of Cy-X victims

23% in our victim data

Cy-X victim delta

In this region we saw an increase in the number of victim organizations of

+ 16%

Most affected country

On its own UK was in second place when it came to victim numbers, with 206 organizations having entries posted on leak sites, around

6% of all victims and a 52% increase from last year.

Hacktivism Ranking

- As a region Europe, including the Nordics, dominates the chart for number of Hacktivism incidents, with 3,404 out of a total of 4,016 recorded attacks.
- The top 5 victim countries are all European, and not surprisingly Ukraine takes pole position by some way with 639 documented attacks.
- The remainder of the top 5 consists of Poland(433), Sweden(338), Lithuania(220) & Germany(219).
- Over 60% of the attacks against Ukraine were by a group known as "CyberArmyRussia". The remaining top 5 countries were primarily targeted by the group "NoName057(16)", with the exception of Sweden who attracted the attention of "Anonymous Sudan".

CyberSOC Ranking

- The top 5 countries when it came to confirmed incidents in our CyberSOCs are all European. Incidents from clients in Sweden(36%) & France(35%) made up the vast majority of true positives, whilst the UK made up the top 3 with 9%.
- The picture changes slightly when we consider false positive incidents instead. Sweden is still top of the pile with 29%, however the UK is now second with 28% and Germany completes the top 3 with 15%.
- When we consider how countries compare with their relative levels of coverage taken into account, we see that the top 5 for confirmed incidents are again all countries in Europe, this time however there has been a significant shift.
- If we now look at false positive incidents the top 2 countries remain the same, however the proportions are slightly closer with France having 60% and Sweden now with 13% of recorded false positives. The UK is now not too far behind Sweden representing 12%, Belgium & Denmark make up the rest of the top 5 again, this time with 6% & 5% respectively.

Region Scorecard

Nordics Region

Cy-X region ranking

Proportionally the Nordics rank

10th in our victim data

Cy-X victim delta

The Number of victims increased from last year. We saw a rise of

+ 21%

Most affected country

Sweden was targeted most heavily with 25 victims recorded:

53% of all Nordic victims.

Hacktivism Ranking

- Sweden was the third most impacted country with 338 attacks, which was followed by Denmark with rank 11, translating into 127 attacks.
- Most of the Nordic countries were impacted by the two groups, namely "NoName057(16)" and "Anonymous Sudan".

Region Scorecard

Africa & Middle East Region

Cy-X region ranking

A total of 142 victims in this region put it in 4th place.

142 victims

Cy-X victim delta

On what we reported in last year's Navigator we saw an increase of

+ 42%

Most affected country

The most victims in this region were from South Africa where we saw 23 organizations, which represents

0.67% of all victims, listed on leak sites.

Hacktivism Ranking

- Israel was the primary focus of attacks in the Africa and Middle East region. They were the target for

102 attacks all initiated by "Anonymous Sudan".

OT Ranking

- Israel, Iran & South Africa were joint tenth in the list with each having

2.5% of reported global OT attacks.

Region Scorecard

South Asia Region

Cy-X region ranking

A total of 71 victims in this region put it in 8th place.

71 victims

Cy-X victim delta

Despite the low number of victims South Asia witnessed an increase of

+ 115%

Most affected country

India is the primary reason for the overall increase in South Asian victims. Indian organizations went from 31 being targeted to 61, a

97% year on year increase.

Region Scorecard

South-East Asia

Cy-X region ranking

A total of 110 victims in this region put it in 5th place.

142 victims

Cy-X victim delta

From the perspective of a percentage increase on last year, South-East Asia was 4th highest with an increase in victim numbers of

+ 67%

Most affected country

Thailand has the dubious honor of top spot in this region with 36 victims, around 1% of all victims globally or almost

33% of the total for this region.

Region Scorecard

East Asia Region

Cy-X region ranking

This region comes in at 6th place with 100 victims this year.

100 victims

Cy-X victim delta

Whilst all other regions were hit with double digit percentage increases, East Asia only experienced a increase of

+ 3%

Most affected country

The cause of the low increase in the region is explained by China, which actually saw a drop from 32 last year to 21, which is a

decrease in recorded victims by -34%

CyberSOC Ranking

This year we saw slightly under 3% of our confirmed incidents originate from clients in China.

Region Scorecard

North America Region (US & CA)

Cy-X region ranking

Highest number of recorded Cy-X victims with 1,845 reported in the past 12 months.

53.5% of the victims

Cy-X victim delta

Since last year's Security Navigator we saw the number of victims grow at

+ 65%

Most affected country

The US was by far the most targeted, both in their region and globally, with 1,683 victims listed

53% of all victims were headquartered in the United States.

Hacktivism Ranking

- Considering the proportion of Cy-X attacks seen in North America the number of recorded Hacktivism incidents is relatively low.
- "Anonymous Sudan" & "KillNet" were the primary perpetrators when it came to the US, whereas Canada only saw attacks originating from "NoName057(16)".

There were 201 targeting the US whilst Canada saw 96.

OT Ranking

- North American companies made up almost a third of all reported attacks on OT.
- With just short of a quarter of the reported attacks on OT it is no surprise that the US tops the rankings of targeted countries globally.
- Canada, while not as prominent as the US, also featured in the top 5 list of targeted countries with almost 8% of all attacks.

Region Scorecard

Latin America Region

Cy-X region ranking

Latin America had the third highest victim count with 205, almost 6% of the total number of victims.

205 victims

Cy-X victim delta

This region saw a fairly significant increase in comparison to what we saw last year

+ 56%

Most affected country

Brazil accounted for most of the Latin American victims with 74, putting it in 8th place of all victims globally.

Brazil accounted for 36% of Latin American victims

Industry Scorecard

Manufacturing

Cy-X industry ranking

Manufacturing was again on the top spot in terms of targeted industries with

20% of all known attacks

and over 17% more than the second placed industry Professional, Scientific, and Technical Services.

Cy-X victim delta

Compared to last year, Manufacturing had 200+ more victims, a year-on-year increase of

+ 42%

Most affected sub industry

As a sub-industry, Machinery Manufacturing had the highest proportion of attacks

with 15%

In joint second Chemical & Fabricated Metal Product Manufacturing both had a 12% share of attacks.

CyberSOC Industry Ranking

- No surprise to once again see Manufacturing top the table for most total incidents. Almost **38,000 incidents** came from customers in this sector, with **over 8,100 confirmed as True Positive incidents.**
- Between them the Hacking & Misuse threat actions made up over 50% of True Positive incidents for our Manufacturing industry clients.
- Internal threat actors accounted for more than half of the Manufacturing True Positive incidents. This ties in with the high proportion of incidents categorized as Misuse.

VOC Industry Ranking

- Manufacturing placed third in terms of **lowest average vulnerability score**.
- On average we saw **15.13 findings per asset**.
- That is **53% less findings per asset** than the industry average.
- The average vulnerability in Manufacturing lives for approximately **3 months** on average.
- Manufacturing has vulnerabilities as old as **4 years** or 1457 days.
- The average age per finding for Manufacturing is **1.19 times higher than the industry average**.
- This industry has a vulnerability score that is **19% lower than the average**.
- Manufacturing averages **4 Critical rated findings per asset, 25.3 rated High, rated 6.6 Medium and 1.9 rated Low**.

Pentesting Industry Ranking

NOTE we do not have enough data for a meaningful analysis.

- our testers saw an average of **5 findings per assessment**.
- Manufacturing sees **35% fewer findings than the average** for a pentest.
- The **average CVSS score per finding was 4.22**.
- Manufacturing pentest projects report **3 risks rated Low on average**.
- Manufacturing pentest projects report **2 risks rated Medium on average**.

Industry Scorecard

Professional, Scientific, and Technical Services

Cy-X industry ranking

Professional, Scientific, and Technical Services were second overall by a considerable margin, with

17% of victims

falling under this banner.

Cy-X victim delta

Professional, Scientific, and Technical Services remained in second place this year but saw an increase in victims of

+ 52%

Most affected sub industry

This sector is a very diverse one, while we see Computer System Design related organizations (17%) being impacted the most, followed by Architecture and Engineering (17%); we find it interesting that we see Offices of Lawyers with 14% (highlight in big and orange) and at the 10% f the victims stem from the overall Legal Services sub-sector. Highlighting that the Legal Service industry has been mostly impacted.

CyberSOC Industry Ranking

- The fourth highest volume of total incidents came from the Professional, Scientific, and Technical Services industry, with 16,425 incidents being recorded. Almost 2,500 of these incidents required investigating by our analysts as True Positive incidents.
- Hacking (35%) & Malware (17%) made up more than half of Professional, Scientific, and Technical Services incidents.
- When it came to threat actor, both External (45%) and Internal (43%) actors were very close proportionally.

Pentesting Industry Ranking

- Professional, Scientific, and Technical Services has an average of 5.11 findings per pentest.
- We see 34% fewer findings than the average.
- The average CVSS score per finding is 4.73.
- Pentesting reports 2 risks rated Critical on average.
- On average 1.4 risks were rated High.
- 2.44 risks were rated Low on average.
- 4 risks were rated Medium on average.

VOC Industry Ranking

- We saw 7.06 findings per asset on average
- Professional, Scientific, and Technical Services has 78% less findings per asset than the industry average.
- The average vulnerability lives for 7 months.
- Some vulnerabilities are older than 3.5 years.
- The average age per finding is 1.58 times higher than the industry average.
- Professional, Scientific, and Technical Services has a vulnerability score that is 68% lower than the average.
- On average we see 3 Critical rated findings per asset, 7.5 were rated High, 5.2 Medium and 3.6 rated Low.

Industry Scorecard

Health Care and Social Assistance

Cy-X Industry ranking

Health Care and Social Assistance is in 6th place this year with

5% of all victims

Cy-X victim delta

Compared to last year, resulting in the move up from 7th place to 6th, we see an increase in

+ 61%

Most affected sub industry

Unfortunately Hospitals made up most of all victims in the Health Care and Social Assistance industry with

20% of all victims.

CyberSOC Industry Ranking

- With 6,000 total incidents, Health Care and Social Assistance were 5th highest, 16 % of those incidents were identified as being True Positive.
- Hacking was by far the biggest threat action reported, with 65% of all True Positive incidents.
- Three quarters of the threat actors for Health Care and Social Care incidents were classified as External.

VOC Industry Ranking

NOTE: we do not have enough data for a meaningful analysis.

- Health Care averages 19 findings per asset.
- We see the lowest maximum finding age of less than 1 year.
- Health Care beats the industry vulnerability score average by 47%.
- We note the third highest average finding age of 244.04 days, that is 2.12 times higher than the average.
- We recorded zero findings per asset rated Critical.
- 1 finding per asset was rated High, 14.5 findings per asset were rated Medium and 30.2 Low.

Pentesting Industry Ranking

- Health Care has an average of 4.86 findings per pentest.
- We see 38% fewer findings than the average pentest
- The average CVSS score per finding is 4.64.
- Pentest projects on average report 1 risks rated Critical on average, 2 risks rated High, 2.33 risks rated Medium and 2.83 risks rated Low.

Industry Scorecard

Educational Services

Cy-X Industry ranking

The fourth highest attacked industry is Educational Services, representing

6% of victims

Cy-X victim delta

This industry climbed from 8th to 4th most affected, representing a growth of

+ 115%

Most affected sub industry

Three quarters of all Educational Services victims are made up of institutions from

Colleges, Universities and Professional Schools combined with Elementary and Secondary Schools.

VOC Industry Ranking

NOTE: we do not have enough data for a meaningful analysis

- Educational Services averages 1.94 findings per asset.
- The maximum finding age is more than 2.5 years.
- We see an average finding age of almost 5 months.
- The finding age is 1.2 times higher than average.
- 3 findings per asset were rated Critical, 2.2 were rated High, 1.2 were rated Medium and 1.1 were rated Low.

Industry Scorecard

Finance and Insurance

Cy-X industry ranking

At around 64% less than top placed Manufacturing we find this industry with

7% of all known victims

Cy-X victim delta

Compared to last year Finance has moved up to the third place in with an increase of

+ 106%

Most affected sub industry

Within Finance & Insurance, 3 subsectors dominated.

Credit Intermediation made up 38%, interestingly Insurance Carriers had 32% with Securities, Commodity Contracts and Other Financial Investments completing the top 3 with 24%.

CyberSOC Industry Ranking

- Finance and Insurance ranked second for total number of incidents, although the total was less than half that of Manufacturing, and only around 12% of those incidents were confirmed as True Positive.
- The Hacking (49%) Threat Action made up the majority of the True Positive incidents. A fairly distant second came Malware with 22%.
- External threat actors were identified for 65% of the True Positive incidents.

VOC Industry Ranking

- Finance and Insurance averages 43.3 findings per asset.
- That is 1.36 times more findings per asset than the industry average.
- We see the youngest average age of 54.3 days per finding.
- The oldest findings as old as 4 years.
- The average age per finding is 2.31 times lower than industry average.
- The vulnerability score is 1.4 time higher than the average.
- 9.5 findings per asset were rated Critical, 31 were rated High, 15.2 Mediumand 5 .2 rated Low.

Pentesting Industry Ranking

- Finance and Insurance has an average of 6.44 findings per pentest.
- We see 16% fewer findings than in the average pentest.
- The average CVSS score per finding was 5.13.
- 1.38 risks were rated Critical on average, 2.25 risks rated High on average, 3.92 risks were rated Medium and 2.55 were rated Low.

Industry Scorecard

Public Administration

Cy-X industry ranking

Public Administration featured in 12th place of Cy-X victims we recorded with just

3% of the total

Cy-X victim delta

As a proportion, Public Administration victims dropped from 10th to 12th place this year, despite seeing 18 victims more, an increase of

+ 22%

Most affected sub industry

Victims in the Executive, Legislative and Other General Government Support sector are top of the pile in the Public Administration with 58% of victims part of this sector. Perhaps worryingly,

almost 8% of victims aligned with the National Security and International Affairs subsector.

CyberSOC Industry Ranking

- We recorded less than 5,000 incidents for clients in the Public Administration space, with less than a third of these being confirmed as True Positive.
- Hacking, Malware & Misuse were all quite close as threat actions for the True Positive incidents, with 19%, 16% & 16% respectively.
- In line with the threat actions, threat actors were also equally dispersed, showing External with 39% and Internal 37%.

VOC Industry Ranking

- This industry averages 35.3 findings per asset.
- Public Administration beats industry vulnerability score average by 14%.
- We see an average age per finding of almost 6 months.
- The average finding age is 1.46 times higher than the average.
- The max unique finding age peaks at 1420 days.
- We see 5.2 findings per asset rated Critical, 15.2 findings rated High, 17.4 findings rated Medium and 3.8 rated Low.

Pentesting Industry Ranking

- Public Administration has an average of 5.56 findings per pentest.
- We see 28% fewer findings than in the average pentest.
- The average CVSS score per finding is 5.10.
- Public Administration pentest projects report 2.5 risks rated Critical on average, 2.33 rated High, 3.42 rated Medium and 1.9 risks rated Low.

Industry Scorecard

Construction

Cy-X industry ranking

This year Construction came in at 7th place with

5% of the victims

Cy-X victim delta

As a proportion of all victims construction fell from 4th place to 7th, but still had a growth in victims of

+ 33%

VOC Industry Ranking

- Construction averages 12.12 findings per asset.
- This industry beats the vulnerability score average by more than 70%.
- The average vulnerability age for Construction is almost 4 months.
- The average finding age for Construction is 3% lower than the average.
- Construction has unpatched vulnerabilities as old as 1.5 years.
- We see 3 Critical findings, 7.5 High findings, 5.2 Medium findings and 3.6 Low findings per asset.

Pentesting Industry Ranking

NOTE: we do not have enough data for a meaningful analysis.

- Construction has an average of 9 findings per pentest.
- The report lists 1.16 times more findings than the average pentest report.
- The test revealed an average CVSS score per finding of 4.6.
- 4 risks were rated High and 5 risks were rated Medium.

Industry Scorecard

Retail

Cy-X industry ranking

The Retail vertical saw significantly fewer victims than our top 2 industries, so we see them in the 9th place. It represents

4% of the victims

Cy-X victim delta

Interstingly this is the only vertical in which we observed a drop in the number of victims by 139, which is

- 20%

CyberSOC Industry Ranking

- With over 17,000 total incidents recorded, the Retail sector was third highest. However looking at confirmed True Positive incidents they came in second behind Manufacturing with 5,376.
- Hacking and Misuse threat actions combined made up almost a third of True Positive incidents.

Pentesting Industry Ranking

NOTE: we do not have enough data for a meaningful analysis.

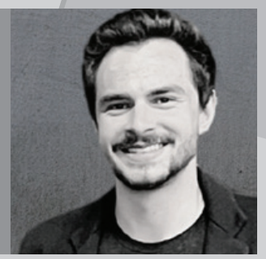
- We saw an average of 10 findings in the pentests.
- The reports list 1.29 times more findings than the industry average.
- Retail has an average CVSS score per finding of 5.79.
- We see on average 2.5 risks rated High on average, 12 risks rated Medium and 3 risks rated Low.

Hacking the Human Mind

Exploiting Vulnerabilities in the 'First Line of Cyber Defense'

Humans are a complex beings with consciousness, emotions, and the capacity to act based on thoughts. In the ever-evolving realm of cybersecurity, humans consistently remain primary targets for attackers. Over the years, these attackers have developed their expertise in exploiting various human qualities, sharpening their skills to manipulate biases and emotional triggers with the objective of influencing human behaviour to compromise security whether it be personal and organizational security.

Ulrich Swart, Training Manager & Technical Team Leader, **Orange Cyberdefense**



More than just a 'human factor'

Understanding what defines our humanity, recognizing how our qualities can be perceived as vulnerabilities, and comprehending how our minds can be targeted provide the foundation for identifying and responding when we inevitably become the target.

The human mind is a complex landscape that evolved over years of exposure to the natural environment, interactions with others, and lessons drawn from past experiences.

As humans, our minds set us apart, marked by a multitude of traits and emotions, often too complicated to articulate precisely.

Human behaviour is complex

Some of our fundamental traits can be outlined as follows:

- **Trust** – Humans place their trust in others, assuming inherent goodness.
- **Empathy** – Humans exhibit care for others and their feelings.
- **Ego** – Humans harbour a competitive spirit, aspiring to outshine their peers.
- **Guilt** – Humans experience remorse for their actions, especially when they harm others.
- **Greed** – Humans desire possessions and may succumb to impulsivity.
- **Urgency** – Humans respond promptly to situations demanding immediate attention.
- **Vulnerability** – Humans often grapple with fear and are candid about their emotions.

While this list is not exhaustive, it summarises common and understandable aspects that drive human behaviour. Human interactions hold essential value, instilling life with significance and advancing cultural norms. However, for attackers seeking to exploit us, the social construct of human-to-human interactions provides a pathway for manipulation.

Our naturally social nature forces us to revert to these traits. Emotions serve as a safety net for communication, problem-solving, and connections in our everyday life and we have come to trust our emotional responses to further guide and protect us in a variety of situations.

I think, therefore I can be manipulated

Attackers exploit this safety net (emotions and fundamental traits) when targeting humans, as it can be manipulated to fulfil their objectives. This safety net weakens even more when we venture into the "online" realm, as certain safeguards fail due to a lack of insight. The abstraction of communication through a name on screen often misleads our minds in interpreting situations in a way that our emotions cannot accurately navigate.

In the realm of manipulation, various models and methods have been employed over centuries to influence human behaviour. In today's context, attackers exploit these models to identify human vulnerabilities, characterised as weaknesses within the system that can be exploited.

In addition to directly manipulating fundamental traits through carefully targeted attacks, attackers tend to target humans through forms of influence and persuasion. These can be summarised as follows, and humans tend to operate mentally in these realms:

- **Reciprocation** – Humans feel compelled to reciprocate what they have received.
- **Authority** – Humans are inclined to comply with authoritative/known figures.
- **Scarcity** – Humans desire items that are less attainable.
- **Commitment & Consistency** – Humans favor routine and structure.
- **Liking** – Humans form emotional connections.
- **Social Proof** – Humans seek validation and fame.

These aspects can be viewed as potential vulnerabilities in the human mind when combined with emotions and fundamental traits. Attackers leverage these aspects to gain direct control over our actions, an occurrence now recognised as social engineering.

Social engineering encompasses various techniques and tactics, yet at its core, it exploits one or more of the areas mentioned above through accurately crafted interactions.

Formula for attack

To describe the modus operandi for attackers targeting humans, we can formulate simple formulas. A standard attacker formula will be as follows:

(Target) + (Vulnerability) + (Exploit) = Compromise

But when applied to the human it could be as follows:

(Human Mind) + (Emotional Trigger/Trait) + (Social Engineering Technique) = Intended Objective through Resultant Reaction

The attack chain is apparent by looking at how these formulas relate to triggers and techniques in combination with vulnerabilities.

Cognitive Influence	Emotional Triggers	Exploitation Techniques	Example
Reciprocation	Trust, Empathy & Guilt	Using goodwill or asking for help	Link to download a donation form to help humanitarian aid or asking for money back after a fake payment was made in excess.
Authority	Trust & Urgency	Using legitimate context or form of power	Email made to look as if it is from Microsoft indicating your account is compromised and you should act.
Scarcity	Greed & Urgency	Using an irresistible offer	Limited offer to win a house if you pay £50 now or clicking a link.
Commitment & Consistency	Vulnerability & Ego	Using an improvement or advantage	Call about wanting to improve asking for information about work and personal life which can be sensitive.
Liking	Trust & Vulnerability	Using causes or loved ones	Impersonating a friend to ask you to open a file or do something you'll only do for close connections.
Social Proof	Ego & Guilt	Using status or threats	Threatens to expose something about you or offer to get you mentioned somewhere important.

Exploitation techniques, often seen in digital channels like email, phone calls, or text messages, are frequently used for phishing. These tactics manipulate established interactions to achieve various objectives, such as deceiving individuals into parting with funds, opening malicious files, submitting credentials, or revealing sensitive data. The consequences of these attacks can vary from individual losses to organizational breaches.

Defending ourselves

To safeguard against these attacks against our minds, we should align our cognitive standards with emotional triggers by asking questions like; what is the purpose, expectation, and legitimacy of the interaction. These questions could prevent impulsive reactions and allow introspection.

Establishing a "stop and assess" mentality acts as a mental firewall, strengthened by vigilance, to enhance personal and organizational security. By considering potential attacks, we heighten our awareness of vulnerabilities and work on resilience. This awareness, coupled with a proactive approach, helps mitigate threats to our minds and humanity, promoting collaboration to disarm attackers and weaken their operations.

Stay vigilant, stay informed, and continue to question everything.

Diana Selck-Paulsson
Lead Security Researcher
Orange Cyberdefense

Data analysis:

Why aren’t we more effective in defending against Cyber Extortion?

An alarming surge in Cyber Extortion in Q1 2023 led us to believe that there was reason enough to dedicate a paper to this problem – looking beyond the typical, technical aspect of "Ransomware”, to understand the true nature of this crime – so we produced our detailed Cy-Xplorer report.

Now, half a year has passed. So what has happened since then? Let's once again take a look at the crime scenes, victims and round up the usual suspects.

Cyber Extortion has surged to unseen levels, despite efforts made to disrupt this form of cybercrime. The question arises: what do current efforts to disrupt this ecosystem look like? We will focus mostly on actions taken by government and law enforcement agencies, however it should also be noted that other entities are also responding to the current threat. Therefore, we'll explore all of the responses we have seen in the past 12 months and investigate whether or not they have been successful or have the potential to disrupt the ecosystem in the near future.

Law enforcement efforts

We've been tracking Law Enforcement (LE) activities for a while now to determine whether the actions they've taken have any disruptive impact on the cybercrime ecosystem. We see increased activity by governments, local authorities, and international collaborations with the goal of fighting some of the types of cybercrime we have been witnessing in the past two and a half years. Our observations are based on news articles reporting on the counter measures taken against various forms of cybercrime and criminal actors. We are not aware of any comprehensive and open access list of activities, so we started our own dataset this year by looking at two and a half years of news coverage on LE activities and government collaborations.

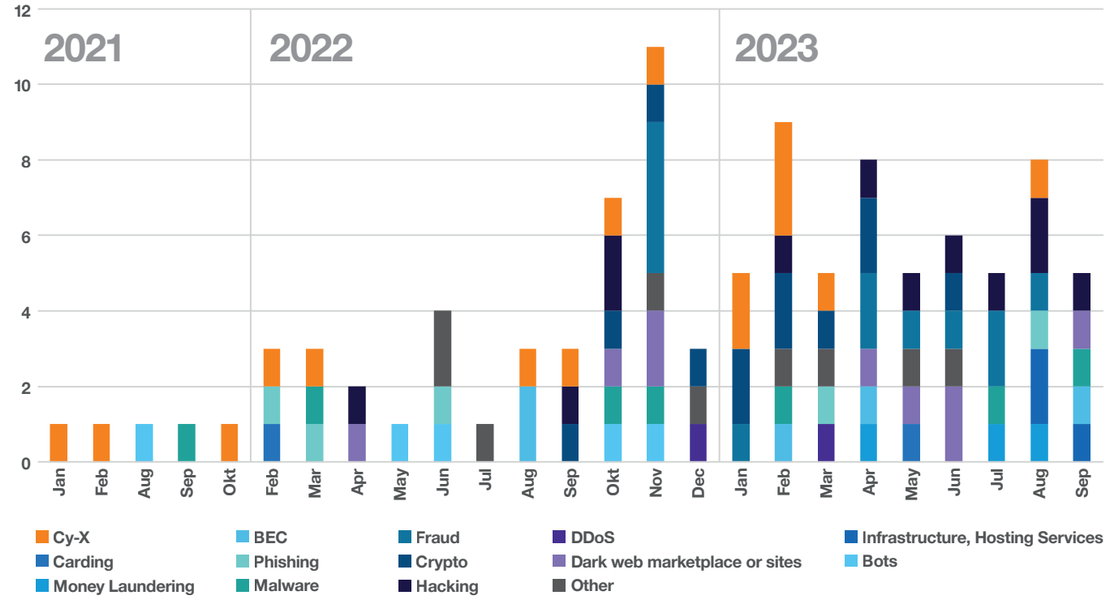
In the last two and a half years we've seen a steady increase in LE activity. We recorded 102 actions that we have been connecting to counter cybercrime in some way. We documented the type of crime, which the action was taken against (e.g. Fraud, Crypto, Cy-X) and what actions the LE operation took to achieve its goal (arrest, takedown, an individual was extradited, etc.). As can be seen below, LE activity increased noticeably by Q4 2022 and there has been a steady increase in efforts to combat cybercrime ever since.

We see Cyber Extortion as the number one crime type being fought against with 15% of all LE actions in our humble dataset. Cy-X is closely followed by Hacking and Crypto which each claimed a share of 12%, and Fraud with 11%; and 9% of all LE activity we recorded had to do with dark web or clear web sites or marketplaces. In 2023, we specifically noted increased efforts to take down or disrupt the infrastructure and hosting services Threat Actors (mis-)used.

A more telling metric is perhaps what actions were taken against those forms of crime we mentioned above. Here, we recorded that almost 60% of LE activities were announcements of arrests and the sentencing of individuals or groups. This is a positive observation because prosecution potentially has a deterrent effect on other Threat Actors, especially very young (potential) offenders.

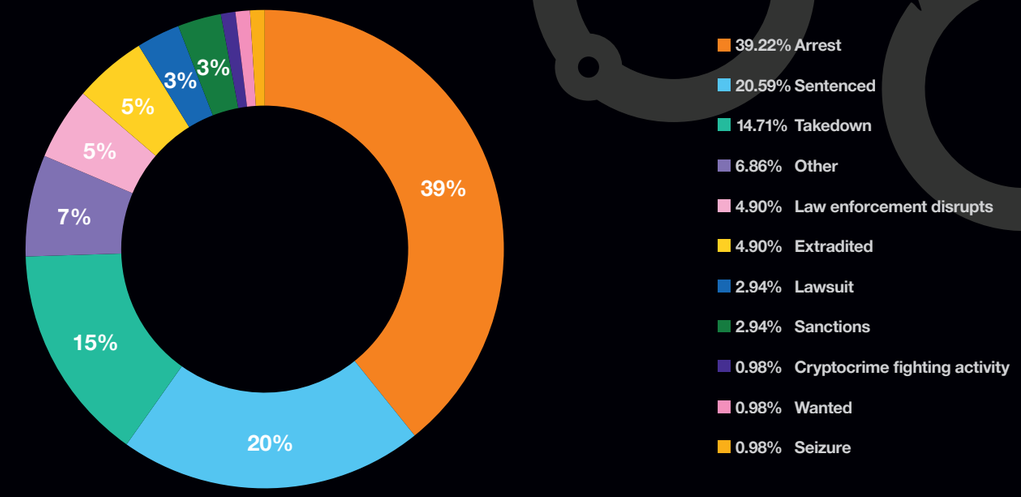
Focus of Law Enforcement

Types of cyber crime Law Enforcement activities targeted in recent years



Types of defense activities

Proportion of different types of Law Enforcement activities observed



The third most common LE action in our dataset is takedowns (15%). These actions targeted dark web marketplaces and sites, Cryptocurrency tumblers, and botnets such as Qakbot[59], which was dismantled in 2023. The Qakbot takedown was a significant milestone in the potential of LE agencies' evolving capabilities.

Besides 'traditional' LE activity, we also observed increased government activities focusing on disruption. This became especially evident after the takedown of the threat actor group 'Hive' in January 2023, which was a result of a collaborative effort by EUROPOL, the German, Dutch and U.S. authorities[60] and others. Hive was something different, here we saw authorities, namely the FBI, infiltrating Hive's network and remaining undetected for a significant period of time. This 'hacking back' operation included the capture of decryption keys and helping over 300 victims to decrypt their data whilst still under attack by Hive, in addition to seizing control of the servers and websites that Hive used to communicate. The subsequent announcement by the U.S . Department of Justice (DOJ) emphasized prioritizing disruption and seizures over other, longer-lasting investigations[61].

This disruptive activity has shown some impact. For instance, they took down the Hive operations and helped hundreds, if not thousands of victims afterwards by providing the decryption keys. They also most likely learned a lot of the group's Tactics, Techniques and Procedures (TTP), given the fact that they had been in their network for several months before taking them down in January 2023. However, no arrests were made. While this particular law enforcement action was unique and significant; if the individuals who ran this Cyber Extortion operation are still on the loose, chances are that they have re-grouped and potentially begun operating under a new name. This is fairly common for this ecosystem and most likely one of the biggest challenges for law enforcement agencies and their efforts to disrupt this form of crime effectively. There are two things to observe for the Hive operation and their takedown.

First of all, others tried to jump onto the 'brand' and its reputation and began copying the appearance of Hive's leak site (RansomHouse). Secondly, a re-brand of Hive surfaced in October 2023, 10 months after Hive was disrupted. The re-brand is called Hunters International[62][63] and so far has victimized two organizations, one in Europe and one in the U.S. Their malware code matches 94% of that used previously by Hive[64], but according to Hunters International themselves, they bought the code from Hive, fixed it and are otherwise not connected to the Hive operation or their members. In a statement from the 24th of October, they say:

> "We started to see that someone falsely decided that we are the Hive ransomware group based on a 60% similarity of encryption code. All of the Hive source codes were sold including the website and old Golang and C versions and we are those who purchased them.
>
> Unfortunately for us, we found a lot of mistakes that caused unavailability for decryption in some cases. All of them were fixed now. As you may see here, encryption is not our primary goal, that's why we didn't do it by ourselves."
>
> Hunters International leak site, under "News"

As a side note, what the Hive hack showed us besides the attempt to disrupt them was the amount of victims they had compromised and encrypted. At the time of infiltration by the FBI, 300 victims were still under attack and 1000 victims had already suffered from an attack. The FBI provided a total of 1300 victims with a decryption key[65]. In our our records, we registered 208 organizations that had fallen victim to Hive, **which makes the actual number of victims 5x higher!** This is an important insight into the problem of not knowing how big the problem actually is and gives us an indication of how high the 'dark number' of victims really is.

Government efforts

In the last week of October 2023, the Biden administration hosted officials from 50 countries for its 'International Counter Ransomware Initiative' (CRI) to discuss potential future policies on regulating ransom payments and information sharing[66]. On November 1st, just in the final days of writing this report, the White House announced that more than 40 countries had signed an agreement pledging not to use central government funds to pay ransoms to cybercriminals[67].

Countries want to lead by example by not paying the demanded ransom and thus stopping the funding of this criminal ecosystem. While this commitment has a big potential to disrupt the ecosystem, it still remains to be seen how effective it will be in the long-term. Denying ransom payments to Threat Actors that are in the majority financially motivated, can potentially have an enormous impact. Leading by example is a good start. However, if we compare the proportion of public and private organizations in our victim dataset; we see that the public sector only represents 3%. Most of the impact of those attacks had to be endured and dealt with by the private sector.

Nevertheless, a collective effort as we see with the CRI 2023 is exactly what is needed. Besides the above-mentioned agreement to not pay ransom demands, other efforts are equally important. Some of the key CRI deliverables of this year's meeting were:

- Developing capabilities with the help of technology, e.g. Artificial Intelligence (AI) and training
- Sharing information via dedicated platforms
- Developing fighting back capabilities, e.g. share blacklists of wallets used by ransomware actors, assist any CRI member with incident response if government or lifeline sectors are suffering a ransomware attack

The CRI deliverables of 2023 are very important efforts that will hopefully show their potential in the long run. We are very curious to see what effect it has on the current Cyber Extortion ecosystem.

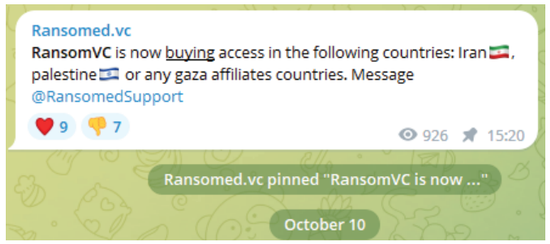
Fighting each other: a vigilante response?

Besides a direct response of law enforcement agencies and a collective effort of certain governments against the increasing threat of Cyber Extortion and ransomware, we have seen other types of responses.

One observation that we are making is a recent event where a hacktivist group has taken actions into their own hands and took down a Cyber Extortion operation in October 2023. The pro-Ukraine hacktivist group called Ukrainian Cyber Alliance apparently took down the Trigona ransomware leak site and its servers. This action was accompanied by the statement "[…] disrupting Russian enterprises (both public and private) since 2014."[68]

This is not the first time we've seen "crossovers" between hacktivist groups and ransomware / Cyber Extortion operations. For example, hacktivist groups such as Anonymous Sudan have demanded ransoms to stop their ongoing DDoS attacks[69]. Another hacktivist group, GhostSec, turned towards ransomware, and has released its own variant, called GhostLocker, as a self-proclaimed "next-gen Ransomware-as-a-Service" operation. GhostSec advertise their locker with the following capabilities: "robust military-grade encryption, undetectable by major AVs, fast C-coded locker for rapid execution, GhostMorph Polymorphic Engine for unmatched stealth", to mention a few. This makes GhostLocker a service to be taken seriously and watched closely. GhostSec belongs to the Anonymous hacktivist collective, and at least one other hacktivist group, Stormous, who belongs to the same collective, has announced that they also intend to use GhostLocker[70].

Finally, we have ransomware / Cyber Extortion groups that have turned from purely financially driven to more politically directed activities. Examples include Conti, CoomingProject and Stormous, who proclaimed their full support for Russia in their war against Ukraine[71]. Ransomedvc posted publicly in their Telegram channel that they want to buy access for Iran or Palestine after the Hamas-Israel war broke out, which may indicate that the group might have picked its side and is planning to attack organizations in Iran and Palestine.



And another example is Cuba ransomware, whose group members began targeting government and military officials in Ukraine for espionage[72][73].

The Trigona case is still slightly different, in the sense that one group took down another group in a vigilante-style operation. Like Law Enforcement activities that are similarly disruptive in nature, the challenge for them is that such takedowns might only be temporary. Additionally, it can always be an opportunity for someone else to fill that void or for the same Threat Actors to re-organize and re-brand. It's important to highlight that the Trigona take down was not an action against cybercrime but was part of a politically driven effort to disrupt any Russian cyber operation. Nevertheless, it was an action of disruption. Given the current geopolitical situation and the number of individuals and groups taking part in geopolitical cyber operations; we anticipate seeing more of these actions in the future.

Reminding everyone on their responsibilities during war

And then another final observation we made in terms of who responds to the current threat landscape; we saw that the International Committee of the Red Cross (ICRC) published a guideline for anyone participating in hostilities by the means of cyber[74]. As we have stated in several places of this report, 2023 has shown how messy cyber space has become. This is mostly due to the ongoing war against Ukraine, which mobilized many different Threat Actors to support either side of the conflict, but we see similar activity in the most recent Hamas-Israel war.

In the context of Cy-X, we see how current geopolitical events have politicized some actors[75], who until recently were financially focused in their actions but have become more politically driven.

Aa a result, the latest “crossovers” between Cyber Extortionists and hacktivists but also the intensification of hacktivist activity generally in recent conflicts, did not remain unnoticed; others observing the same concerning trends.

As a response, the ICRC has posted a guide of 8 rules for “civilian hackers” during war, and 4 obligations for states to restrain them, written by Tilman Rodenhäuser and Mauro Vignati[76]. They are emphasizing the importance that even in times of war, civilian hackers must respect the law of the countries they are in, or where the national laws are not enforced, or being disregarded in times of armed conflict, international humanitarian law (IHL) provides a set of rules to safeguard civilians, soldiers and others from war.

Consequently, this is addressing two issues at hand, first of all we are witnessing civilian hackers execute cyber operations in an armed conflict. Participating directly in hostilities[77] means that participants have the potential to cause real harm against civilians, risk exposing themselves and people close to them to military operations; and hence the risk for civilians grows. Secondly, civilian hackers do not live in cyber space and should comply to national laws, states should not encourage or tolerate hackers conducting cyber operations in armed conflict, say the authors.

They continue, stating:

> **“Any State that is committed to the rule of law or a ‘rules-based international order’ must not close its eyes when people on its territory conduct cyber operations in disregard of national or international law, even if directed against an adversary .”**
>
> Tilman Rodenhäuser and Mauro Vignati [78]

Is it (im)possible to disrupt a dynamic ecosystem?

We have explored the side of law enforcement and government responses, highlighting how difficult it can be if the ecosystem is so effective in causing such a high amount of victims yet at the same time still managing to remain so flexible. As we have argued previously, it’s an opportunistic crime. One’s takedown and inability to participate in the criminal market of victimizing organizations for millions of USD; is another’s opportunity. We are long aware of this dynamic. It also does not help that many operations are run as a cybercrime-as-a-service operation thus increasing their efficiency by outsourcing certain attack stages, e.g. Initial Access, to others who have specialized in it. The adoption of affiliates who then help increase covering more 'victim ground', has certainly had an impact on the sheer number of victims. Through this, the ecosystem as such can be perceived to be bigger than it actually is.

A good example of this is that we see almost the same number of Threat Actor Groups participating in Cyber Extortion in 2023 as we saw 2 years ago (in a year on year comparison). However, the victim numbers have increased so much that it seems that more individuals and groups of individuals have joined the Cy-X party. That is in fact not the case in our two-year comparison. But noteworthy, the Threat Actors that extorted victims two years ago, are of course not the same constellation of Threat Actor we now observe in 2023. By tracking Cyber Extortion operations as actively as we do, we do feel that the sheer amount of new leak sites we had to add to our tracker has exceeded anything we did in previous years.

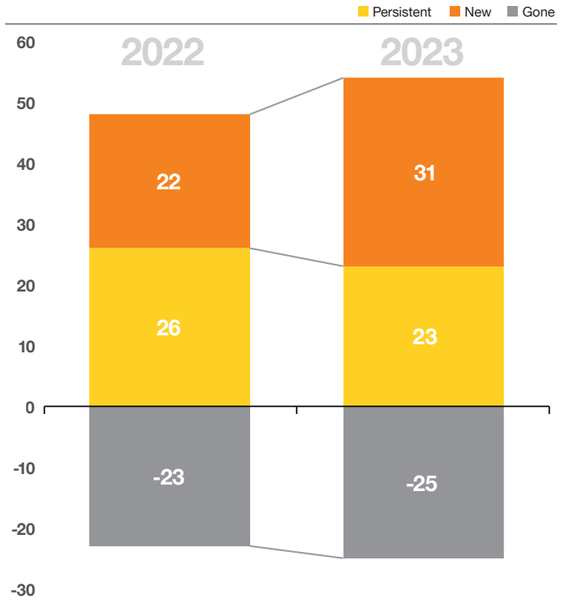
Therefore, we started to investigate this, tracking all the Threat Actor Groups we have been collecting in the last 3 years to see if we can track the threat actor movements. For this we began looking at groups we tracked between 1st of October 2020 to 30th of September 2021 and called this time frame “2021”. We continued doing this for the next two years, which gave us an overview of which threat actor groups were active in each respective year (2021, 2022, 2023). We then compared 2021 to 2022 to check whether or not the groups we observed in 2021 were still active 12 months later. This gave us the 2022 actor distribution. We repeated this calculation with 2022 to 2023, which resulted in the 2023 actor distribution

We gained three insights:

1. Groups that only started extorting in the past 12 months; we called **“new”**.
2. Groups that we have not seen active in the past 12 months; we called **“gone”**.
3. Groups that we are still seeing active over a period of 12 months and longer, we called **“persistent”**.

Below we show the results of this investigation into the movements of Threat Actor Groups of the past 3 years.

Actor lifecycle changes



Interestingly, we see different movements in both periods, as was our expectation (as can be seen above). In 2022, we saw 26 persistent threat actors that we had already observed and monitored the year before. A similar number of groups, 23, closed operations during that time, and we tracked 22 new groups that weren’t active the year before. It’s noteworthy that new groups don’t necessarily have to be entirely new but can be a re-brand of an old group. Our CERT team tracks new groups and re-brands and other aspects in a cartography that can be found on GitHub[79].

What does that mean for the actor movements between 2022 and 2023? The almost equal number of groups which perished and groups that began their criminal operations underlines an argument we have been making for some time: It’s very opportunistic and gaps are very quickly filled by other motivated Threat Actors.

However, while in the 2022 period, we saw more persistent groups than new ones; in 2023 that has changed. In fact, we see the opposite proportion of activity. We see many more new groups (which was our feeling all along) than we see persistent groups or groups that have closed down operations. But at the same time, we observe less persistent groups in 2023; which in itself does not change the fact that there are other active groups about, e.g. the new ones, extorting victims. In fact, it increases the problem, since we see a higher number of active groups (2023: 54) than we saw in 2022 (48). And finally, similar to our argument of opportunity, we see many more new groups active in this criminal space than we see groups being closed or choosing to close operations.

Consequently, Cyber Extortion seems lucrative enough for new groups or slightly new groups (re-brands) wanting to join this ecosystem.

For the curious minds, below are some examples of groups we classified for the past 12 months.

Examples of “New” (and re-brand) groups:

Play, Royal, Akira, etc.

Examples of “Gone” groups:

Conti, Pysa, Grief, etc.

Examples of “Persistent” groups:

LockBit3, ALPHV(BlackCat), BlackBasta, etc.

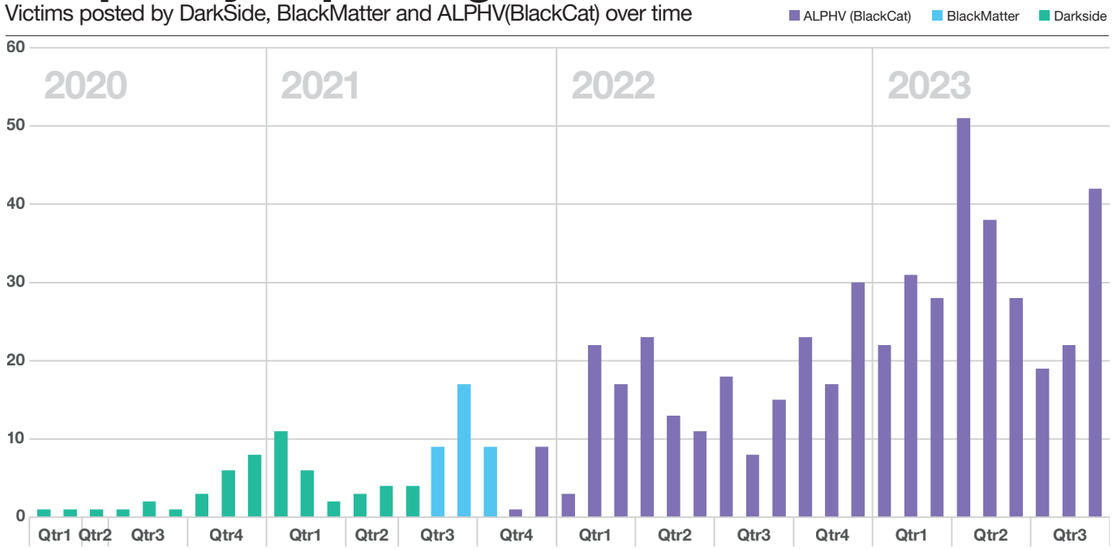
New name, new threat profile

Often re-branding helps threat actors to “start over” and/or cover their tracks. In some cases, vulnerabilities in their encryption or weak OpSec in their own operations will motivate Threat Actors to close operations and “come back” under a slightly different name/brand, sometimes in different settings (new developer team, etc.).

One example that we have been tracking since 2020, both in terms of victimology but also Threat Actor Group attribution[80], is the Cyber Extortion operation currently known under the name ALPHV aka BlackCat. In 2020, this group was known as DarkSide, which re-branded and began victimizing organizations - most recognized victim being Colonial Pipeline - under the DarkSide brand in 2021. And shortly after DarkSide closed operations in July 2021, BlackMatter began extorting victims between August 2021 and October 2021. Just one month after, in November 2021, the new brand "ALPHV (BlackCat)" began extorting victims[81].

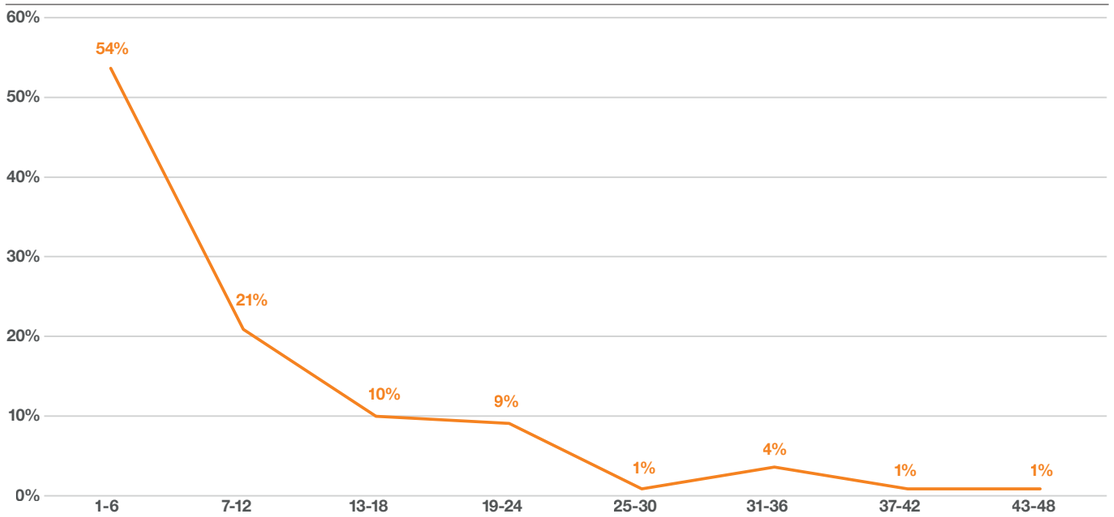
Frequency of posting victims

Victims posted by DarkSide, BlackMatter and ALPHV(BlackCat) over time



Lifespan of actor groups

Amount of groups and their life-span in months



Given the fact that we do see a lot of movements, what kind of lifespan do these operations have, especially when we consider their age (in months)? We looked at all Threat Actor Groups we have collected in our victim dataset since January 2020. We tracked a total of 110 different operations since then. Of those, we wanted to know what their lifespan looked like, for this we split the lifespan into 6 month intervals.

Interestingly, half of all the Cyber Extortion operations only made it to the first 6 months. Another 21% had a lifespan of 7-12 months. 10% of all operations made it to the age of 13-18 months. As can be seen above, only a very few make it to 2 years and older.

This highlights the challenges for anyone defending against or attempting to disrupt Cyber Extortion operations. By the time one realizes that they have become a real problem, impacting organizations around the world, half of the Threat Actor Groups have closed operation within the first 6 months. The average age in months of all the tracked Cyber Extortion operations is 9 months. Of the groups that have made it the longest, we in fact only see one Threat Actor Group, which has been active more than 43 months and that is Cl0p – who at the time of writing are still active. The second oldest Threat Actor Group representing the 1% within the 37-42 months lifespan was RagnarLocker, who at the time of writing had just been dismantled on the 20th of October 2023[82].

Conclusion

As we have shown, Cyber Extortion is a complex ecosystem that is under constant evolution. At the same time, it is a serious problem, especially for private organizations globally. The volumes of victims do not seem to decrease, in fact we see the opposite with significant increases in victim count that are unproportional to the increase of Threat Actors participating in the crime of extortion. We therefore conclude that the ecosystem, as fast paced as it is, has become much more effective than the defending entities. Even though we do see increasing efforts by law enforcement agencies and local authorities, especially in the fight against ransomware / Cyber Extortion; we don't see any significant effect yet.

However, there are some promising trends that potentially could have an impact in the near future. The most promising efforts are those that are taken collectively, just as cybercriminals use and re-use their resources and capabilities, so should we as defenders. Witnessing the successful LE actions and collaboration between different law enforcement agencies and countries shows that collectively we can have an impact. Additionally, we see governments committing and joining the fight against Cyber Extortion, hopefully helping by sharing information, training, and developing technologies that can assist with this goal and positively impact the efforts.

In the end, it still remains a big challenge, investigations can be lengthy and thus disproportionate to the actual lifespan of criminal groups. Disruptive efforts and takedown definitely have an impact but in cases where no arrests are made, individuals have the chance to re-organize themselves and continue extorting victims. We have seen several arrests in the past 2,5 years which shows the effect of efforts and at the same time can have a deterrent effect for future offenders.

Alternatives, such as publishing guidelines and appealing to states and individuals engaging in crime or even hostilities in times of armed conflicts, as we are experiencing now, are also important to raise and remind.

As we have studied the current threat landscape of Cyber Extortion, we unfortunately need to admit that current efforts to disrupt the Cy-X ecosystem have not shown any effect when looking at the ever-high victim count. Nevertheless, the defender's space has become at least as busy as the offenders space; which hopefully means that in the (near) future those efforts will show effect.

Hacking a factory

A safe way to testing ICS/OT environments

The number of known malware targeting industrial systems keeps on increasing and was intensified in 2022 due to the war against Ukraine[83]. These systems, also referred to as Operational Technology (OT), differ from the Information Technology (IT) that we are familiar with and can be described as hardware and software components used to control physical and mechanical processes. It includes equipment, protocols, software, and processes specifically used in manufacturing, energy, transportation, or even building management systems.

Claire Vacherot, Security Auditor, **Orange Cyberdefense**

Used to be an island

Historically, OT systems used to be closed, standalone systems. They eventually became interconnected and started using IT standards in addition to their own, to simplify the processes of supervision, operation and maintenance. In other words, the OT became reachable remotely to its authorized users, but also to illegitimate actors.

From safety to security

While industries have long been concerned about safety, cybersecurity was not a priority until a few years ago. Some thought that OT was not a relevant target, while others believed that the cybersecurity controls that are commonly endorsed on IT wouldn't cope with the technical and operational differences of OT systems. Consequently, the level of awareness and the technical measures available to enforce them is often far behind what we can find on information systems, while the means of attackers have evolved. Fortunately, the situation has changed, and OT cybersecurity has emerged, with measures either specific to OT, or borrowed from the IT and adapted to the industrial world. Penetration testing is one of these measures.

Assume it's insecure until it's tested

A penetration test is used to simulate malicious operations performed by a malware or an attacker, and this type of test is quite common in organizations' internal networks (IT). During such assessments, security auditors explore the system, trying to find exploitable flaws that could be combined into realistic attack scenarios. The aim is to provide a prioritized mitigation plan for these vulnerabilities, based on real-world attack techniques. It can also be used to raise awareness on cybersecurity risks.

Needless to say, unlike real attacks, the auditors will adapt their testing process to make sure that they don't disrupt the system. When applied to OT, this is probably the most important part of the tests. Indeed, many OT components are not designed to be exposed and may not handle invalid or superfluous network traffic and operations. Above all, involuntary disruptions may have disastrous consequences.

Penetration tests on industrial systems must be carried out with utmost care, preferably on environments under maintenance or on a test bench.

When performed on a running environment, the assessment requires an important preparatory phase. Sensitive components may be excluded from the tests to minimize the risks on availability and integrity while preserving the safety.

How are penetration tests on industrial systems conducted?

The most common entry point to the OT is through the IT, connected to the Internet. Several industrial malware such as the ones from the BlackEnergy family were introduced using phishing and spread until they reached the OT[84]. Therefore, most penetration testing processes start from the IT. The auditor tries to find a way to the OT, most likely by making use of network segmentation issues such as authorized network flows or dual-homed stations between the two environments. Another scenario consists of simulating an attack introduced directly in the OT, using a compromised device (maintenance station, USB drive, etc.), or via a device exposed on the Internet.

Once the OT is reached, the penetration tester first needs to identify its technical assets. She looks for workstations and servers as she would do on IT, but also for industrial components. This includes software, protocols, and devices such as programmable logic controllers (PLCs), HMIs, actuators, sensors, and any type of equipment that is not an IT asset . This discovery phase is usually conducted with the help of network scans.

However, as we discussed before, such an environment is likely to include old devices, and sending them unexpected network traffic may have harmful side effects. For this reason, additional information is required beforehand to locate critical or sensitive components. The auditor will still explore the network as an attacker would, but she will exclude or be careful with assets that could become unstable and take extra measures when contacting components (run restricted and targeted scans, use only genuine tooling, etc.). It is also important that a technical contact is available at any time on site during the assessment. This person is contacted immediately in case of a suspected issue.

The next step for the auditor is to search for vulnerabilities. The main difference with penetration tests on IT is that, here, she does not do any malicious operation nor action that may have side effects. For instance, it is strictly forbidden to run a man-in-the-middle attack to intercept traffic in industrial networks, while this is a common test on IT networks. So, how is a test conducted?

From our experience, we noticed that most of the time, an attacker who can reach an industrial component on the network is already able to misuse it or make it unavailable. Thus, the auditor first tries to reach as many components as possible. She may use the access she gains to find hosts with extended network permissions that are used as "pivot" to access additional components.

Once accessed, the auditor evaluates the attack surface of the components. Assessing the cybersecurity of servers and workstations follows a similar process as on IT (namely, abusing Linux, Windows, and Active Directory weaknesses) . This is different for the other industrial components. Here, the aim is to gain as much information as possible on it: what type of device it is, what it is used for, what it is interconnected to, which version is used by each of its modules, what network services are enabled, what functions are available, and how they are configured. As mentioned before, this is usually sufficient to show how damaging an attack could be. Indeed, many of them have not been designed or configured with cybersecurity concerns. For instance, a lot of industrial network protocols are neither encrypted nor authenticated: sending the appropriate network request may change a device's behavior. Also, it is common to find devices with unused services enabled, default credentials, or available security features disabled.

Finally, it is likely that some components are exposed to public vulnerabilities, as updating and applying security patches on industrial systems is difficult considering operational and availability constraints. Malware such as Pipedream[85] embed exploitation codes for several vulnerabilities targeting specific versions of PLCs. The auditor does not exploit these flaws in production, but may ask for a test environment, if available, to provide proof of concept.

Test successful!

The last step is the reporting phase: all the findings are combined to build the attack scenarios, along with the remediation plan that will help prevent them.

Although every plan is unique to its context, the first improvement we usually recommend is network segmentation between the IT and OT as well as between trust zones within the OT. As long as they are not secure, and even then, the best we can do is to ensure that no attacks reach industrial systems.

Dr. Ric Derbyshire
Senior Security Researcher
Orange Cyberdefense

Making Sense of Operational Technology Attacks: The Past, Present and Future

When you read reports about cyberattacks affecting operational technology (OT), it's easy to get caught up in the hype and assume every single one is sophisticated. But are OT environments all over the world really besieged by a constant barrage of complex cyberattacks? Answering that would require breaking down the different types of OT cyberattacks and then looking back on all the historical attacks to see how those types compare. That's exactly what we've done for this chapter.

Over the next few pages, we want to demystify what is going on with OT cyber security and what attacks we are facing. To do this, we define 5 types of cyberattacks that can affect OT, which are split between 2 categories. We then analyse 35 years of OT cyberattacks and get further context by seeing how they stand up when compared to our proposed types and categories. This leads us to some findings that spark questions about the future of OT cyberattacks and whether we'll see a shift in type or category in the medium to long term. We then conclude with an example of how we think OT cyberattacks may evolve in the future.

The types of OT cyberattacks

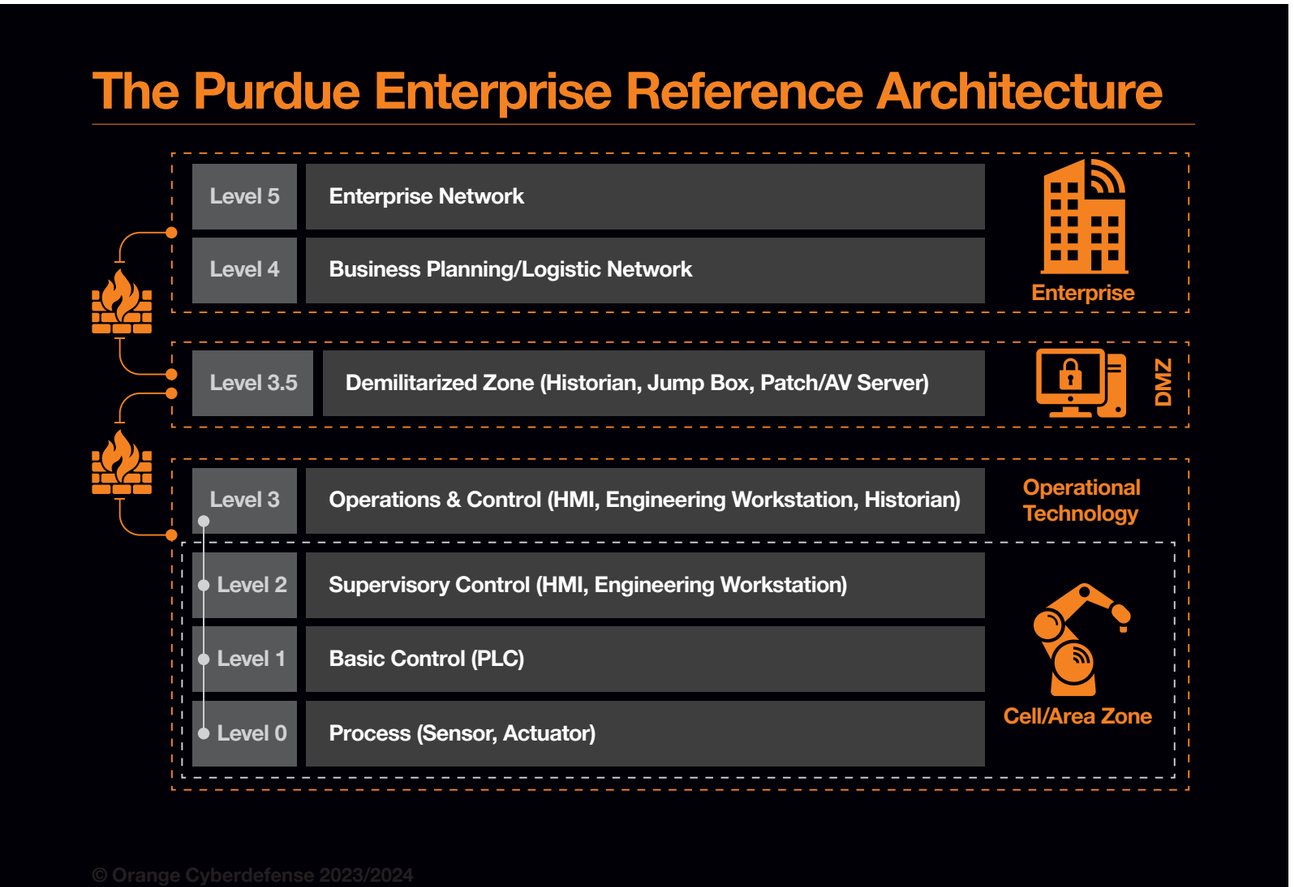
Over the past few decades, there has been a growing awareness of the need for improved cyber security practices in IT's lesser-known counterpart, OT. This significantly accelerated at the turn of the 2010s with the discovery of perhaps one of the world's most advanced offensive cyber capabilities, in the form of malware embedded within the OT of Iranian nuclear centrifuges. We are, of course, shamelessly starting a chapter about OT with a reference to no other than the infamous Stuxnet. There is a good reason Stuxnet references are so commonplace, its discovery and ensuing awareness has almost singlehandedly brought to fruition the OT cyber security industry as we know it today. What made Stuxnet such a watershed moment in OT cyber security is the complexity and precision with which it targeted OT-specific hardware and software. No known attacks before or after Stuxnet have achieved quite the same level of sophistication, particularly in their specific targeting of OT. In fact, the lines of what constitutes a cyberattack on OT have never been well defined, and if anything, they have further blurred over time. Therefore, we'd like to begin this report with a discussion around the ways in which cyberattacks can either target or just simply impact OT, and why it might be important for us to make the distinction going forward.

How we're defining OT

Before we define any types of OT cyberattack, we need to define what we're considering as OT. Most OT environments are unique due to several factors, such as the different applications and use cases, the numerous vendor ecosystems, and the simple fact that there are multiple ways to engineer a physical process, to name a few. Because of this, it helps to turn to the Purdue Enterprise Reference Architecture (PERA), commonly known as the Purdue Model, depicted below.

The Purdue Model describes the conceptual structure and separation of various processes and networks in an organization that utilizes OT. It is important to note that the Purdue Model is only a reference architecture, meaning it is a basic approximation and not something that should directly define an implementation. However, we can use this model to describe OT and its constituent devices, as well as provide a reference point for the types of attack OT may experience. So, this is an application where it is particularly useful.

From the top, it begins by outlining levels 4 and 5 as the Enterprise Zone, where traditional IT is encountered. Next is level 3.5, the Demilitarized Zone (DMZ), which acts as a separator between IT and OT and therefore the OT's perimeter. The remaining levels below the DMZ are all OT. Levels 2 and 3 are similar in that they both may monitor, control, and even configure the physical environment.



However, level 2 is typically specific to a single cell or process and perhaps even physically close, whereas level 3 is generally centralized, particularly in geographically dispersed organizations. Level 1 is the heart of OT, where devices such as programmable logic controllers (PLCs) will sense and actuate the physical world according to the logic they have been provided. Finally, we reach level 0, which for all intents and purposes is the physical world and contains the sensors and actuators that the PLCs use to manipulate it.

The different types of OT cyberattack aren't necessarily defined by the assets that they impact, rather the assets that they target and how they are targeted. More specifically, the precision, skillset, and intent with which they are targeted. While that distinction may sound pedantic, it changes the threat landscape that defenders need to consider and makes it challenging for traditional IT controls to keep up. There are 5 types of OT cyberattack that can be grouped into two distinct categories, let's explore them.

Category 1: IT TTPs

The first category of cyberattacks endured by OT is the most frequent in public reports, such as Dragos[86] and Waterfall[87]. They are characterized by the use of only IT tactics, techniques, and procedures (TTPs) but still manage to affect production in some way. There are 3 types of OT cyberattack in this first category.

Type 1a: IT targeted

The first type, 1a, occurs when the OT environment isn't even reached by an adversary. So, as far as the adversary is concerned, their attack does not target the victim's OT. Instead, there are cascading impacts from an uncontained IT cyberattack, such as Cyber Extortion (Cy-X) delaying shipping systems that requires production to stop. Alternatively, the OT is disconnected or shut down by the victim as a precaution. Meaning in this type of attack, the OT may only be affected indirectly as the victim attempts to maintain safety and integrity of the OT network. The OT impacts of this can range from a temporary loss of telemetry all the way to complete loss of production and a complex, time consuming process to bring it back online. It is important to note that every OT cyberattack type may also result in a disconnect or shutdown of the OT environment as part of the response and recovery efforts, which would ultimately cause similar affects.

Type 1b: IT/OT targeted

The second type, 1b, is when the OT is reached by an adversary either by accident or just because they could. Still conducting IT TTPs, the adversary may deploy ransomware or exfiltrate data for double extortion. However, perhaps due to a weak or non-existent DMZ, the adversary's attack may extend to some OT assets in levels 2 or 3 of the Purdue Model. The affected OT assets may include devices such as engineering workstations, Windows-based human machine interfaces (HMIs), and other IT-based technology. Although the adversary has managed to directly affect OT assets, the targeting is generally not deliberate. The impact of this attack type may include loss of configurability or even control of the OT environment, but it is unlikely to affect production on its own unless there are cascading effects or until the victim begins response and recovery.

Type 1c: OT targeted

The third type in this category, 1c, is the most nuanced and the closest in nature to the next category. Here an adversary with little to no OT capability may deliberately target the Windows-based OT assets of an organization with IT TTPs. This may be to trigger more of a response from the victim or to cause a more serious impact than from just affecting IT. This attack type may deliberately target OT assets, but only those with which an IT-focused adversary would be familiar. There is otherwise no OT-specific intent or utilisation in such an attack, nor is there any precision in the way production is impacted. As with type 1b, the impact of this type of attack may include loss of configurability or control of the OT environment, and production is only likely to be affected by cascading effects or response and recovery efforts.

Category 2: OT TTPs

The second category includes the two types that likely spring to mind whenever OT cyberattacks are mentioned. These are characterized by the inclusion of OT-specific TTPs and have the primary intention of directly affecting production in some way.

Type 2a: OT targeted, crude

The overall fourth type and first of the second category, 2a, is sometimes known as the nuisance attack. This type of cyberattack is predicated on the adversary reaching the OT, regardless of DMZ. It leverages rudimentary OT-specific knowledge and TTPs, but in a blunt fashion with little precision or complexity. Rather than just disrupting Windows-based assets such as in category 1 attacks, it may target OT assets in deeper levels of the Purdue Model, closer to the physical process, such as PLCs and remote telemetry units (RTUs). The OT-specific techniques leveraged are crude and frequently use publicly known exploitation frameworks and tooling. The impact from this type of OT cyberattack generally will involve stopping PLCs cycling or imprecisely changing PLC outputs. This will undoubtedly affect production, but such blunt attacks are often overt and trigger a swift response and recovery effort.

Type 2b: OT targeted, sophisticated

The final type, 2b, is the most advanced but also most rarely observed. By exercising advanced OT capability, these cyberattacks are precise and complex in both their execution and impact. They involve extensive process comprehension, an OT-specific tactic of gathering information to understand the physical environment and how the OT interacts with it. Adversaries will combine their advanced OT capability with process comprehension to craft an attack that is bespoke for the OT environment they have gained a foothold in and affect it in a very deliberate way. The possible impacts caused by this type of OT cyberattack are near limitless but depend highly on the process under consideration. It is unlikely the impacts would be overt or simple, such as stopping the process, unless it was in an extreme and permanent way. Instead, the intended impacts are more likely to involve, for example, stealthily degrading the process or exfiltrating details of it to replicate it elsewhere.

Why is this important?

OT cyberattacks are frequently sensationalized in the news, and it is important to know when the hype is real. When distinguished by the two categories and further broken down into the five types between them, it becomes clear that not all OT cyberattacks are equal, and many are not worthy of the hype. In fact, you might find that under this lens many cyberattacks reported to have been against OT are relatively unremarkable IT cyberattacks that lie in category 1. In fact, the trend of category 1 attacks affecting OT appears to be growing with the ever-increasing interconnectivity between IT and OT. This is due to concepts such as the Industrial Internet of Things[88] and Industry 4.0[89] demanding more telemetry and control, in turn increasing the size and complexity of the OT perimeter and resulting attack surface.

In the short term, the skew towards category 1 might be saving us from the much-vaunted OT apocalypse. Many current OT cyber security controls are borrowed from IT, and as such, they are better at detecting and preventing category 1 attacks. However, as access to knowledge and equipment grows and as adversaries develop OT modus operandi that are relevant to their respective causes, there's a real possibility that we'll see a growing number of category 2 attacks. While we cannot ignore the upstream category 1 attacks, we must consider the truly unique OT threats on the horizon and begin to develop the relevant OT cyber security controls to detect and prevent them. An early step in doing this, therefore, is distinguishing the categories and types of attack to better understand how and when those category 2 attacks are on the rise.

35 years of OT cyberattacks

Thanks to Miller et al. for providing the data behind their paper[90] that gave us a great head start in this section, as well as to Nicolas Pairoux and Carl Morris for their help in gathering the remaining data.

The types of OT cyberattack that we've defined and the reasons for why they are important all rely on some bold claims. So, rather than expect you to take our word for it, we thought we'd put them to the test. To do this we've collected and analyzed every publicly reported OT cyberattack we could find, from 1988 to 2023. Before we get into that analysis, let's briefly talk about our data collection method for transparency.

Method

As is clear from our types of OT cyberattack, defining them in the first place can be quite difficult. However, our primary criterion was that each incident must have affected OT, at minimum a type 1a scenario. If an organization uses OT but only their IT was affected by a cyberattack, meaning their production was not affected, we did not consider it to be an OT cyberattack.

To further ensure that we had the richest data to work with, an incident was only recorded if we could find at least 4 of the 5 following criteria:

1. **Year of incident**
2. **Country of incident**
3. **Victim sector**
4. **Adversary type**
5. **Initial access vector**

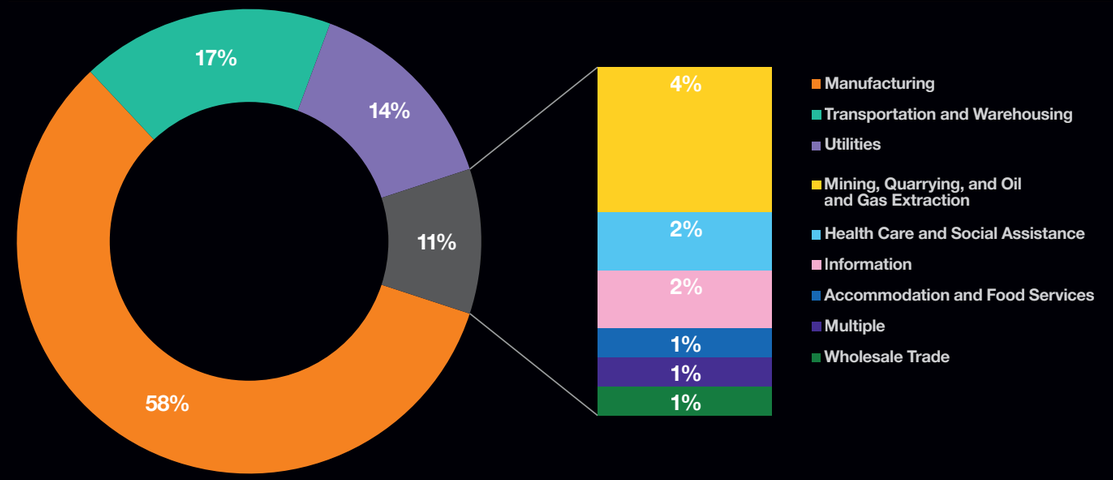
Collecting these minimum criteria did two things. First, it meant that each incident we recorded strongly contributed to our overall data. Second, it meant that the data sources were usually verbose enough for us to confidently speculate on the category and type of the attack, as well as the depth of the Purdue Model the adversary was able to target (not impact). If we weren't confident on that second point, the incident would also be discarded as this was crucial to our analysis.

What this means is that we were left with 119 recorded incidents over 35 years. We'll be the first to admit that it doesn't contain every OT cyberattack within that timeframe: it only contains incidents that were publicly reported, it only contains incidents that we could find, and it only contains incidents that were well reported enough for us to find all the data required. However, we do think that it provides us with a good insight into how OT cyberattacks have progressed over time and lets us put our categories and types to the test.

With all that said, let's check out the data.

Victims by sectors

Proportion of victims of OT attacks by industry sector



Analysis

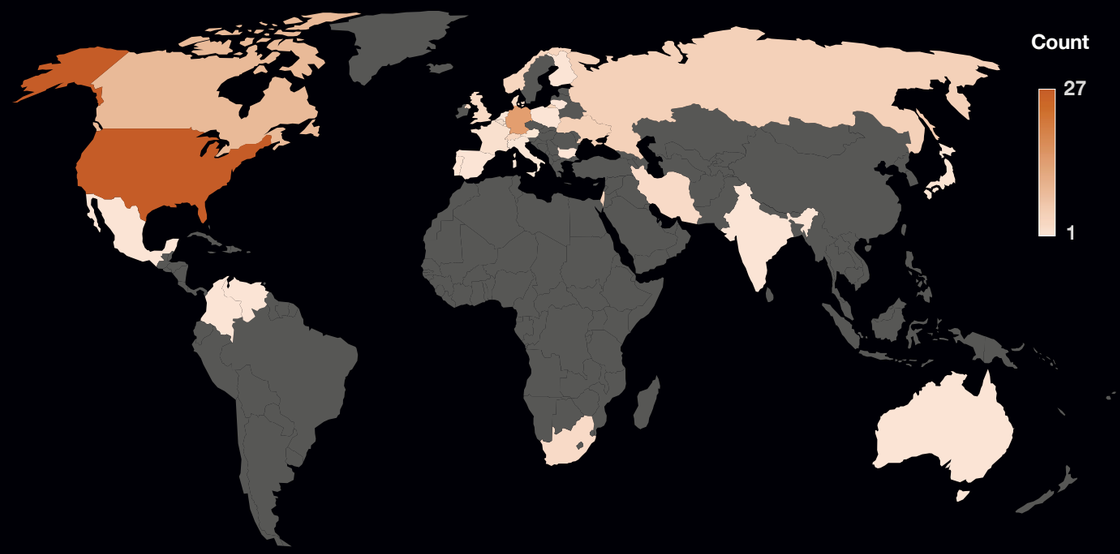
Despite being a relatively small data set for a Security Navigator article, there's a surprising amount to unpack and discuss, particularly because OT cyberattacks have changed over 35 years. This means that we can pick out some other interesting points from this data.

Overall demographics of OT cyberattack victims and their adversaries

To categorize our victims by sector we referred to the North American Industry Classification System (NAICS). What we found was that, over the 35 years, Manufacturing was the most frequently attacked sector and made up 58% (69) of all incidents. This is similar to our other datasets, such as Cy-X, it's just a little more exaggerated because there are a limited number of sectors that use OT. Transportation and Warehousing was the second most frequently attacked sector at 17% (21), followed by Utilities at 14% (17).

Country perspective

The geographic distribution of the victims was quite broad and not entirely what we had expected. It wasn't particularly surprising that the USA saw the most victims with 23% (27) of incidents, this is consistent with other datasets. However, we did see Russia as the 5th most targeted country with 4% (5) of incidents, which is different from what we see in other datasets – especially Cy-X. Although, this disparity is easily understood given the unique shape of Cy-X victimology. Russia's prominence is due to 4 hacktivists attacks shortly after their invasion of Ukraine in 2022. Germany saw 12% (14) of attacks, which is an uncharacteristic prominence in comparison to other datasets. 11% (13) of attacks impacted victims in multiple countries and were therefore recorded as 'multiple'.



When it comes to the types of adversaries conducting these OT cyberattacks, any nuance of individual groups or organizations was lost due to the long time over which they occurred. Therefore, we decided to group them into generalized categories for simplicity.

We found that criminals were the most frequent offender, perpetrating 61% (73) of our recorded OT cyberattacks. These were all Cy-X incidents, most involving ransomware. This may come as a surprise to those who were under the impression OT cyberattacks were all sophisticated government attacks against critical national infrastructure. However, nation-states were only the second most frequent offender, who conducted 13% (16) of OT cyberattacks. These mostly consisted of the commonly discussed attacks that typically spring to mind when one thinks of a sophisticated OT cyberattack (…Stuxnet).

Everything changed in 2020

For those who have been paying close attention to recent OT cyberattacks, the criminal adversary dominance probably didn't come as much of a surprise. However, those who did not expect it can be forgiven for two reasons. First, you've probably been bombarded by doomsaying marketing implying that critical national infrastructure the world over is on the brink of cyber apocalypse from hyper sophisticated nation-state cyberattacks (we hope, if anything, this report provides you a more pragmatic outlook). Second, and most importantly, it hasn't always been this way – at least not so publicly.

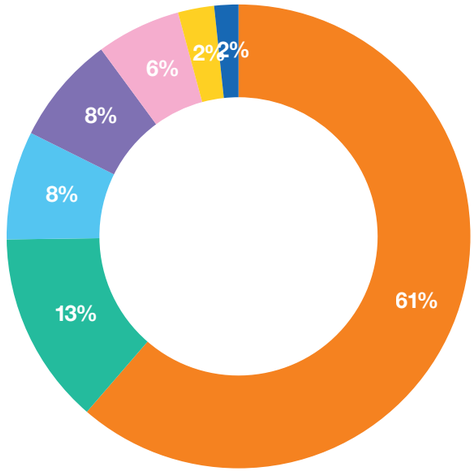
In 2020 we saw the advent of double extortion. Rather than stopping at using ransomware to encrypt everything they could on a victim's estate, criminals began to exfiltrate sensitive data too. Then regardless of whether the victim had paid their ransomware ransom, they'd be threatened with that exfiltrated data being leaked if a further ransom was not paid. What's more, these threats would be made publicly.

With the rise of double extortion, we have seen a rise in cyberattacks impacting OT. This could be because there are more attacks, or it could be because they're now much more public with the second phase of extortion. It's probably because of both, as well as a whole host of other small reasons all amalgamated together. Whatever the reason, a very distinct change happens around 2020 in our data.

Given that this is an issue caused by criminals, we'll start with adversary types. Once we look at what adversary types we witnessed by year, we begin to see the extent of the modern OT cyber security issue and the reason criminals dominate our data. Prior to 2020 there was a varied ecosystem of adversaries attacking OT, and notably fewer overall. We still find that variety in a post-double extortion world, it's just drowned out by the overwhelming number of criminal attacks.

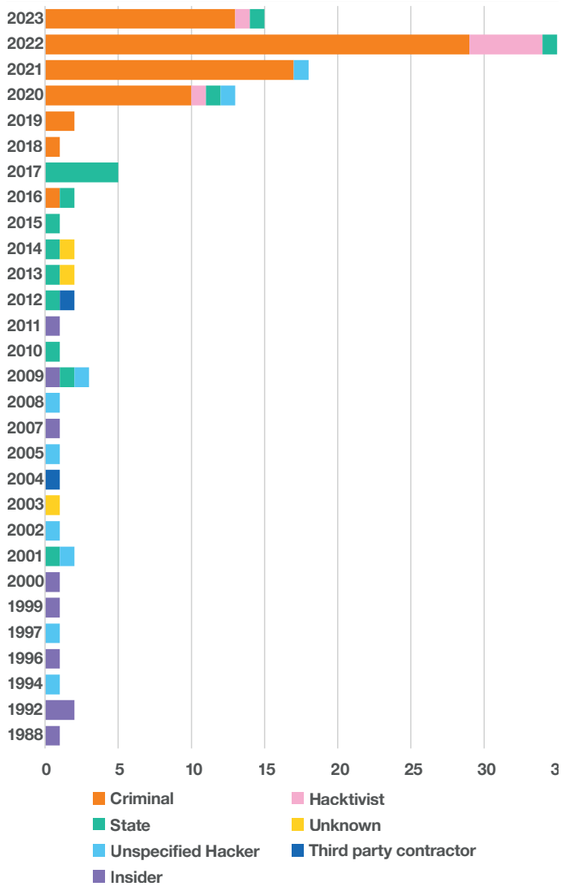
Adversaries

Proportion of different threat actors



Actor types over time

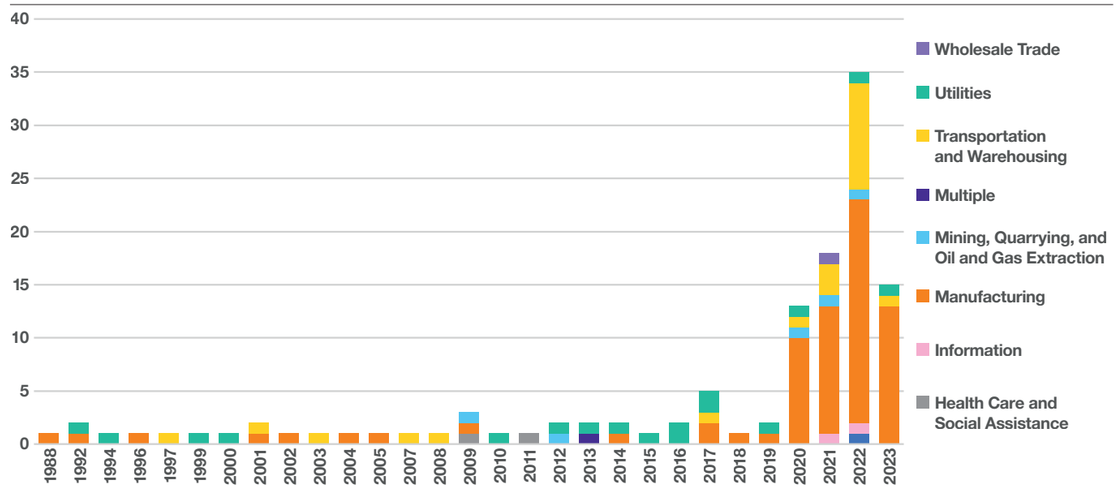
Adversary count per year



The rise of double extortion didn't just change the overall types of adversaries attacking OT, it also changed the overall victim sectors affected. When we break down the victim sectors by year, we also see a significant shift from a diverse range of sectors to being heavily manufacturing focused. However, given that Cy-X tends to favor targeting manufacturing, this makes sense.

Shift in victim count per year

Victims in different sectors over time



Types of OT cyberattacks in action

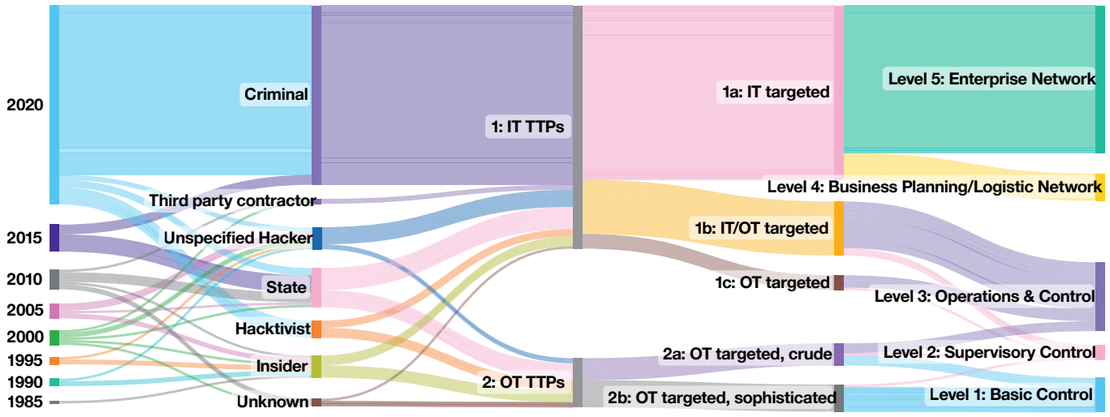
Before we look at how our data looks through the lens of our categories and types of OT cyberattack, let's have a very quick refresher about what they are.

Category 1 attacks are those which are for all intents and purposes IT attacks, due to the fact they do not utilize any OT-specific knowledge or TTPs. However, whether through collateral damage, circumstance, or opportunity, these attacks still manage to affect production, and therefore the OT. Category 2 attacks include the use of OT-specific knowledge and TTPs. These may either be crude attacks that clumsily use exploitation frameworks and tooling, or they may be sophisticated attacks that utilize process comprehension to expertly affect the OT and its processes.

Category	1 IT TTPs			2 OT TTPs	
Type	1a	1b	1c	2a	2b
	IT targeted	IT/OT targeted	OT targeted	OT targeted, crude	OT targeted, sophisticated
Characteristics	IT attacked, production impacted indirectly as collateral damage	IT attacked, Windows/Linux-based OT attacked with IT TTPs directly or as collateral	Windows/Linux-based OT attacked with IT TTPs directly	Dedicated OT devices attacked with OT-specific TTPs crudely, little precision or complexity	Dedicated OT devices attacked with OT-specific TTPs with sophistication

Flow: Attack operations

From year to adversary to category to type to Purdue depth

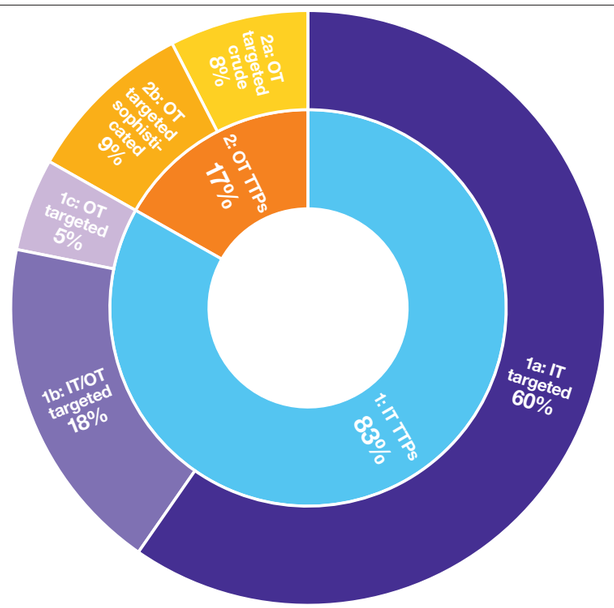


The above flow chart shows us flows of OT cyberattacks. The year of an attack, grouped into 5-year bins for clarity, flows from the left into the adversary that conducted the attack. The attack flow continues from the adversary to the category of OT cyberattack, through to the type. Finally, the type of attack flows into a representation of the deepest level of the Purdue Model the attack reached in terms of targeting (it may have impacted the OT completely even from Level 5).

The immediate takeaway from this visualisation is the drastic increase in attack frequency in 2020, which overwhelmingly saw criminals committing IT TTPs against IT targets, resolving at levels 4 and 5 of the Purdue Model. Moreover, every flow prior to 2020 has a much more varied ecosystem of adversaries. While not a novel discovery, it reinforces the two narratives we described occurring before and after the advent of double extortion in 2020.

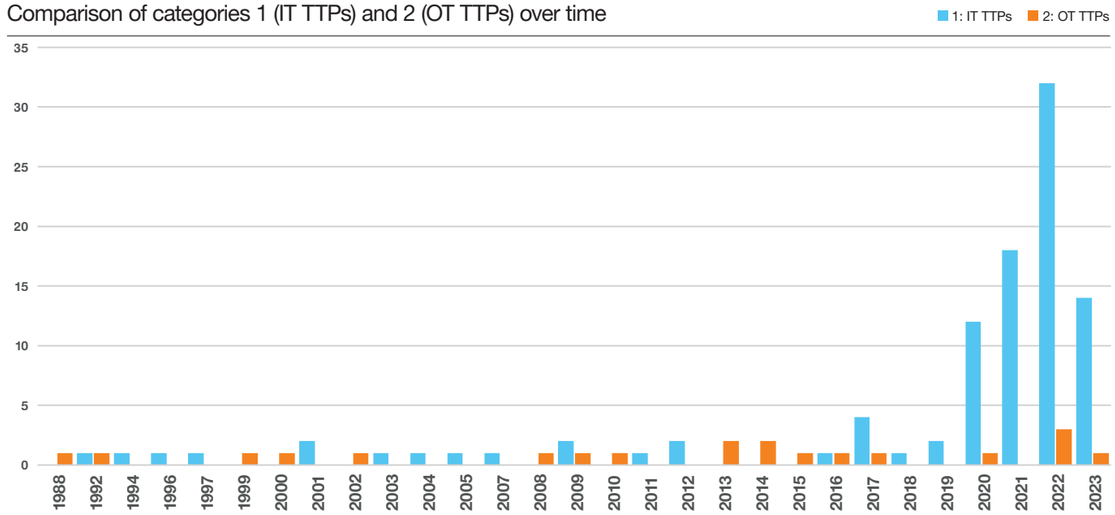
Distribution of categories and types

Overall count of OT attack categories and types



TTPs used over time

Comparison of categories 1 (IT TTPs) and 2 (OT TTPs) over time

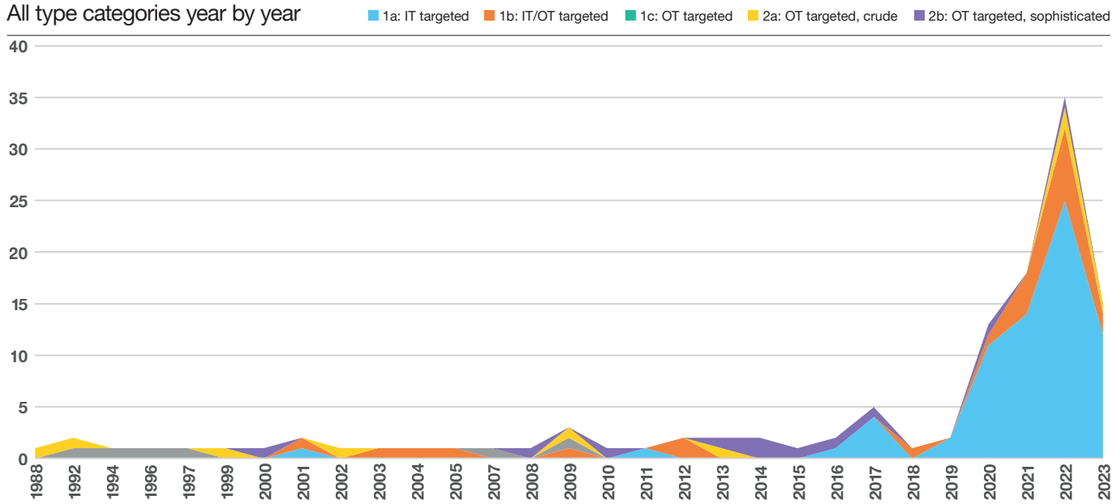


Delving into a deeper analysis of the categories and types, it becomes clear that a significantly larger number of cyberattacks that cause OT impact are category 1 and use only IT TTPs at 83% (99) of the total. This is bolstered by the large representation of type 1a attacks at 60% (71) of the total, which specifically target the IT, meaning levels 4 and 5 of the Purdue Model. By comparison, attacks that included the use of OT TTPs were poorly represented at 17% (20) of the total.

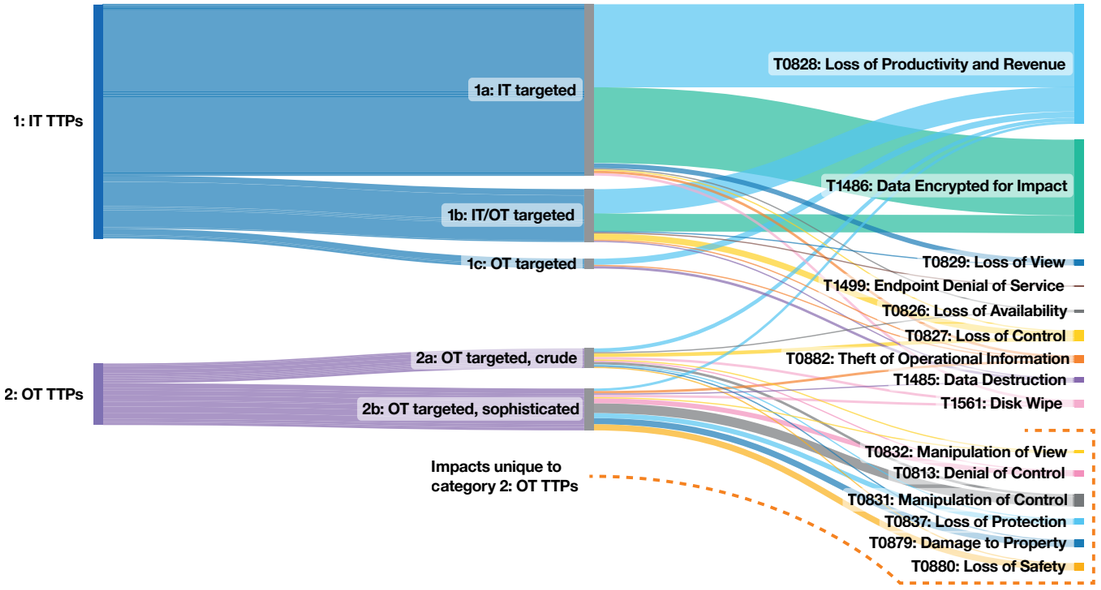
Breaking down the categories and types by year presents us with a familiar story. Prior to the 2020 rise of double extortion, the attacks were an approximately even split of categories and types, but Cy-X has taken over. Since 2020, type 1a OT cyberattacks (and therefore category 1) have erupted, which is to be expected as that is the type most likely to be associated with Cy-X attacks focusing on IT TTPs and targets.

All incident classifications over time

All type categories year by year



Categories to types of ATT&CK impacts



Whenever an OT cyberattack report's source described a specific impact, it was aligned to the MITRE ATT&CK® and MITRE ATT&CK® for industrial control systems (ICS). T0828: Loss of Productivity and Revenue was a prominent impact when production was affected and T1486: Data Encrypted for Impact was seen frequently due to 2020's rise in Cy-X. However, one interesting point is the cluster of towards the bottom right of the visualisation that only occurred as a result of category 2 OT cyberattacks. Of these category 2-specific impacts, T0831: Manipulation of Control was seen most frequently.

What does this all mean?

This analysis has explored the history of OT cyberattacks to understand the changing landscape and what we may face in the imminent future. The most notable takeaway is that the landscape is shifting heavily towards type 1a OT cyberattacks, those which use IT TTPs to target IT and only inadvertently affect OT. This trend provides fortunate breathing room for OT defenders. With a dearth of OT cyber security controls that are built from the ground up for an OT environment, defenders are typically left with reappropriated IT cyber security tools.

By breaking down OT cyberattacks into categories and types we can track shifts in whether OT TTPs are included in attacks, and how sophisticated they are. This allows us to understand what impacts adversaries are intending to achieve, which in turn allows us to better plan our defences and understand the areas of improvement for OT-specific cyber security controls as they are developed.

Conversely, the recent data from 2020 onwards, when split into its categories and types, shows that we shouldn't believe the hype of OT cyberattacks. Instead, we should be focusing on tackling the Cy-X issue in the short term. This means building operational resilience and confidence into our OT to withstand attacks on Levels 4 and 5 of the Purdue Model. We are, however, aware that is easier said than done.

So, where do we go from here? What will the future hold? Are all OT cyberattacks just IT TTPs on IT targets and circumstantial OT impact? Or might we see the relentless onslaught from criminals turn towards category 2 attacks for greater brutality?

Will criminals turn to OT TTPs?

Regardless of organizations that use OT, the current type 1a Cy-X attacks appear to be relatively lucrative for criminals, and the veritable pandemic may get worse before it gets better. However, all good (for them) things must come to an end at some point. If organizations begin to build up a resilience to contemporary Cy-X attacks, whether that is through good backup processes or otherwise, it is logical that criminal modus operandi (MO) will change. Given the prevalence of OT-using organizations as Cy-X victims, could we see that change in MO be towards category 2 OT cyberattacks? Fortunately, to facilitate a discussion around that question, we can turn to routine activity theory (RAT)[91].

RAT is a criminological theory that states a crime will be likely to take place given three elements are present: a motivated offender, a suitable target, and the absence of a suitable guardian. Here we'll provide a brief discussion on each point based on what we have seen so far.

Motivated offender

As can be seen from the OT cyberattack data we have presented here and the wider Cy-X data in this report, for whatever reason, criminals currently have a penchant for organizations that happen to use OT. What's more, the way current Cy-X attacks heedlessly affect their victims' OT environments makes it clear that criminals are not concerned about physical consequences. Either that or they are possibly even intentionally causing threats to safety. Lastly, if we see ransom payments for IT-focused Cy-X decline, that will likely pressure criminals into changing their MO to something for which their victims are less defensively prepared.

Suitable target

Criminals may already be specifically targeting organizations that use OT because they see the effect of impacting production as valuable. If existing methods for doing this, such as type 1a Cy-X attacks, decline in reliability, criminals may seek to target the OT directly instead. In our data, 40% (48) of all OT cyberattacks and 16% (12 of 73) of those conducted by criminals managed to reach the operational technology to affect it. These were type 1b, 1c, 2a, or 2b OT cyberattacks.

Adversaries, and to a lesser extent criminals, are already accessing OT environments. Should they require access to deliberately target the OT, it isn't inconceivable that criminals would be able to achieve it.

One important point regarding whether OT is a suitable target is its unfamiliar context to most criminals. However,while they would need to develop technical capability, has context menu, there is a growing base of OT cyber security knowledge in the form of courses, books, talks, and even dedicated conferences from which they could learn. Moreover, OT devices such as PLCs and HMIs are becoming less prohibitively expensive for learning and eventual attack testing. All of this culminates in lowering barriers to entry from a technical perspective.

The most fundamental point of this component is the suitability of the victim organisation itself. This suitability includes a large attack surface, available time for the adversary to conduct the attack, and the value specific assets may have to the victim. As we can see in historical Cy-X attacks, adversaries are already finding plenty of vulnerabilities to exploit in their victims and clearly do not often encounter what would be described as best practice cyber security. Moreover, the uptime and efficiency of an OT environment is often well quantified, meaning the value of OT impact is likely not as nebulous as encrypted or leaked data. This all presents a clearly suitable target in OT-using organizations.

Absence of a suitable guardian

If criminals consider moving away from conducting category 1 Cy-X with IT TTPs, it will primarily be in response to effective guardianship from IT cyber security controls. Therefore, they may move to exploit the challenge encountered in defending against OT TTPs caused by a lack of available controls that are specifically made for OT.

Technical security controls are not the only form of suitable guardian, of course. RAT considers other forms of guardianship, such as informal (community) and formal guardianship. The latter, formal guardianship, implies efforts made by law enforcement and governments, and it's something we explore the effectiveness of for IT Cy-X in another chapter of this report. Ultimately, OT will face the same challenges in disrupting the criminal ecosystem and so the absence of a capable guardian, or its effectiveness to disrupt crime, is a realistic outlook.

What this means

It wouldn't be prudent to outright declare that criminals are going to begin attacking OT with novel Cy-X techniques in response to less reliable ransom payments. However, it also wouldn't be prudent to say this is never going to happen, either. At the risk of sitting on the fence, we'll say that there is a genuine possibility that we may see Cy-X evolve to target OT-specific assets, it may just take a particularly innovative Cy-X group.

Dead Man's PLC

While we've been considering whether there may be a shift to criminals targeting OT with category 2 cyberattacks, we've been working on some interesting, speculative research. It has culminated in a novel and pragmatic Cy-X technique specifically targeted against OT devices; in particular, PLCs and their accompanying engineering workstations. We call it Dead Man's PLC.

As we can see from the 35 years of historical attacks, there hasn't been a publicly reported Cy-X attack that deliberately targeted PLCs. That might be because traditional, encryption-based ransomware isn't quite effective (or perhaps even achievable) against them. Firstly, the criminal would require specific vendor/device exploits to attain root level access on each device they want to target, which means attacks across multiple organizations that utilize different vendor ecosystems are hard to scale. Secondly, typical engineering response and recovery practices involve replacing faulty devices with new ones and flashing the configuration back to them, which would render encrypting individual devices ineffective. However, you don't need to rely on IT TTPs or encrypt PLCs to perform Cy-X against OT, because in OT we have something that can be targeted that isn't possible in IT Cy-X attacks – the physical world.

Dead Man's PLC starts at the engineering workstation, the asset where engineers will create configurations and load them onto PLCs across the OT environment. Nozomi recently reported that 34.7% of attacks in OT environments are facilitated by engineering workstations[92]. Moreover, we've seen in this report that there is no shortage of OT cyberattacks reaching the depths of the Purdue Model where engineering workstations may reside – generally levels 2 or 3 depending on numerous factors.

When the criminal is on the engineering workstation, they can view existing 'live' PLC code in their project files, edit them, and download new configurations to the PLCs.

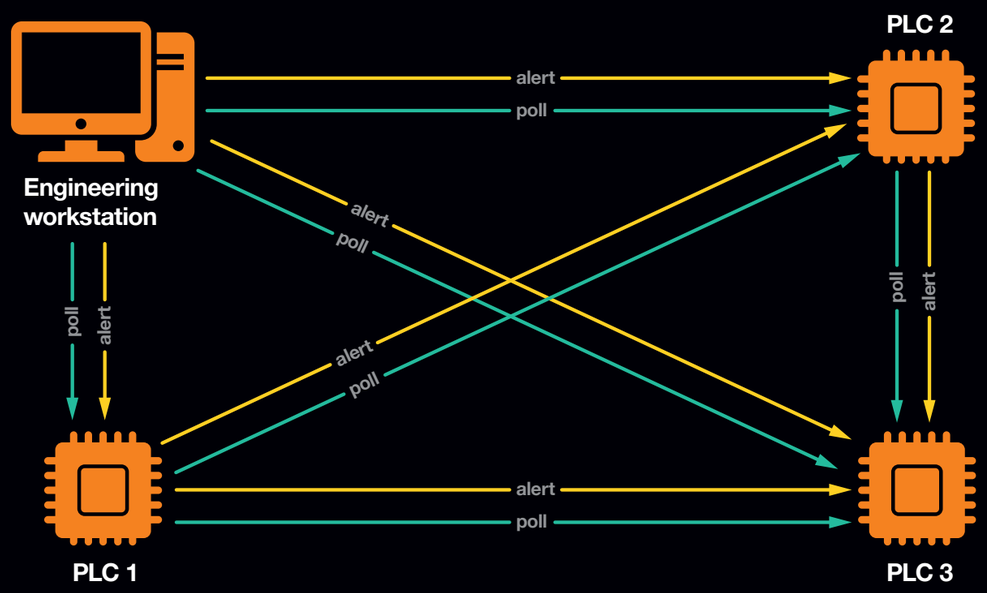
Dead Man's PLC takes advantage of this capability, as well as existing OT functionality and seldom-used security controls, to hold the victim's entire operational process and, by proxy, the physical world to ransom.

Dead Man's PLC works by adding to the legitimate, operational PLC code to create a covert monitoring network, whereby all the PLCs remain functional but are constantly polling one another. If the polling network detects any attempt from the victim to respond to the attack, or the victim does not pay their ransom in time, polling will cease, and Dead Man's PLC will trigger akin to a Dead Man's switch and detonate. Detonation involves deactivating the legitimate PLC code, responsible for the control and automation of the operational process, and activation of malicious code that causes physical damage to operational devices. This leaves the victim with no realistic option but to pay their ransom; their only other alternative recovery method is to gracelessly shut down and replace every affected PLC in their operational process, which will cost them in lost production time, damaged goods, and the cost of new materials.

It has generally been believed that OT-specific Cy-X presents an unlikely risk, due to the requirements placed on criminals from a technical perspective. The inability to easily recycle an attack across multiple environments also acted as a deterrent, due to the time and effort required to attack each victim. However, we think that Dead Man's PLC is an effective and pragmatic technique for holding the entire operational process to ransom. Most importantly, Dead Man's PLC acts as a starting point for defenders to rethink the risk ransomware and Cy-X could pose to OT, beyond the current surge of IT TTPs and type 1a Cy-X we see today.

If you'd like to read more about Dead Man's PLC and how it works, its dedicated research paper[93].

The Dead Man's PLC process



Dominic White
Managing Director South Africa
Ethical Hacking Director
Orange Cyberdefense

Pentesting and CSIRT stories

Hack the Planet!

We love bringing you tales of fresh hacks in each Security Navigator, and while we've got a new batch of interesting and unexpected stories for you, I wanted to take a moment to talk about why we do it.

There's a strange dissonance to being a hacker - spending your time finding strange and unexpected ways of manipulating systems interactions and functionality to make them perform unauthorised computations then making the jarring shift out of the rabbit hole into an industry that proffers best practices you know would rarely meaningfully impede your ability to manipulate these systems. This is why we share these stories, to help you see what we see - how systems fail when faced with a human adversary. Only by doing this, will we ever conceptualise a real model for how to build resilient systems.

There's another reason too - it's thrilling. One of the best things about this work is that the people who do it only develop their expertise through having spent far too much time sitting in front of a computer. What drives them is the enduring thrill of the hack. And while our industry continues to successfully embrace automation, there remains something truly magical about watching an artisan engage in this work - and the results are equally so. It's rare to be able to harness enjoyment into a public good when so often it's hidden from view. We hope you get a sense of what it's like crowding around the desk (or chat channels) of our peers as they plumbed these depths.

I leave you with the enduring words of Dade Murphy:
Hack the Planet!

CSIRT story: A close cut for Conti

As is often the case, the balloon went up late afternoon when a client called us to say they had noticed some behavioural anomalies on one of their Domain Controllers (Group Policy Objects had been deleted and the DC had unexpectedly rebooted). Fortunately, the client exercised an impeccable response procedure by isolating the server and calling the Orange Cyberdefense hotline!

Gordon Brebner, Senior Incident Response Analyst, **Orange Cyberdefense**

1 They come out at sun-down

By the early hours of the evening, the CSIRT had deployed XDR to the client's network and gained real-time visibility of the situation.

Quickly the CSIRT found the attackers were still active on several servers, including their initial foothold (an internet facing webserver) and an application server communicating to the internet over a Sliver malware C2 channel.

2 Working the night shift

CSIRT analysts worked throughout the night to effectively identify and contain the attackers, utilizing advanced AI tools to isolate all compromised servers and to deploy prevention rules to stop any further execution of malicious tools.

As dawn broke, the team were confident they had contained the incident and could switch to a more forensic style of investigation.

3 How did they get in?

Having collected and analyzed a plethora of digital forensic artefacts from affected servers and network devices, the CSIRT discovered the attackers (probably linked to the infamous 'Conti' Ransomware-as-a-Service group), gained initial access to the client's network by exploiting a known vulnerability on an internet facing webserver to deploy a publicly available web shell script.

4 I'm an admin, let me through!

The attackers enhanced their persistence and elevated privileges by creating their own highly privileged accounts that allowed them to move freely throughout the network, deploying Sliver malware C2 payloads on various servers, eventually gaining access to a Domain Administrator account.

5 Restoring security the very last minute

The attack culminated in the attackers disabling firewall settings and deleting Group Policy Objects on a Domain Controller to deploy various malicious tools, including commercial software for remote access, a Sliver malware beacon for C2 and a Conti ransomware payload. Fortunately, the collective efforts of the CSIRT and the client thwarted all attempts by the attackers to execute the ransomware payload and achieve their final objective.

Lessons learned

An understanding of what abnormal network behaviour looked like led to the fast isolation of a server and the seeking of assistance from the Orange Cyberdefense CSIRT. This is an important lesson and stands to highlight how good preparation can lead to fast containment actions – and ultimately limiting the damage.

The rebuild of critical systems prior to CSIRT involvement is a risky move and often impairs an investigation. Fortunately, in this case the client had backed up copies of the affected systems in a known-compromised state, allowing us to collect the necessary evidence from them.

Due to the obscurity of the vulnerable webserver component, in this case it is likely standard vulnerability scanners would not have identified the outdated software. This highlights the importance of penetration testing, in particular one using a black box methodology, to show the organization how an attacker would scope out an attack on the network.

CSIRT story: SEO-optimized compromise

Considering everyone's favorite search engine is a common thing to do. That applies to home use as well as the work place. But attackers know this as well, and leverage this fact to prey on the unwary. This example shows how manipulated search results set in motion a chain of events that ended in a serious incident.

John Askew, CSIRT Analyst, **Orange Cyberdefense**

1 "Is a handwritten receipt legal?"

That is a legit question, right? Pursuing an answer the user asked Google and was presented with a couple of answers.

Among the top links presented happened to be a forum, which helpfully offered a .zip file for download. Others had already responded and found it helpful, so what can go wrong?

2 Lucky, lucky, the answer is in the zip!

The user downloaded the .zip and opened it. Unfortunately, instead of the answer to the question it contained the infamous hacking/ remote administration toolkit Cobalt Strike. At this point the attackers could establish complete control over the users laptop.

3 Dogs that don't bark may bite all the harder

Just 20 minutes after the initial infection the reconnaissance tool Bloodhound was executed by the attackers.

Following that some more tools like ADTimeline, PowerSploit and Advanced IP Scanner were installed to sniff out the network and move laterally, identifying critical servers...

4 I think I'm Rclone now

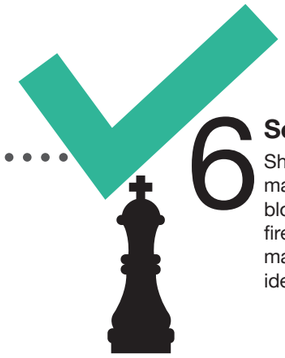
Within a few days data is removed from the servers en masse by the attackers deploying the commercial file copying tool Rclone.

At that point a third party alerted the customer's IT that there was potential C&C traffic from 3 specific servers: 2 domain controllers and a file storage. **CSIRT is called in immediately.**

5 Catch them by the endpoint

Immediate deployment of EDR monitoring and analysis tools revealed the attack chain and initial attack vector.

The Cobalt Strike beacons could be extracted and compromised servers were identified, isolated and cleaned.



6 Security restored

Shortly after that all malicious traffic was blocked at the perimeter firewall, and no further malicious activity was identified past this point.

Lessons learned

- Do not trust random search results. Google is among the most powerful search engines of the web, but hackers can and will use it to spread malware via SEO poisoning techniques as shown here. Raising awareness and training employees to identify such attempts is key in turning the human factor in cyber from a weakness into a strength.
- Be aware of Cobalt Stike. While it is by far not the only tool attackers use for first level compromise, it is among the most commonly seen. About 80% of the C&C traffic that we track involves Cobalt Strike.
- Endpoint detection and response capabilities are essential in identifying and containing incidents rapidly, hence minimizing the attacker's time window for stealing data or damaging critical systems.

Pentesting story: In third parties we trust

This security assessment was focussed on an Android application and an administrative web portal with the goal to identify security issues. From the administrative web portal, it was possible to create users and a user would receive a QR code to log in to the Android application.

Paul van der Haas, Security Specialist, **Orange Cyberdefense**

1 Credible QR

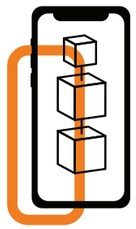
QR codes can be static and dynamic. The QR code itself consisted of user credentials and connection details and did not change.

This meant that if this QR was leaked, lost or stolen it could be used multiple times to log in as the user resulting in a higher impact if the QR code is compromised.

2 Digging into the APK

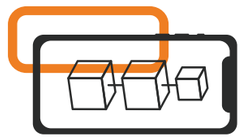
Moving to the Android application, which was available for anyone, the first thing we did was try to decompile the APK. We do this to understand the application logic and to identify sensitive data like passwords, API keys, API endpoints, etc.

The application did not have protections to prevent us from modifying (patching) the application with our mobile penetration testing tool Objection.



3 Meet our new app!

The modified application made it easier to intercept (HTTP) traffic. The analysis done on the decompiled APK and the intercepted traffic resulted in the identification of both an unauthenticated download of sensitive files and a possible way to inject SQL commands into the underlying database.

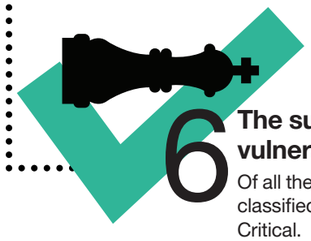


4 SQL injection, anyone?

Dropping modified SQL commands is better known as SQL injection and the vulnerability is older than some of our analysts are. The SQLi was quickly identified, but using specific payloads for full database compromise required the help of some experts. Luckily, we have a lot of knowledgeable colleagues!

5 Full remote control admin

The vulnerability gave access to multiple databases containing Personally Identifiable Information (PII) and a way to escalate privileges to the administrative web portal. The session tokens of administrators were extracted leading to a full compromise of the application remotely.



6 The sum of all vulnerabilities

Of all the findings, only one was classified (according to CVSSv3) as Critical.

Using CVSSv3 alone could give a false impression of the overall security as the attack chain described led to a full compromise of data and applications.

The sum of a few non-critical vulnerabilities can be as severe as a single critical one.

Lessons learned:

The Android application was built by a third-party and they were trusted to have the application developed with security built in. In these cases, one should:

- Include security as part of the requirements and design
- Evaluate third parties regarding their security methodologies and standards
- Verify if security is indeed built-in (security assessments)

Mobile applications are not magic. They can most often be reverse engineered and be tampered with. Make sure the applications are securely developed and hardened.

Pentesting story: Intercepting Communication in the Flutter Framework

During a recent assessment, the South African ethical hacking team assessed an Android Point-of-Sale (POS) application for a local bank. Generally, intercepting HTTPS communication from mobile applications is easily performed. However, the client's application was not cooperating in this particular case. We later learned that it was developed using the Flutter framework, notorious for making traffic intercepting difficult. However, not impossible!

Jacques Coertze, Security Specialist, **Orange Cyberdefense**

1 The Flutter Framework

At its core, Flutter is an SDK. This SDK exposes UI and other common elements (i.e., HTTP/S clients) that map behind the scenes to native equivalents in the Android and iOS spheres. The SDK achieves this through a combination of Dart and C/C++ integrations.

2 Diving into the Android SDK: Shared Libraries

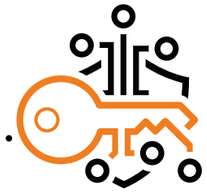
Android Flutter-based applications are primarily driven by two shared libraries: libapp.so and libflutter.so. The libflutter.so file contains the required functionality for using the OS (network, file system, etc.) and a stripped version of the DartVM. Meanwhile, the libapp.so file is a loader for the libflutter.so file. Both files contain an MD5 hash (the snapshot_hash), which uniquely maps back to the public GitHub repositories of the Flutter framework and Dart SDK.

3 Narrowing in on the SSL Verification Logic

We learned from the public GitHub repositories that the Flutter framework does not perform SSL certificate verification. Instead, it depends on a third-party SSL library known as BoringSSL. While scouring the public source code of this library, we identified that the SSL certificate verification logic resided in the /ssl/ssl_x509.cc file and the contained ssl_crypto_x509_session_verify_cert_chain function – a function that returns a Boolean indicating whether the SSL certificate is valid.

4 Penetration Patch

A public utility (reFlutter) exists that can patch any Flutter-based client application to bypass the SSL verification logic. It works very well. However, we wondered whether one could achieve similar results using the ever-popular Frida instrumentation toolkit.



5 I know what's on your memory!

Our research found that the Frida toolkit could indeed be used to map to the function in memory while the mobile application was running. However, we needed a signature whereby the function could be identified.

6 Full compromise

Using a reverse-engineering tool (Ghidra), we managed to track down the starting bytes of the function. We ultimately wrote a custom Frida script to dynamically hook into the function and bypass the SSL verification logic. Thus, serving as yet another method whereby this could be achieved.

Lessons learned:

Some lessons that could be learned from this exercise:

- While the Flutter framework does make traffic interception difficult, it does not serve as a silver bullet solution for keeping attackers away.
- Developers should always work on the assumption that their applications' network traffic is visible and could be tampered with.
- Implement adequate anti-tampering and debugging routines in mobile applications to prevent attackers from modifying the shared libraries or memory contents at runtime.
- Always ensure that sufficient server-side validation is present for any client-supplied data – work on the assumption that data originating from the mobile application is unsafe by default.

Charl van der Walt
Head of Security Research
Orange Cyberdefense

Research:
Fake News and False Positives

Every year since we started the Navigator project, we've kept track of the ratio between confirmed 'True Positive' findings, and 'Other' Incidents statuses like False Positives, Unconfirmed, and others.

Over the years since, our CyberSOC teams have also been integrating worldwide operations, upgrading platforms, introducing new detection technologies, enhancing processes, and generally improving the depth and breadth of our capability. This continuous internal evolution can make tracking a single metric (like the True Positive / False Positive ratio) tricky. Nevertheless, by normalizing our incident data as far possible over time, some clear and compelling patterns emerge.

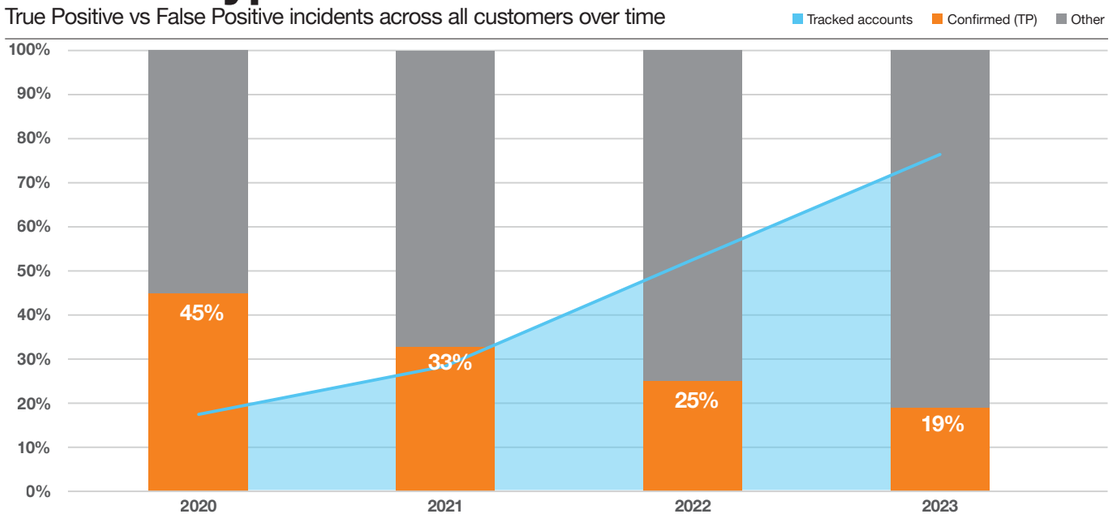
Research Question:

How does the age of a customer effect incident proportions?

We find that Incident volumes grow rapidly as more security telemetry is added. False Positives grow more quickly than Confirmed Incidents, but the longer our clients remain in our service, the more efficient and effective becomes, until we reach highly optimized level of accuracy.

Incident type over time

True Positive vs False Positive incidents across all customers over time



The chart above illustrates the increasing number of incidents and the changing ratio between Confirmed and Other incidents we've been observing over the years. We see clearly how Incident volumes have increased (from 39,000 to 129,395) as the clients in scope per year increased by 343% between our 2020 and 2023 datasets.

But we can also see how the proportion of True Positive (Confirmed) incidents has decreased from 45% to 19% of total Incidents over the same period.

CyberSOC Operations

Our CyberSOC teams note the same ratio of Confirmed Incidents that we do. They define a Security Incident as follows:

"Any potential or proven, undesirable and/or unexpected event, impacting (or presenting a capacity of impacting) information security in the criteria of Confidentiality, Integrity, and/or Availability".

Since April 2022, we have tightened up our definition of a 'Confirmed' True Positive Incident, which requires us to receive specific confirmation from the Client. A high number of Incidents impacts the CyberSOC - not the client - as our analysts review each Incident before it is raised. Automation is used to reduce the load from common False Positives on the CyberSOC analyst, and centralized tuning process identify problematic use case to improve or remove.

Rigorous tuning is essential to both the client and the Service Provider, and regular tuning noticeably improves detection efficiency. But tuning to improve efficiency without compromising effectiveness requires a close cooperative working relationship with the client. We'll show later in this section how clients who have retained our services over time and are able to provide feedback on the Incidents we raise will have dramatically improved detection efficiency.

The client only ever sees the small number of 'Confirmed' Incidents reflected by the orange bars in the chart above. But the closer the relationship we have with our clients, the better we are able to tune and the more efficient the detection systems become.

The Usual Suspects

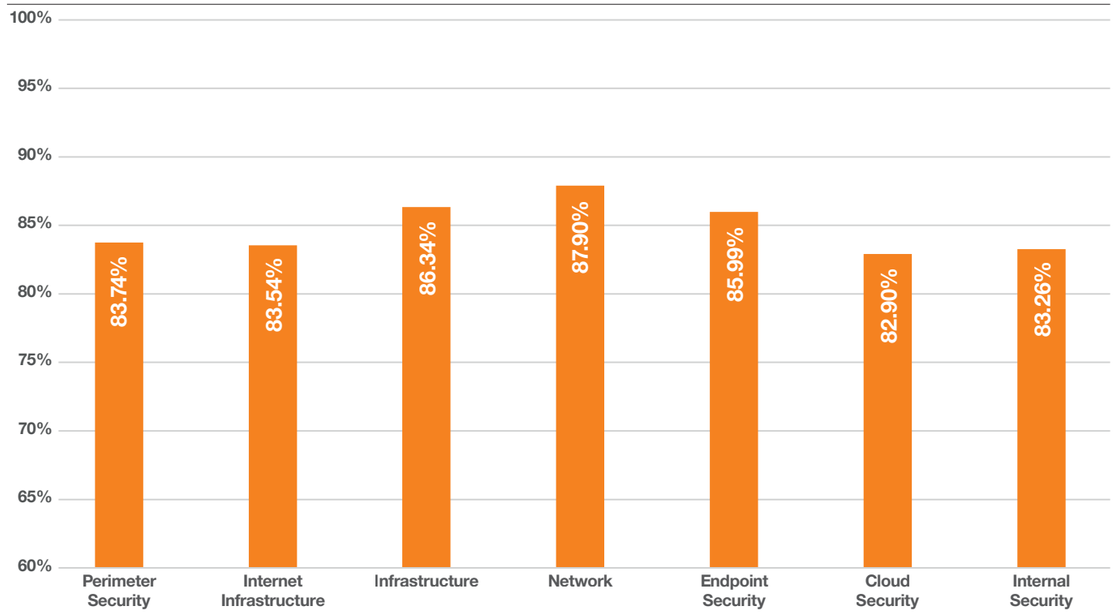
The detection domains listed in the chart below are described in more detail later in this report. The chart shows Other' (Unconfirmed) as a proportion of all Incidents for clients who have 60% or higher coverage for the domain illustrated.

We note that Unconfirmed are the most frequent for customers with significant coverage in the 'Network' and 'Infrastructure' detections domains. High levels of Endpoint detection coverage also correlate with high levels of unconfirmed incidents, while clients with high levels of 'Cloud' visibility experience the lowest levels of Unconfirmed incidents.

It's important to note however that the levels shown below are correlated with high levels of visibility, but are not necessarily caused by it. There are of course other factors that contribute the level of detection efficiency we deal with from client to client.

False Positive level by detection domain

Proportion of incidents classified False Positive for different detection types



Why so much?

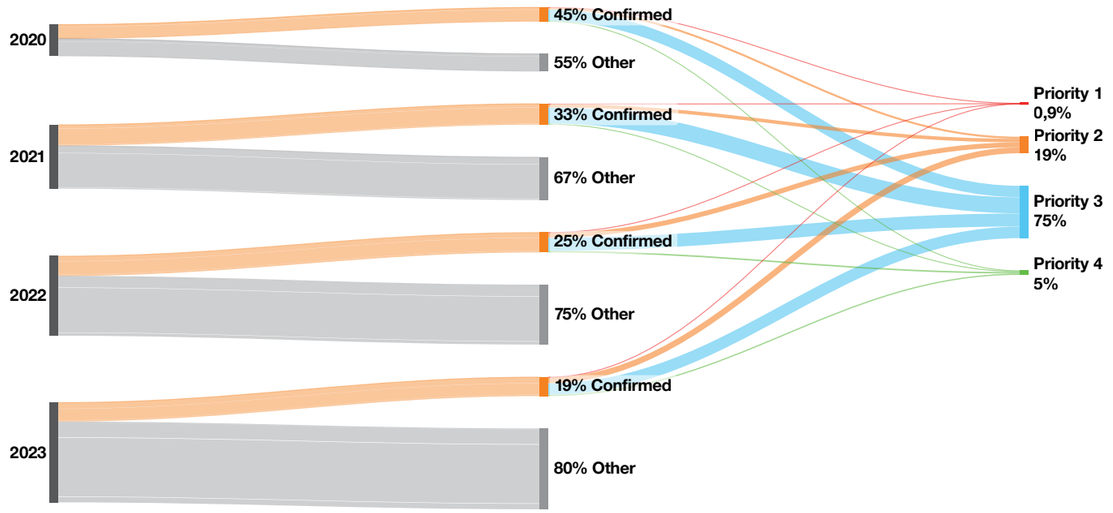
It's natural to wonder about this apparently low proportion of Confirmed Incidents. So, we investigated further, and three observations present themselves.

1. Quantity vs Quality

The chart below once again shows how the proportion of 'Confirmed' vs 'Other' Incident Status from our dataset has decreased from 45% to 19% over the past four years.

Incident priority flow by year

Proportional criticality of True Positive incidents across all customers over time

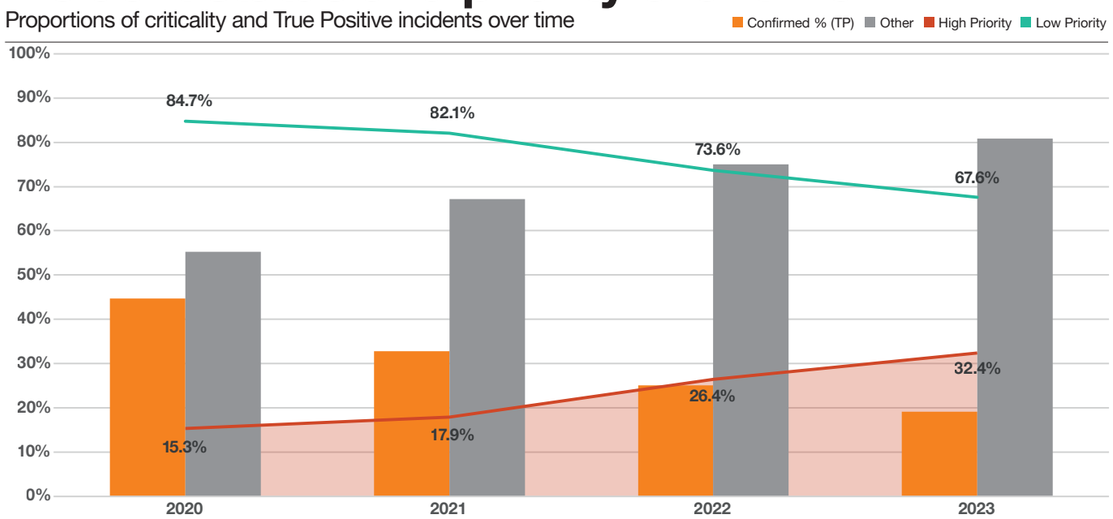


It's clear from the Sankey Chart above that most Incidents are not considered Confirmed True Positives. Of those that are, most of them are assigned a level 2 or level 3 ('Medium') priority. The chart also clearly illustrates how the proportion of True Positives has sunk over time.

To better understand this dynamic, we grouped Incident Priorities into 'High' (Priority 1 and 2) and 'Low' (Priority 3 and 4). The chart below shows how the ratio between High and Low Priority Findings has changed over the years.

Incident status and priority over time

Proportions of criticality and True Positive incidents over time



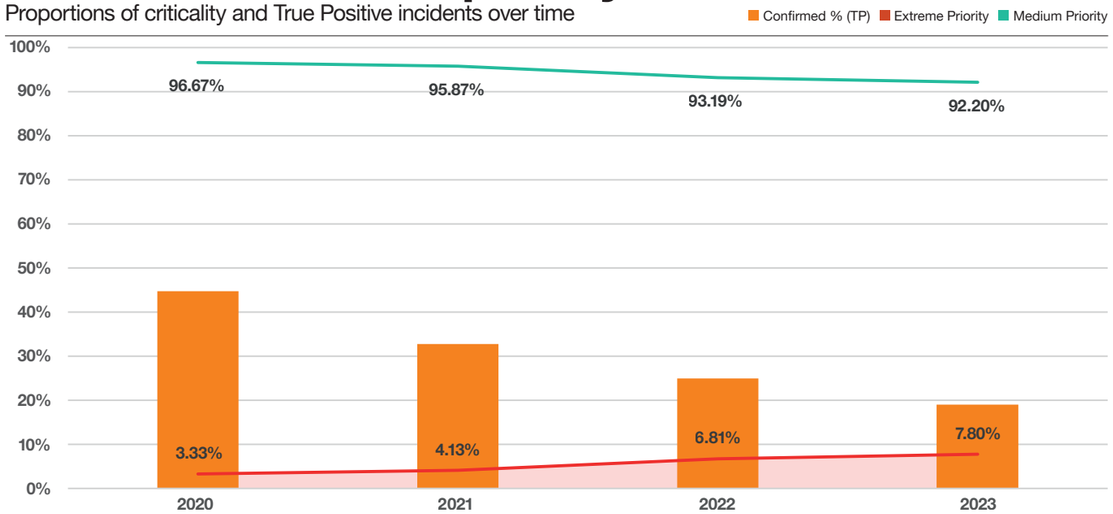
We see again how the proportion of 'Confirmed' vs 'Other' Incidents has decreased over time. However, by tracking ratio between High and Low priority incidents over the same time, we can also see how the proportion of 'Low Priority' True Positives (level 3 & 4) has decreased, while the proportion of 'High Priority' True Positives (level 1 and 2) has increased.

While Low Priority Incidents have become less common (84.70% in 2020 vs 67.60% in 2023), the proportion of High Priority Incidents has grown from 15.30% to 32.40% over the same period.

A similar period emerges when we track the occurrence of 'Medium Incidents' (Priority 2 and 3) versus 'Extreme Incidents' (Priority 1 and 4):

Incident status and priority over time

Proportions of criticality and True Positive incidents over time



The prevalence of 'Extreme' priority Incidents has almost doubled over the last two years. This reflects a more acute and considered prioritization process, with a lower tendency toward more generic 'Medium' priorities like 2 and 3.

This clearly shows that the volume of Confirmed incidents we report is shrinking, while the Severity of the Incidents we report is increasing.

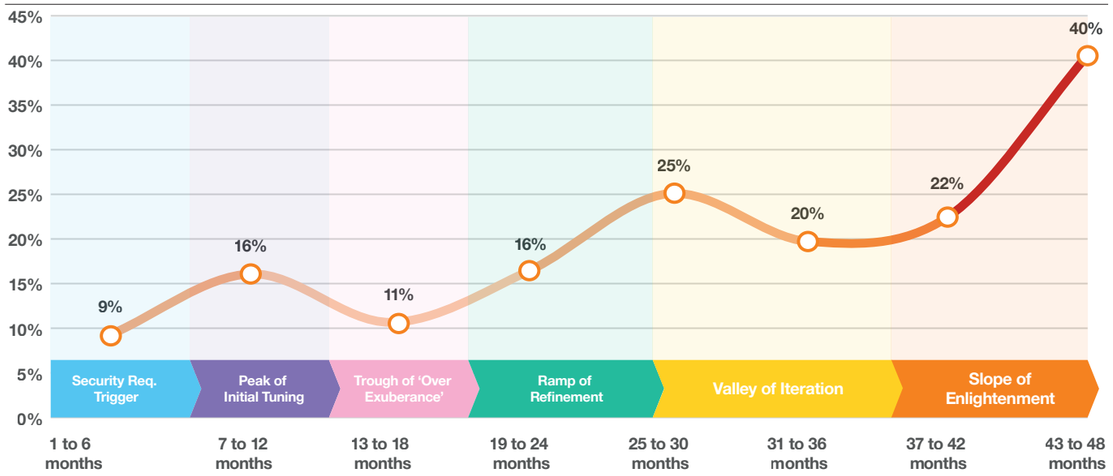
Seen together we believe that these two trends suggest a general maturing in the discipline of Threat Detection. Despite increased security event data and visibility, competent Cyber Security Operations Centers are becoming better at filtering out noise and bringing only confirmed, relevant and urgent incidents to their customers' attention.

2. Age and Wisdom - The Threat Detection Maturity Wave

'Waves' and 'Cycles' are all the rage in the research and analyst worlds these days, and as it happens a very compelling 'wave' with familiar properties emerges when we consider how detection efficiency changes as our clients mature with us.

Threat Detection Maturity Wave

Percentage of confirmed incidents relative to customer age



Our engineers typically recommend starting with the larger alert sources that may require more tuning effort, so we can maximize the time we have to do so - usually firewalls, AD, Sysmon; leaving lower impact but high data sources like DNS until the end. The repeated processes of adopting and tuning new data sources results in the cycle of waves we see illustrated in the chart above:

1. Security Requirement Trigger [Month 1-6]

A new client decides to engage with us because they consider Threat Detection to be a necessary security capability and consider a Managed Security Service to offer positive ROI. Upon signing a contract, we commence a structured onboarding process to deploy the required technology and start collecting events from in-scope security event data. The efficiency of these initial sources is low (around 9%), but quickly improves as the detection tuning process commences.

2. Peak of Initial Tuning [Month 7-12]:

As tuning efforts proceed, the value of the initial data sources improves, increasing to 16% within the 1st 12 months of deployment. While this number is still quite low, the customer starts to receive high-value alerts, and gets excited by what the service can offer. The overhead associated with the remaining False Positives never impacts the client because our CyberSOC analysts triage and vet every alert. As per the agreed schedule, onboarding of additional data sources commences.

3. Trough of 'Over Exuberance' [Month 13-18]:

After the value proposition for the CyberSOC service becomes clear, and service delivery has stabilized, additional data sources are added. The initial efficiency of this new security event data is sub-optimal, dropping all the way back to 11%,but tuning commences and efficiency rapidly starts to improve.

4. Ramp of Refinement [Month 19-24]:

Over this 6-month period tuning on the increased set of event sources continues, immediately bringing improved efficiency. At the end of this period False Positives are significantly reduced and efficiency reaches 26%.

5. Valley of Iteration [Month 19-36]:

It appears that customers will go through an additional cycle of security event data onboarding and tuning. This results in another efficiency dip to 20%, before tuning results in a new efficiency high of 28%.

6. Slope of Enlightenment [Month 36 and beyond]:

Although we may anticipate some further troughs and peaks as changes occur in our service offering or in the client's environment, we note that detection efficiency rises to around 40% after 3 years.

Over 60% of clients in the age group older than 3 years have an efficiency rating of over 30%. Those that are four years old even have efficiency levels of 45% and above.

At this maturity, efficiency is much higher than the average of 19% over all customers in the 2023 report year. Achieving the optimal balance between Efficiency and Effectiveness in Threat Detection is a journey that can take several years to complete. A healthy working relationship with a capable security partner, whether in-house or external, is clearly essential to ensuring optimal results over time.

3. The unknown Unknowns

As mentioned earlier in this section, our distinction between ‘Confirmed’ and ‘Other’ Incidents masks a deep pool of complexity. Aside from True Positives our analysts record False Positives, True Legitimates, and ‘Unknown’ outcomes. The Unknown outcomes indicate tickets where we have not received any feedback from the client, leaving us unable to determine whether an Incident was legitimate or not. The alerts we raise with our customers are carefully analyzed and vetted and only raised with the Client when we have high level of confidence in them. Still, we can often not be completely certain until we have received confirmation from the client.

We only mark Incidents as ‘True Positive’ when we have specific confirmation from the customer that a real security Incident confirmed.

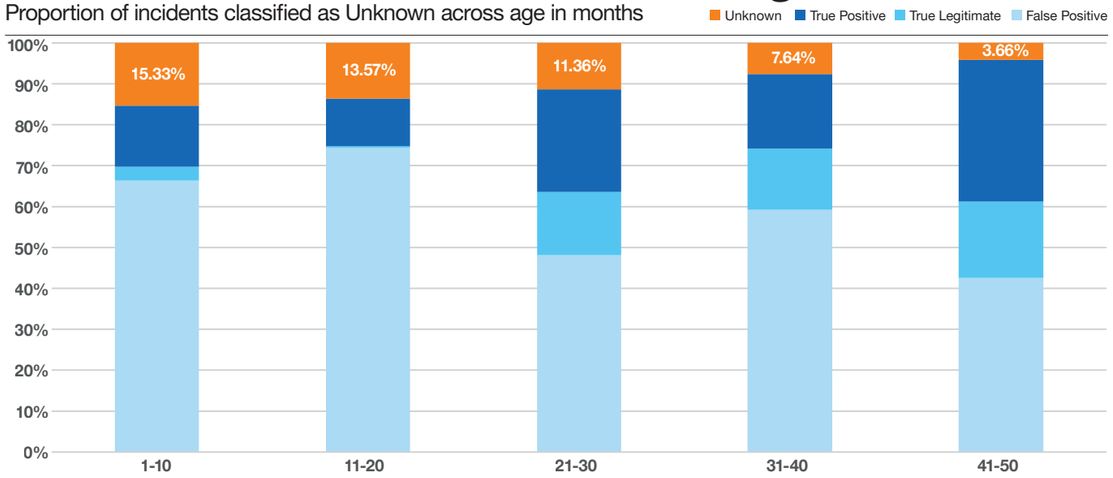
As it happens, this confirmation very often doesn’t come, and so the Status remains ‘Unknown’ in our records. In the analyses presented in this section, such ‘Unknown’ incident outcomes fall under ‘Other’ and may therefore skew the true prevalence of Confirmed True Positive Incidents.

If Unknown incidents were simply classified along the same proportions as the rest of our events, True Positive Incidents would increase to 22% of the total.

Our CyberSOCs have noted that there is a strong correlation between the detection efficiency of a client, and the degree of feedback we get from the client. This is clearly illustrated in the chart below, which once again looks at Incident Status relative to amount of time a client has been with us:

Distribution of Status vs. Client Age

Proportion of incidents classified as Unknown across age in months



As this chart shows, the longer a customer has been with us, the lower the level of ‘Unknown’ Incident statuses becomes. We’ve noted previously that at this ‘Age’ the detection efficiency of client accounts could be twice as good as the average (45% or higher). It seems to us therefore that the three variables are correlated.

It seems to us therefore that the three variables are correlated:

- client ‘Maturity’ as reflected in the ‘Age’,
- the level of feedback on Unknowns, and
- the detection efficiency.

And it might be the level of feedback that drives the efficiency, rather than other way around: As our client’s ‘mature’ in their consumption of the service they improve their ability to act on the Incidents we raise with them and refine the process of providing us with feedback. With sufficient feedback we are able to perform intelligent tuning and thereby improve detection efficiency, in a repeating cycle.

Our CyberSOC operations strongly emphasize how important it is that the Client works together with their Security Service Provider in a mature, transparent and trusting manner.

With strong bi-directional communications the service can improve much more rapidly, resulting in higher efficiencies and better security outcomes.

Summary

It is clear that the efficiency of our detection operations (as expressed by the proportion of potential Incidents that are labelled as ‘Confirmed’ by our analysts) is decreasing over time, although we must emphasize that this categorization has a huge blind spot in the form of Incidents we report but get no feedback on. We argue that this is the natural and inevitable consequence of increased levels of visibility, as expressed by our rudimentary ‘Coverage’ metric.

We note, however, that a decrease in apparent efficiency is not a bad thing, especially for Clients who don’t have to deal with growing volumes of unconfirmed Incidents. Indeed, we show that while the ‘quantity’ of incidents we report to our clients has decreased proportionally over the years, the ‘quality’ (as expressed by the proportion of Confirmed High Priority Incidents) has actually increased. We argue that this is a function of detection tuning, more rigorous analysis, and other service enhancements.

We illustrate how an overall ratio between Confirmed and Other Incidents is actually misleading, as this ratio varies greatly from Client to Client. Indeed, as we examine this variance, we observe that the efficiency of mature, established clients can be four times higher than that of new Clients who are just starting their onboarding journey with us. We believe this client maturity is strongly expressed in the frequency with which we receive feedback on the Incidents we raise. The more regular and detailed feedback we receive, the better our tuning and analysis becomes, and the more detection efficiency improves.

Finally, we introduce the ‘Threat Detection Maturity Wave’, which captures the repeating phases of data ingestion and tuning that ultimately lead to a plateau of productivity where Confirmed Incidents constitute almost half of all processed events and appear to continue trending gradually upwards from there.

Research Question:

Is more security visibility better?

Adding more telemetry to a detection capability undoubtedly increases the 'effectiveness' of the program (the number of incidents that will be identified), but also decreases the 'efficiency' (the ratio between Confirmed incidents and 'noise').

Covering our Assets

Since last year we have attempted to assess the level of coverage our clients have in terms of detection capabilities. The idea is to get a sense of how much potential security telemetry we are actually 'seeing'. As we are an external provider to our clients, the amount of security telemetry we have access to varies greatly.

Further detail on the extent of our coverage scores is provided in the research notes - Extent of our Threat Detection Coverage Assessments over time.

This process is imperfect and incomplete, but we believe it is a first step toward providing some essential context around our CyberSOC incident data.

Since each client can be assigned a maximum of 5 'points' for coverage in a given domain, we can assess how much visibility we have across our clients relative to the visibility we'd 'like' to have in each domain.

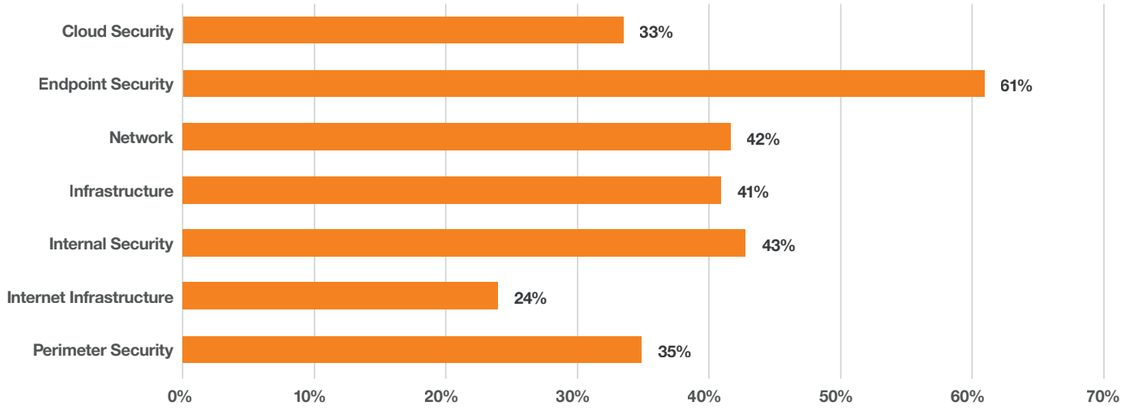
Perhaps unsurprisingly, we assess that we have the highest degree of visibility into our clients' 'endpoint' telemetry, which includes EDR, Sysmon and other endpoint security solutions. The lowest degree of visibility is reported for 'Internet Infrastructure' on the other hand.

What we can see

As there is no hard quantitative means of deriving the level of coverage, we rely on a manual assessment involving the people who work directly with the client.

Insight per detection domain

Actual visibility as a proportion of total potential per detection domain



Is more less?

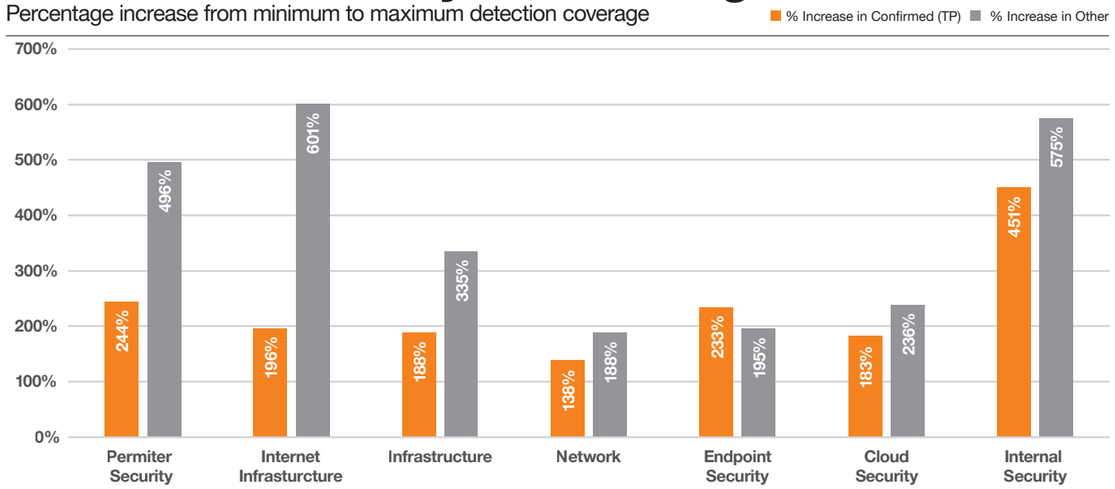
We've argued elsewhere in this report that adding more telemetry to a detection capability undoubtedly increases the 'effectiveness' of the program (the number of incidents that will be identified), but also decreases the 'efficiency' (the ratio between Confirmed incidents and 'noise'). Obviously, the amount and type of telemetry we are monitoring for our clients will have a significant impact on the volume and type of incidents we are reporting, including the ratio of 'Confirmed' to 'Other' incidents.

Detection efficiency can be improved with careful tuning over time, but efficiency appears to drop as Coverage increases. Thus, the trade-off between effectiveness and efficiency in Threat Detection appears to present as another immutable law of cybersecurity.

This immutable principle has varying impacts in different domains of detection, however, as the chart below illustrates:

Detection efficiency vs. Coverage

Percentage increase from minimum to maximum detection coverage



As we can see from the chart above, 'Confirmed' Incidents generally increase more slowly than 'Other' incidents as Coverage increases.

But in our dataset there are some exceptions, notably:

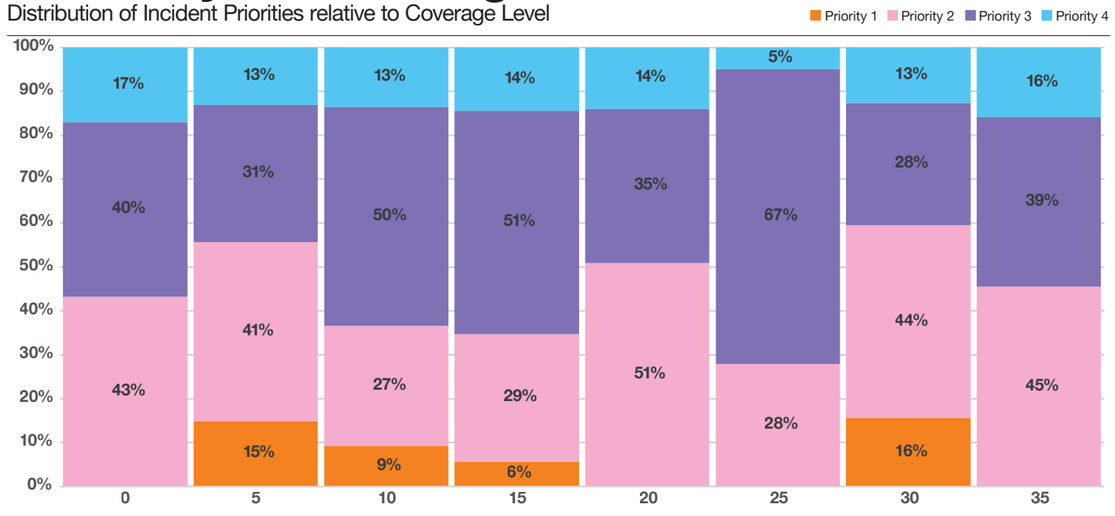
- 'Network' detection includes Internet traffic, Internal East/West Traffic and Network Traffic Analysis (NTA). As we increase detection in this domain, we observe Confirmed Incidents increasing much faster than Others.
- 'Endpoint' detection includes Anti-virus, EP/EDR, Sysmon and MS Defender. In this domain, Confirmed Incidents increase at 233% while Other incidents only increase at 195% as Coverage increases from Minimum to Maximum levels.

Getting more serious

How does the Priority assigned to Incidents change with Coverage? The chart below depicts the proportion of Incidents at each Priority level for Confirmed Incidents, relative to the assessed coverage score of customers on a scale of 1 to 35:

Criticality vs. Coverage

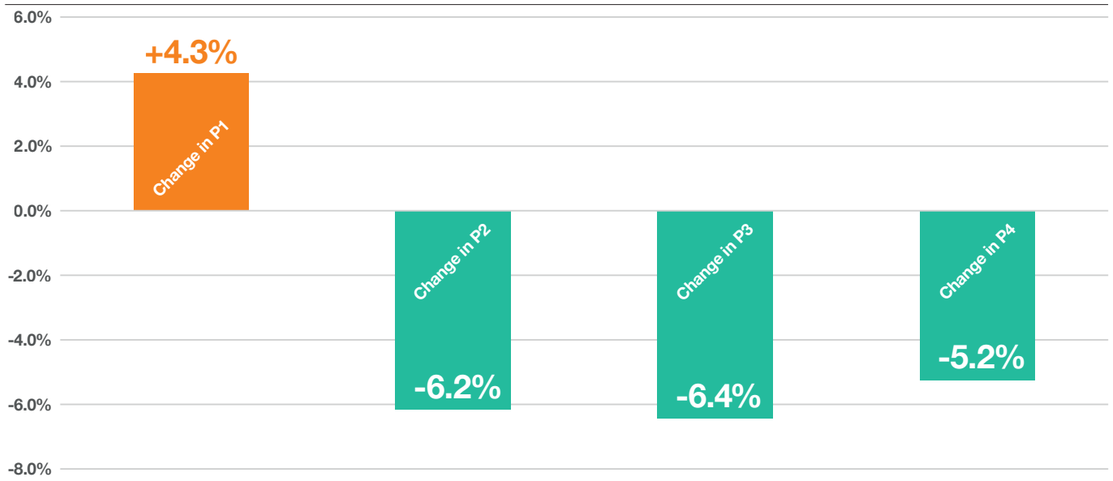
Distribution of Incident Priorities relative to Coverage Level



There is clearly some variance in the distribution of priorities as coverage changes. These peaks and dips probably have more to do with specific attributes of the client then other factors. However, when we look at the difference in each Priority level as coverage increases, we note that some Priority levels vary more drastically than others:

Criticality delta vs. Coverage

Change in the distribution of incident priority as coverage increases



The chart above illustrates that, as our visibility into a client's security telemetry increases, the proportion of 'Low' Priority Incidents (Priority 2, 3 and 4) tends to decrease (by 6.2%, 6.4% and 5.2% respectively), while the proportion of Priority 1 Incidents increases (4.3%). Note that we observe significant variation here from client to client, so these figures should be considered with some caution.

Summary

It's interesting to assess how increased coverage impacts the quality and quantity of the Incidents we raise with clients. There's no doubt that the volume of Incidents increases with coverage – including Confirmed True Positives and Other.

It's harder to assess whether increasing coverage also changes the quality of the Incidents raised, but it does seem clear that the number of False Positives or Unconfirmed Incidents increases more quickly than Confirmed Incidents as Coverage increases.

We also see some evidence that the 'quality' of Incidents (as reflected in by the severity of Incident Priorities) increases with coverage. We caution however that the data used in this assessment has limited solidity and so present this finding as a thinking point, rather than a confident assertion of reality.

Research Notes

CyberSOC Data:
Defining Threat Detection 'Coverage' Scores

To gain a sense of how much of our clients' security telemetry we have access to, we derive a simple metric that describes the breadth and depth of detection coverage our clients in this dataset have. The 'coverage rating' scores are estimated by our Technical Managers closest to each client and range from 0-5 as explained below:

Coverage Rating Scores

0. No coverage
1. Minimal coverage
2. Some coverage, but less than recommended
3. Appropriate coverage, including all the basics
4. Good coverage, including the basics and more
5. Complete coverage

We assess the coverage level for the following detection domains:

Perimeter Security, e.g.

- Firewall logs,
- WAF Logs,
- IDS/IPS Logs,
- Email Gateway Logs,
- VPN / Remote Access Logs

Internal Security, e.g.

- AD / Authentication Logs,
- Firewall Logs

Infrastructure, e.g.

- DHCP Logs,
- DNS Request Logs,
- Web Server / Web Application Logs

Internet Infrastructure, e.g.

- Web Server / Web Application Logs,
- Web Proxy Logs

Network, e.g.

- Internet traffic
- Internal East/West Traffic
- Network Traffic Analysis (NTA)

Endpoint, e.g.

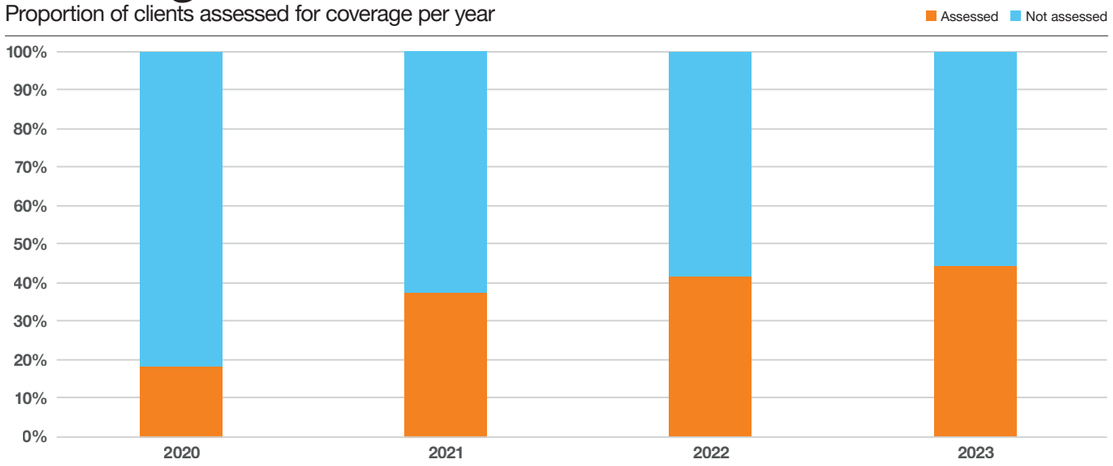
- Anti-virus,
- EP/EDR,
- Sysmon,
- MS Defender

Cloud, PaaS & SaaS, e.g.

- Azure - AD, Audit,
- KeyVault & VM,
- O365,
- Lacework and Mondoo,
- Palo Alto Prisma Cloud,
- Checkpoint Cloudguard,
- Platforms like Adaptive Shield

Coverage Assessment

Proportion of clients assessed for coverage per year



As coverage assessment is a manual process, not all clients have completed assessment scores at the time of writing this report. For the 2023 year, 45% of clients were assessed for detection coverage.

Cyberwarfare

What we know, what we predict and what you should be prepared for

When envisioning cyberwarfare, one might think of another Hollywood blockbuster movie, but it is in fact a concerning reality. The growing sophistication of these acts of cyberwarfare, combined with increasing aggressiveness by nation-state actors supported by non-state actors, could heavily impact countries around the globe.

Tamara Hendriksen, Information Security Officer
Jort Kollerie, Strategic Advisor
Orange Cyberdefense

What is Cyberwarfare?

The concept of cyberwarfare is difficult to define, and no absolute definition is widely agreed upon. There is an ongoing debate among scholars, experts and governments on the definition of cyberwarfare and the characteristics that should be included. There is the same ongoing debate with the term 'terrorism'. Researchers, over the years, cannot agree on a solid definition, also because tactics and technologies are ever-changing. This impacts the way we can define such concepts. Most definitions do consider the same elements to explain what constitutes cyberwarfare: nation-states, non-state actors (organizations), cyberattacks, (vital) information systems and disruption. An example of a definition used is: "the use of cyberattacks against a nation-state, causing comparable harm to actual warfare and/or disrupting vital computer systems".

Sometimes you will see different terms used interchangeably: cyberwarfare, cyberwar and even cyberterrorism. Some experts state that these terms describe the same situation. However, there is controversy on the way these terms are used. According to our research, using the term 'cyberwarfare' is to be preferred, as 'warfare' includes the techniques, tactics and procedures that make up the complexity of this term. It includes the engagement and form of war, acknowledging the fact that these cyber activities are often part of hybrid warfare. The term 'war' refers to a specific situation: a state of armed conflict between nation-states or groups within a country. A pure cyberwar is very unlikely to ever occur, as this would be a situation where conflict would be purely fought with "cyber weapons." Cyberterrorism consists of unlawful attacks on (critical) systems/networks that are politically, religiously or socially motivated. It can result in severe violence, intimidation or aims to generate a level of fear in society.

Research, however, shows us that cyberattacks on critical systems do happen, but are not yet conducted by terrorists or aiming at the damage and goals that would qualify as cyberterrorism. Therefore, when researching cyberattacks against nation-states, the term cyberwarfare is used preferably.

The advancement of technology has increased attention on the topic and the use of cyber activities in the geopolitical sphere can eventually lead to actual harm of civilians and critical infrastructure.

This is something that we see more examples of in the current world we live in. A good example is the war of Russia against Ukraine, where cyber activities play a big part in the overall warfare.

Types of Cyberwarfare

Nowadays, cyberwarfare is almost always part of a hybrid warfare, where it can pose a significant threat to a nation-state. cyberattacks can assist as a supporting means of traditional warfare. There is a difference between 'hard' and 'soft' threats, where hard threats can be seen as attacks on, or tampering with, systems/networks and soft threats are threats focusing on propaganda or espionage. Often, a combination of tactics and techniques is used. Types of cyberwarfare that can be identified are:

Espionage

This refers to the act of spying on another nation-state to obtain confidential or secret information. Traditional forms of espionage, as well as cyber-espionage, in and of itself are not an act of war, but these activities can be considered as an ongoing, standing situation between nation-states. Tactics, like using a botnet or spear-phishing attack can be used to gain access to systems.

Disruption

This refers to modern economic systems that rely on, often complex, computer systems and networks. Attacking systems of economic facilities like banks, stock markets, large multinationals or payment systems can give attackers access to funds or negatively impact the operations of a company or nation-state.

Propaganda

The use of the cyber domain to control information in all available forms to try to control the minds and hearts of people living or fighting in the nation-state that is being targeted. It can be considered as a form of psychological warfare, using fake news and social media. Doing so can expose embarrassing truths or spread lies that may cause people to lose their faith in their own country, or even sympathize with the enemy.

Sabotage

Not all threats originate from foreign groups or other nation-states. Third parties that you may work with, competitors or even insider threats (disgruntled/negligent employees) can cause serious damage by creating disadvantages or stealing confidential information and sabotaging daily operations.

Surprise attack

These attacks can be seen as having the same impact and effect on a nation-state as the events on 9/11 or Pearl Harbor. These are massive attacks that will catch an enemy off guard and might weaken their defences. It can be used to weaken the target and to prepare for follow-up attacks in a hybrid form. This type of cyberwarfare is debated among experts, as it is considered unlikely that one cyberattack can cause the same impact on a state as 9/11.

Information Warfare

A crucial component that is supporting cyberwarfare is called information warfare. With information warfare, it is the objective to gain an advantage over the opponent. Unlike traditional analogue warfare and analogue techniques, no large financial resources are needed yet to initiate information warfare; the vast knowledge of systems, networks, applications, and tooling are the only requirements. Some of the possible types/methods and/or tactics to gain an advantage over the opponent are:

- **Datamining:** from the early days of the internet, commercial companies (like Facebook, Apple, Google and Microsoft) offering online services have been able to collect huge amounts of data on citizens and organizations. Some government agencies are actually playing catch-up to collect that data as well, to use it to monitor citizens and society. This is mainly enforced by various regulations and legislation, with projects to tap data on a large scale;
- **Legal Arms Race:** between the West and the 'rest of the world', there can be considered to be a legal arms race. The West is 'bound' by digital regulations that curb activities like monitoring of citizens, and they must often deal with new or modified rules and legislation that are often countered by privacy activist groups. While some non-Western countries also have certain rules and legislation in place, in most cases, it is limited to the home country and does not focus on their foreign activities;
- **Spy Tech:** the growth and rapid adoption of digital technology, its solutions, products and applications have become indispensable in today's society. The origins of suppliers and manufacturers are from all over the world. They could play a conscious and unconscious role in the intertwining of technology between companies and governmental bodies;
- **Weaponization:** data on citizens, organizations and countries is being collected on a large scale. This information is usually publicly available (e.g., social media, search engines and other platforms), but data captured in hacks and dumped online also plays a crucial role. The effects of weaponizing data can be seen in for instance, election fraud and interference or mis/disinformation of news.

Attack timeline

	Target	Operation
2010	Iran	Stuxnet began to infiltrate and destroy the network of a nuclear enrichment facility.
2011	Netherlands	DigiNotar hack resulted in the compromise of CA servers & certificates.
2012	Saudi Arabia	Shamoon, nearly 30k systems wiped and caused major disruption.
2013	Belgium	Operation Socialist was enforced by GCHQ to breach the telco infrastructure of Belgacom.
2014	USA	The network of Sony Pictures got compromised and a vast amount of data got leaked.
2015	Ukraine	Russia triggered the first-ever blackout induced by a cyberattack, turning off the power of Ukraine.
2017	Global	WannaCry ransomware cryptoworm attack affected +/- 300k of computers worldwide.
2017	Ukraine	NotPetya, the data-destroying worm targeted Ukraine but caused havoc worldwide.
2018	Netherlands	Russians, with a car full of electronic equipment, plotted to hack the world's chemical weapons watchdog (OPCW) in the Hague.
2020	USA	Intrusion of SolarWinds Orion caused the boldest supply chain attack ever. This attack set thousands of organizations at stake.
2021	USA	Colonial Pipeline suffered from a ransomware attack that heavily impacted computerized equipment and disrupted gas supply.
2022	Ukraine	Prior to Russia's war against Ukraine, the country was under digital pressure and attacks.

Legend: Surprise Attack; Attack on industry/OT; Espionage/ intelligence; Disruption attack

The multi-domain battlefield

Over centuries, the battlefield has expanded from land, sea and the air, to now include the space and cyber domain. Related to this, today's world consists of the human landscape, physical landscape and information landscape. Combined, a multi-domain battlefield has been created. Within the multi-domain battlefield, cyberwarfare has found its place; it has become the most attractive domain for power projection in the world. This is indeed what we have seen in recent years and what can be considered to take dangerous forms.

Examples of substantial catastrophic situations have not occurred yet, but they may arise in the near future. Nation-states have always attempted to use new forms of technology in their use of warfare, so the same applies to the use of cyberwarfare methods. The threat lies in the expanding belligerence that nation-states are willing to deploy to strengthen their position in the geopolitical sphere. The possible effects of collateral damage, regarding this belligerence, will also greatly increase over time.

An important contributing factor here is that within the cyber domain, the defense does not know what the offence strategy, strength and/or capabilities are. Moreover, activities within cyberwarfare are often cost efficient and can be conducted almost in real-time. The added advantage on top of that is that these activities are often stealthy.

The usual suspects

To get a better understanding of cyberwarfare and how this is perceived around the globe, we have gathered 93 publications and reports over the year 2022. These documents were released by several governmental bodies and security vendors. The most profound finding is that 94% of the reports originated from western countries. The others (6%) originated from non-western countries. We can conclude that our perception on the topic of cyberwarfare is clearly shaped by the fact that these reports mainly focus on the threats originating from non-Western countries. Also, the majority of the reports that discuss cyberwarfare, describe which nation-states they perceive as the actors that form the greatest risk. These Countries can be found in almost all sources referred to as "usual suspects". Countries that can be expected to be on such a list and can be found in almost all of the sources. However, we can say with certainty that the battlefield of cyberwarfare is also shared with Western nation-states as well. When researching the cyber strength and capabilities of nation-states, the United States will almost always be on top of the list, as they have extensive offensive and defensive capabilities. An interesting fact is that we have seen an increase in more non-Western reports this year, albeit from their perspective of course. Whatever nation-state is the source of such a report, we must take into account that there is always a form of bias that may affect the information in the reports and the way we perceive it.

People's Republic of China "Panda"

+/- 136 APTs identified, most notable: APT1, Comment Crew, Comment Panda, Byzantine Candor, APT2, Putter Panda, Group 36, SearchFire, MSUpdater, 4HSCrew, SULPHUR, TG-6952, APT31, Storm-0558

Threat level: ■■■■■

Russian Federation "Bear"

+/- 49 APTs identified, most notable: APT28 (Fancy Bear, Pawn Storm, Sofacy, Strontium), CyberBerkut, CyberCaliphate, Sandworm, APT29 (Cozy Bear, Office Monkeys, Duke, CozyDuke, CozyCar, Nobellium), Turla APT (Snake, White Bear, Uroburos, Waterbug, Energetic Bear, Berserk Bear, Venomous Bear)

Threat level: ■■■■■

Democratic People's Republic of Korea "Chollima"

+/- 12 APTs identified, most notable: Bureau 121, Lab 110, Unit 180, Unit 91, 128 Liaison Office, 413 Liaison Office

Threat level: ■■■■■

Islamic Republic of Iran "Kitten"

+/- 42 APTs identified, most notable: APT33, APT35 (Charming Kitten), APT39, G0069, G0077, APT34 (OilRig, Shamoon, DarkHydrus, Helix Kitten)

Threat level: ■■■■■

Future

Attacks are borderless since IT (Information Technology) is distributed globally and we live in an interconnected world. IT/OT (Operational Technology) convergence and its associated risks can affect organizations accross segments and countries. Geopolitics dynamics will accelerate countries towards increased measures for digital resilience.

Computers are scaling, they get faster and will permeate all aspects in our lives. New techniques will also dramatically increase the impact of cyberwarfare on a global scale since there are limited obstacles in adopting it.

So, to speak, the evolution of technology will be followed by the use of more sophisticated attacks within the concept of cyberwarfare. Since there are no limits, the origin of the perpetrators requires international awareness and knowledge gathering of these emerging threats from across the world.

If cyberwarfare becomes the main mode of warfare of the future, we should be prepared for a global scale of impact on society. This is what is called collateral damage and since we live in an interconnected world and we cannot eliminate or prevent cyberattacks, we must focus on reducing the blast radius.

Conclusion

With many different opinions and views on the concept, what can we take away from research on cyberwarfare? There are a few things to consider within the cyber domain that may be of impact to cyberwarfare. It is important to address the effects of geopolitics; it is undeniable that political situations or changes in the geopolitical sphere between nation-states can impact cyber activities undertaken. Objectives and the changes in threats from nation-states or (state-sponsored) threat actors can be influenced by those changes in geopolitics and negatively impact the world.

Cyber activities are often borderless and limitless. In our modern world, we live in an interconnected world. It is often relatively cheap, anonymous, and stealthy to use cyberattacks to target other nation-states and create an impact. Organizations need to be aware and create an understanding that they sometimes can be the ultimate gateway in the execution of an attack. To be aware of your own position in the cyber domain and your relation to, for instance, governmental bodies, can aid in creating an assessment of the posed risk and the steps you might need to take in making yourself more cyber-resilient. Even though cyberwarfare activities are often aimed at nation-states, there might be collateral damage, when organizations and civilians are impacted in the supply chain or fall victim to one of the cyberattacks that may be part of a hybrid warfare.

Diana Selck-Paulsson
Lead Seurity Researcher
Orange Cyberdefense

Victims & Impact:

Hacktivism revisited

Hacktivist groups like Legions of the Underground, Anonymous and the Syrian Electronic Army have been a feature of the threat landscape for decades. Several individuals have also been responsible for personally motivated Denial of Service attacks or website defacements. Groups like Lulzsec caused mayhem in the name of their own brand of naïve, pseudo-moralistic messaging and groups like Guardians of the Peace are suspected to faux political fronts for cynical state-backed actors. Hacking, crime, espionage, politics and ideology have long been difficult to tease apart, and hacktivism has always been a central, if somewhat benign element of this complex mix.

But in the past 2 years we have seen an apparent increase of activity in the hacktivism space. Hacktivism can be understood as a form of computer hacking that is done to further the goals of political or social activism. It therefore calls the public's attention to something the hacktivist believes is an important issue or cause[94]. Often the cause is religiously or politically driven, and the hacktivist's goal is to disrupt services or otherwise using hacking techniques made visible to bring attention to a specific cause.

Research Question:

Have we experienced a big hacktivism surge since the war against Ukraine began?

Hacktivism incidents in 2023

The majority of hacktivism we have observed in the past 12 months cannot be described as 'major incidents', although this is of course a question of perspective. However, we are observing two significant trends.

First, we have observed a significant surge in hacktivism activity.

Secondly, we see how individual hacktivist groups are joining collectives that then enable them to tap into additional resources of this collective and hence increase their capabilities. Examples for this include recent #OpCountry operations such as #OpSweden, #OpAustralia and #OpFrance, in which hacktivists call out to their fellow hacktivists to join a campaign to attack targets in a certain country. Often sectors such as media, energy, governmental and telecommunications are affected by these attacks.

Until recently (or until the beginning of the war against Ukraine), hacktivism generally emerged in one of two extremes: truly impactful attacks or low-level disruptions. With the beginning of the war, the line between these two extremes began to blur, and at the same time a massive surge in activity could be observed. This was especially apparent after the hacker collective Anonymous declared 'war' on Russia[95] and the Ukrainian Minister of Digital Transformation Mykhailo Fedorov asked individual hackers on the internet for help at the beginning of the war[96][97], creating the first IT Army of Ukraine[98]. Again, collective efforts were used to increase the potential impact of hacktivist efforts.

Since then, attacks from hacktivist groups involved in the conflict, siding with either Russia or Ukraine[99], have reached unparalleled levels. But of course, hacktivist activity observed in the past 12 months is not only bound to the war against Ukraine, other geopolitical events have sparked the creation of new groups that are not engaged with the ongoing war. Most recently, new waves of hacktivist activity spurred after the Hamas-Israel war began anew.

These hacking activities are significantly inter-connected with each other, and with events occurring in the real world. Not only do we witness cyber events that impact the physical world; but we observe physical events that illicit a direct cyber response from Threat Actors, thus in turn causing an escalation of those very same geopolitical tensions. We see a new levelling of the physical and cyber battlefields, resulting in a very thin line between physical (war) and cyber (hacktivism) [100].

As Dr Vasileios Karagiannopoulos and Professor Athina Karatzogianni put it [101]:

"Contemporary events show us that hacktivism has become mainstream and is now an inevitable dimension of political conflicts, even those that end up in kinetic clashes between states, testing the virtual limits of symbolic, sensationalist hacks, vigilantism, cyberespionage, and even cyberwarfare."

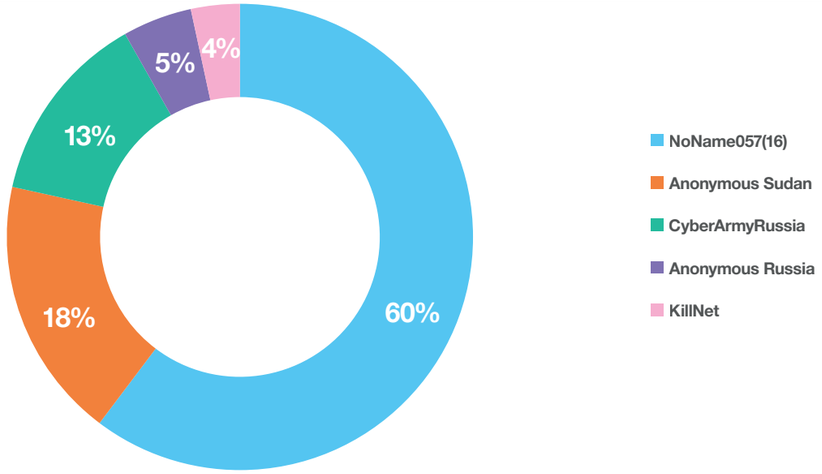
Hacktivist groups in support of Russia

Most of the hacktivist attacks that we are observing are Distributed-Denial-of-Service (DDoS) attacks. Simply put, DDoS attacks are when an attacker floods a server with internet traffic to prevent users from accessing connected online services and sites. Hacktivists target private and government organizations alike, and we have seen that hacktivist groups can take down even the biggest national or international websites. Some hacktivist groups have developed strong DDoS capabilities, while others are rather noisy about their capabilities and impact, applying a language and narrative that is disproportional to their actual action (and impact).

In both cases the result is Fear, Uncertainty and Doubt (FUD) – the escalation of anxiety, distrust, and disharmony – in an already tense and complex geopolitical context.

Top 5 (pro-Russian) Hacktivist Groups

As observed in the past 12 months (data contributed by Intel471)



Such FUD is emblematic of a continuous evolution towards 'cognitive' attacks, which seek to shape perception through technical activity. The impact has less to do with the disruptive effect of the attack or the value of the data or systems that may be affected (e.g. stolen, leaked or destroyed), but with the impact that the attacks have on societal perception, discourse and policy.

In the past 12 months, our research team has given special focus to tracking the patterns in these hacktivist operations, specifically pro-Russian hacktivist groups targeting Western organizations. Additionally, our team collaborated with Intel471, who have shared their data on current hacktivist activity with us. We used this data for the analysis shown in the following sections.

The chart above reflects all hacktivist groups that we observed operating in this context during 2023.

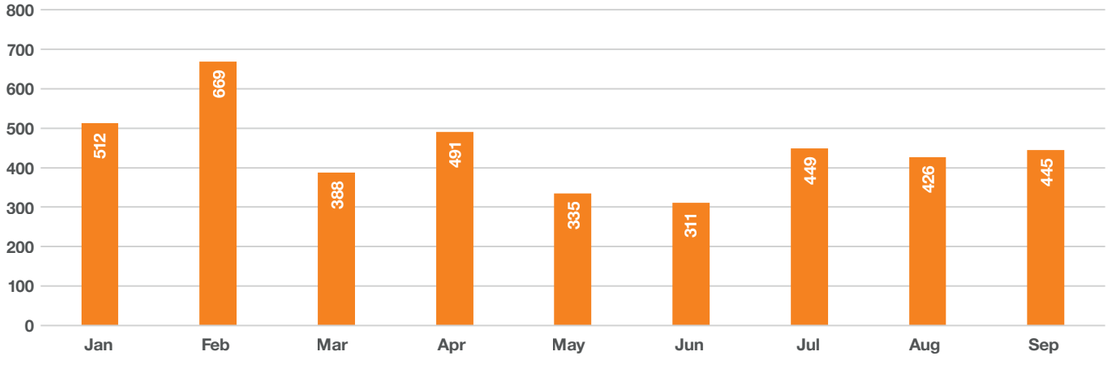
The tracking primarily relies on announcements these groups are posting in their publicly available channels. They often use messenger apps such as Telegram to either announce future victims or claim current victims. Motivation can vary from group to group.

In some cases, hacktivists use screenshots and links to prove responsibility for ongoing attacks, often using a 'check host' link, which is a tool for checking availability of websites, servers, hosts and IP addresses[102].

KillNet is an unusual case and should be understood as a hacker collective that shares common objectives with like-minded hacktivist groups. Groups that are believed to have joined the KillNet collective are: Anonymous Russia, Anonymous Sudan, Infinity Hackers Group, BEAR.IT.ARMY, Akur Group, Passion Group, SARD and National Hackers of Russia[103]. KillNet is really known for producing content on their social media channel. They don't execute many attacks themselves but work through members of their collective such as Anonymous Russia and Anonymous Sudan .

The highest level of hacktivism activity we have seen was in February 2023, as can be seen below. This corresponds with the emergence of hacktivist group Anonymous Sudan at the end of January 2023, who heavily targeted countries such as Sweden, Denmark, the Netherlands and Australia during February.

Hacktivism Activity 2023 (Q1 - Q3)

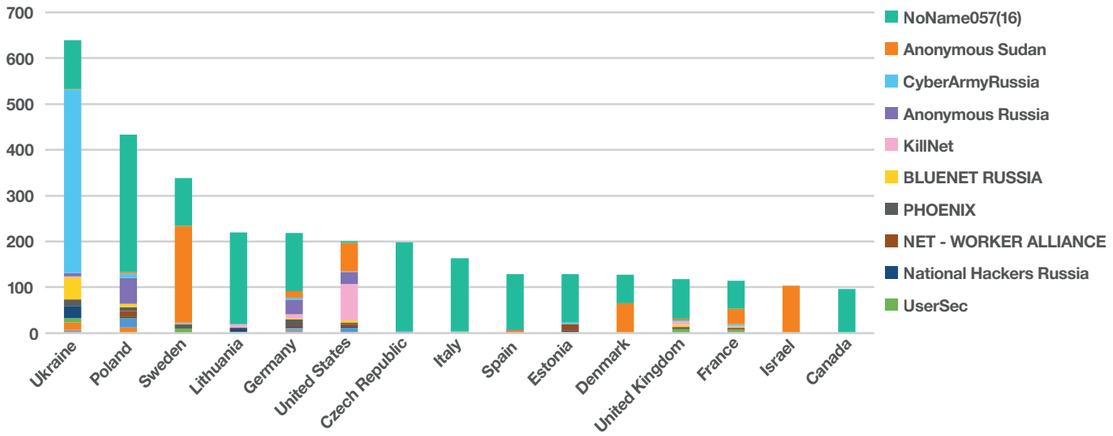


During 2023, countries that were impacted the most by pro-Russian hacktivist attacks were Ukraine, Poland and Sweden.

The focus on Ukraine is simply understood as the use of hacktivism as a tool in the war by Russia. The second most impacted country was Poland, which most likely is due to its geographical location. As can be seen below, the hacktivist group that attacked Poland the most is NoName057(16), which was responsible for up to 70% of all attacks against that country. Sweden has been the third most impacted country since the beginning of 2022.

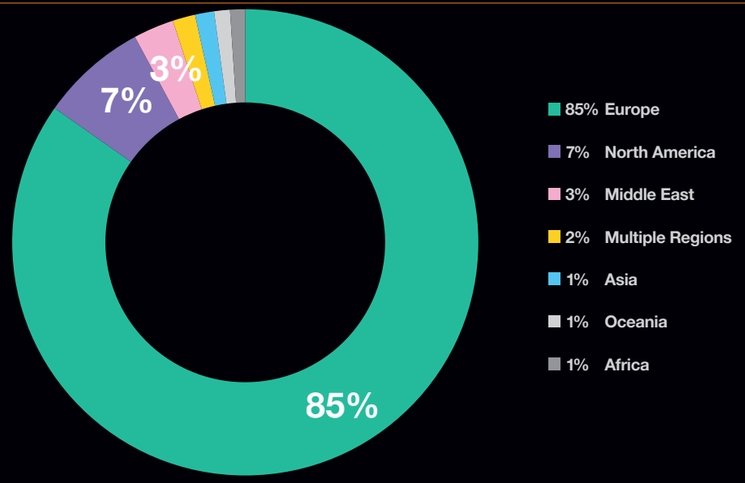
However, Sweden only emerged in our data between January and March 2023, when the hacktivist group Anonymous Sudan heavily attacked Sweden and Denmark. We will dive into the Nordics and our observations of Sweden's geopolitical situation in the cyber and physical world later in this chapter.

Active Hacktivist groups and their targets



Most affected regions

Zooming out to a regional level, we see that Europe was impacted by 85% of all attacks seen in 2023 (n= 4016), followed by North America (n=297) and the Middle East (n=113).



Who are the hacktivist groups and what are their motivations?

Two hacktivist groups that we have been tracking closely are Anonymous Sudan and Noname057(16). Both are directly or indirectly engaged with the ongoing war against Ukraine. NoName057(16) emerged as a direct response to the war and has been active since March 2022. They appear to be politically motivated. To reach a broader international audience, the groups launched an English-speaking Telegram channel in August 2022, which translates selected messages and announcements from their Russian channel to English.

Anonymous Sudan is apparently religiously motivated, but the group's activity and motivation are highly controversial, resulting in differing opinions on their origin, sponsorship and motivation. NoName057(16), on the other hand, state clearly that they are pro-Russian, and this is supported by their choice of language, narrative and hashtags such as [Russian flag] "victory will be ours". An interesting observation is that they've stopped using this phrase since the beginning of August 2023. Why they have removed the slogan is unclear at this point.

A brief look at Anonymous Sudan

Although Anonymous Sudan seemingly started their hacktivist activities in response to demonstrations addressing religion; they seem to have been distracted during late summer by other conflicts that appear closer to their base location.

As we stated earlier, the origin, financial funding and motivation of Anonymous Sudan is highly controversial[104][105][106][107]. We believe many clues point to the fact that they are indeed located in Sudan. However, that does not mean they do not support Russia. In fact, in their early days of January and February 2023, we believe that their attacks were most likely aligned with Russia's objectives to exasperate geopolitical tensions.

We explore what we have observed since day one of Anonymous Sudan's activities.

Anonymous Sudan created their Telegram channel @AnonymousSudan on the 18th of January 2023. Their first post read like this:

Later, Anonymous Sudan would change their purported motivation to attacking anyone 'opposing Islam'. Their Telegram channel was created 3 days before the burning of the Qur'an in Stockholm, Sweden on 21st of January. There is indeed an interesting correlation between the creation of the group itself and the first burnings in Sweden in 2023.

The January burning was the beginning of a chain of events which would complicate the ongoing application by Sweden to join NATO, but also lead to a questioning of the fundamental, democratic right of freedom of speech in Sweden and its tolerance for the burning of religious scripts. It would also increase the terror threat levels[108] in Sweden and spawn the introduction of a bill to ban the burning of scripts in Denmark. The full chain of events can be seen in the timeline on the next page.

The name Anonymous Sudan first mislead observers into believing the group was part of the notorious hacker collective "Anonymous". But that notion was quickly dispelled by the Anonymous collective themselves on the 19th of February, when they distanced themselves from Anonymous Sudan. This happened on the same day that Anonymous Sudan announced that they had joined the pro-Russian KillNet collective. One day later, Anonymous Sudan commented to the public, stating:

> "message to all the idiots who think that we are Russians, we are 100% from Sudan and regarding that we support Russia, yes we support Russia and we will continue to support it and we will not stop because they supported us and they supported Sudan before" (sic)
>
> Telegram message on 20/02/2023

A timeline of recent geopolitical events, showing pro-Russian hacktivist activity impacting the Nordics between January and August 2023

Physical world

27/01/2023
Rasmus Palludan, right-extremist, burns the Qur'an in Copenhagen[117]

22/01/2023
Turkey's president condemns the Qur'an burning and is not willing to support Sweden in it's effort to join NATO[109][110][111]

22/01/2023
Right-wing politician Edwin Wagensveld in the Netherlands tore up and burned pages of the Qur'an

21/01/2023
Rasmus Palludan, right-extremist, burns the Qur'an in Stockholm

18/01/2023
Anonymous Sudan creates their Telegram channel

16/06/2023
Sweden releases official press release on the 12th regarding a support package for Ukraine [112]

After 29th of June
The repercussions of the Qur'an burnings have extended beyond Sweden, as several countries, including Iraq, Kuwait, the United Arab Emirates, and Morocco, have summoned Swedish ambassadors in protest[114][115].

29/06/2023
Turkey's president condemns Qur'an burning in Sweden, signaling that this would pose another obstacle to Sweden's bid for membership[113]

19/07/2023
Iraqi police officers trying to disperse a protest outside the Swedish Embassy in Baghdad

20/07/2023
Iraq expelled the Swedish ambassador in response to another planned Qur'an burning in Stockholm[116]

28/06/2023
Salwan Momika, an Iraqi refugee in Sweden burns pages of the Qur'an

19/02/2023
Anonymous Sudan joins the pro-Russian KillNet collective

30/01/2023
Anonymous Sudan begins DDoS-ing Danish institutions because of the burning of the Qur'an

23/01/2023
Anonymous Sudan begins DDoS-ing Swedish and Dutch institutions because of the burning of the Qur'an

03/02/2023
Anonymous Sudan declares cyber war on Sweden because of the burning of the Qu'ran

During February & March
Anonymous Sudan attacks Swedish and Danish institutions because of the Qur'an burning by Palludan (who is Swedish and Danish citizen & done similar demonstrations in Denmark and Sweden in the past)

21/08/2023
Swedish Security Services raises terror threat level

22/07/2023
Several Qur'an burnings took place in Denmark, Sweden[120]

25/08/2023
Denmark presents bill banning the burnings of scriptures [121]

Events don't stop here - but this is meant as an excerpt of the chain of events.

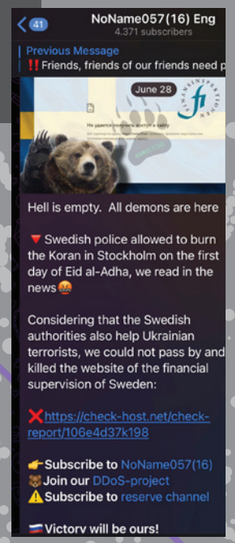
14/08/2023
NoName057(16) condemns the burning of the Qur'an in Sweden.

29/06/2023
Several known and unknown hacker groups including AnonymousSudan, 1919 Team, Islamic Hacker Army, Host Kill Crew, US NEXUS HACKER, Mysterious Team Bangladesh, KEP TEAM, UserSec collective, Team Heroxr, Electronic Tigers Unit, Team R70, GANOSEC TEAM, and Türk Hack Team executed DDoS attacks on several Swedish websites. Another #OpSweden campaign begins[119].

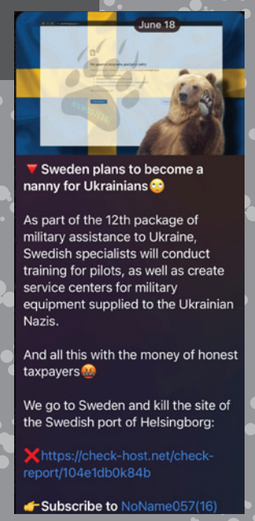
🇸🇪 Why did the Swedish police allow people to burn the Qur'an in front of a mosque in Stockholm? ❌

🔥 We had already warned you back then: If you burn the Qur'an then we burn your servers. ⚠️

28/06/2023
NoName057(16) reacts to the burning and attacks Sweden as a direct consequence



18/06/2023
NoName057(16) attacks Sweden due to aid given to Ukraine[118].



28/06/2023
Anonymous Sudan attacks Sweden after the burning of the Qur'an, they state:

"We missed Sweden very much. And today they burned the Quran again. Well, from now on, we will attack Sweden continuously for months.. We will target all vital infrastructure."

Digital world

By the end of January, Anonymous Sudan began attacking Sweden, Denmark and the Netherlands with the apparent motive to punish the respective countries for supporting or allowing anti-Islam demonstrations. Indeed, during the first quarter of 2023, Anonymous Sudan would attack a wide variety of countries and institutions for religious reasons, as can be seen in the chart below.

In May, however, something shifted. Anonymous Sudan showed signs of becoming financially motivated, for example, claiming in their Telegram channel they have data to sell, from an attack on an airline[122] . They also demanded a ransom from the Scandinavian Airlines (SAS)[123] in order to stop their DDoS attacks. This suggested a challenge to their hacktivist identity.

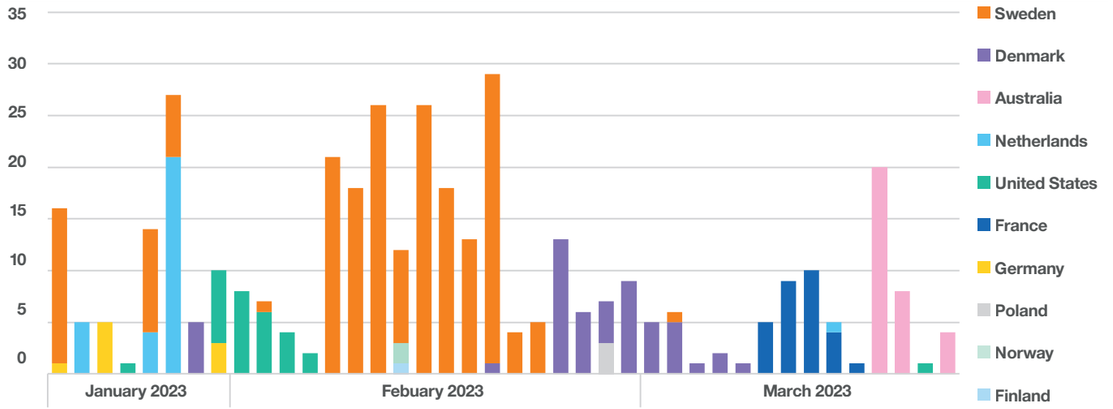
By extorting victims for money, the group had transitioned from being religious and politically driven to being financially motivated.

Technically Anonymous Sudan cannot be simply categorized as “hacktivists”, but have adopted a Cyber Extortion and cybercriminal label also.

And hence, the group also adopted a new form of DDoS attacks with a financial touch, referred to as Ransom DDoS (RDDoS). During June they continued the new modus operandi, attacking Microsoft services on a large scale and demanding US$ 1 million to desist in their attack[124]. As far as we know, however, no ransom was paid to them.

Anonymous Sudan in Q1 2023

Anonymous Sudan victim countries January-March 2023



At the end of June, another burning of the Qur’an took place in Sweden, which sparked a wide-spread international response from diverse countries, but also lead to several hacktivist groups calling out for attacks against Sweden. The campaign **#OpSweden was launched anew**[125]. Another month of burnings in Sweden and Denmark began.

July marked the escalation of geopolitical pressure against Scandinavian countries (namely Sweden and Denmark) for allowing the hostile burnings of the Qur’an. News coverage circulated about a Qur’an burning in Norway, which was investigated by Orange Cyberdefense Norway and shown to be fake news. In fact, images used in the news coverage was material from 2019, when an actual burning in Norway took place. Still, the incident illustrates the power of misinformation campaigns, which add to the already tense geopolitical situation in the Nordics.

Indeed, hacktivism and mis/disinformation have emerged as two sides of the same coin, and have increasingly come to characterize the use of cyber within geopolitical conflicts.

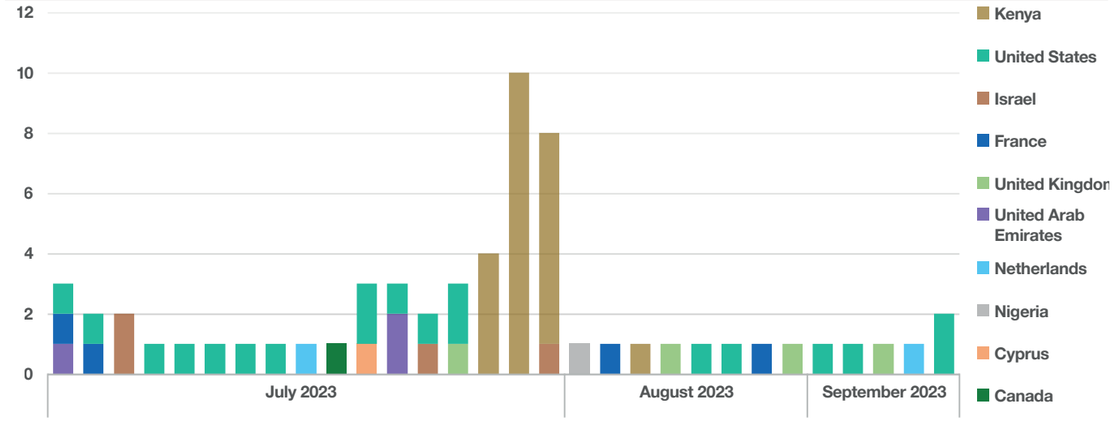
More detailed chain of events can be seen in the timeline.

But despite the tension that was now quite visible to the international public, Anonymous Sudan seem to have been distracted by other events. During July and August, they focused heavily on another real-world conflict, the ongoing fighting in Darfur, Sudan[126][127]. If we review the countries where Anonymous Sudan claimed victims during July and August, we note that they were shifting their geographical focus towards United States, Kenya and Israel. This is a very big shift of impacted regions in comparison to Q1, as can be seen in the chart on the next page. Their justification for attacking the respective countries has also shifted. During July and August, they apparently became politically focused, they concentrating heavily on countries that appeared to interfere with the conflict in Sudan.

So the shape of their victimology also changed: it has moved closer to their self-proclaimed ‘home’ – Sudan - and the group has moved from an agenda driven by religion towards more politically motivated activities. In Q3 especially, we see that Kenya was the most impacted country, correlating with the ongoing Sudan conflict, in which Kenya’s president offered to play a mediation role.

Anonymous Sudan in Q3 2023

Anonymous Sudan victim countries July-September 2023



Throughout the short life of the threat actor, we noted several geopolitical events that Anonymous Sudan commented on, and that also matched the actual ongoings in Sudan. Here are some examples:

1. Amnesty International reports that since the 15th of April 2023, the Sudanese Armed Forces (SAF) and the paramilitary Rapid Support Forces (RSF), who are rival factions of the military government of Sudan, have been fighting for control in Sudan. Extensive war crimes are being committed in Sudan[128]. On the same day, Anonymous Sudan posts to their Telegram channel: “Prayers for Sudan”, followed by the message “In the event that they shut down the Internet from Sudan, we will be back, do not worry”. They continue with a warning to other countries: “message to all countries that are trying to show the world that they are the ones who carried out the cease-fire in Sudan. We only see you when something big happens so that the world says, ‘Wow, look, this country has done this and this. We see everything. We warn any country that tries to interfere in Sudan's internal affairs. We will attack it immediately’”. #AnonymousSudan’, on the 15th of April 2023.

2. On the 22nd of April 2023, Anonymous Sudan attacked the official website of the Rapid Support Forces, which is a paramilitary force formerly operated by the Government of Sudan. It grew out of, and is primarily composed of, the Janjaweed militias which fought on behalf of the Sudanese government during the War in Darfur, and was responsible for atrocities against civilians. Its actions in Darfur qualify as crimes against humanity according to Human Rights Watch[129].

3. On the 23rd of April, Anonymous Sudan stated that “The internet has been closed by 90% of Sudan. We hope Elon Musk open Starlink in Sudan as soon as possible #AnonymousSudan”.

This pronouncement is in line with external reports that Sudan experienced electricity outages, and that the internet connectivity was at 2 percent of the usual level[130]. Additionally, two days prior to the internet outage (21st of April), Anonymous Sudan DDoS-ed the social media platform Twitter (now called X), with the reasoning that “Twitter has been down .The reason for our attack, we want to send a message to Elon Musk [SOS emoji] - Open Starlink [satellite internet service] in Sudan[…].” This could be a reference to the help Elon Musk and Starlink provided to Ukraine[131], - asking for the same support in the ongoing conflict in Sudan.

4. The group repeated their action on July, 1st, attacking the social media platform X and posting the following message on their Telegram channel: “Twitter been down for hours? Elon Musk, do you have intentions to open starlink in Sudan?”. They repeated this action on 28th of August, trying to gain Elon Musk’s attention.

5. On June, 1st 2023, the United States took measures to respond to the crisis in Sudan[132]. Anonymous Sudan responded to this on the 3rd of June, warning the United States not to get involved or “invade again”.

The examples above support the claim that the group might be Sudanese and either originate, or are currently located in, Sudan. However, we can only assess the narrative presented to us by the Threat Actors themselves, along with their observable impacts. In August, an interview between Anonymous Sudan, IntelCocktail[133] and BBC cyber correspondent Joe Tidy[134] [135] surfaces, a group member called ‘Crush’ shared their live location on Telegram as proof that they are based in Sudan.

How politically consistent are these groups?

Disinformation is difficult to identify. In the end, the truth remains elusive: Is Anonymous Sudan a group of skilled Sudanese 'cyber warriors' as they claim to be? Or are they distracting us with false claims, while actually operating in another nation's interest and maintaining 'plausible deniability[136]' as defenders of Islam striking at the West?'[137].

Anonymous Sudan is not very consistent. Our observations show that they have attacked victims all around the world, shifting their purported motivations and reasonings frequently. Despite the apparent identity crisis, the group has proven to be capable, not only technically, but also at making noise and seeking attention. But while they have made a name for themselves with their volume of activity in 2023, their claims often exceed the real impact of their attacks[138]. In the end, they are dependent on media attention and thrive on the attention of the wider public.

Let's do a quick dive into NoName057(16)

The other hacktivist group we have been observing during 2023 is NoName057(16). NoName057(16) might be more politically consistent than Anonymous Sudan has proven to be.

NoName057(16) has been active since the war against Ukraine began and has been targeting countries that are members of the the North Atlantic Treaty Organization (NATO) and countries that are considered to oppose Russian interests. By monitoring the publicly available Telegram messages on the English-speaking channel of NoName057(16) Eng, we deduce that the group specifically and directly impacts countries that are providing aid to the Ukraine in the ongoing war.

NoName057(16) thus allows us to explore whether we can find a correlation between publicly stated commitments of aid to Ukraine and NoName's apparent selection of targets. As an example, we can use the announcement by Sweden on the 15th of August about their thirteenth aid package[139], which triggered a response by NoName057(16) three days later.

On the 18th of August, with an announcement being posted in their Telegram channel, the group detailed the military equipment that was promised in the support package.

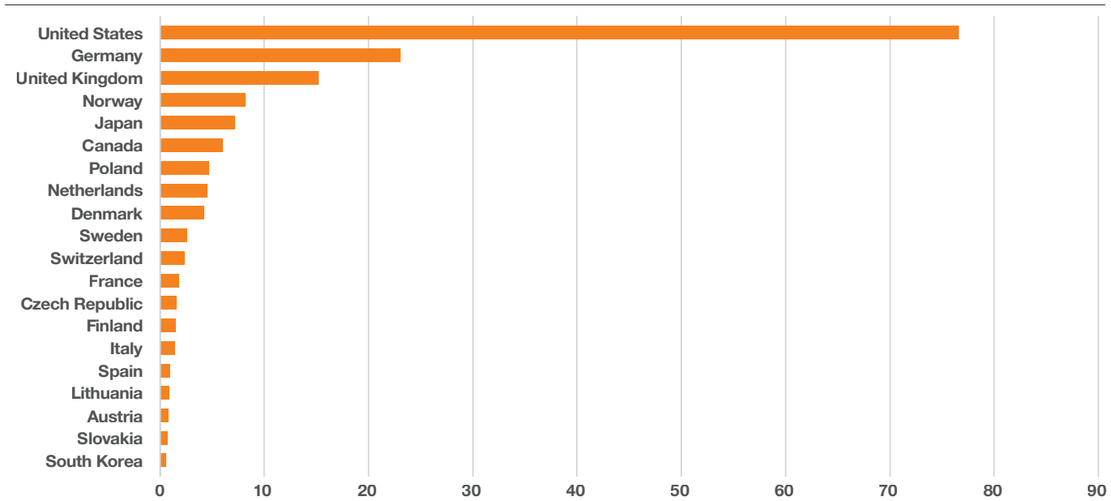
Political hacktivism as a 'proportionate' response

Using an external dataset that has collected official announcements of countries committing to support Ukraine, we can correlate NoName057(16)'s attacks against the specific countries providing the promised support.

For this purpose, we use the Ukraine support tracker database that has been created and is regularly updated by the Kiel Institute for the World Economy[140].

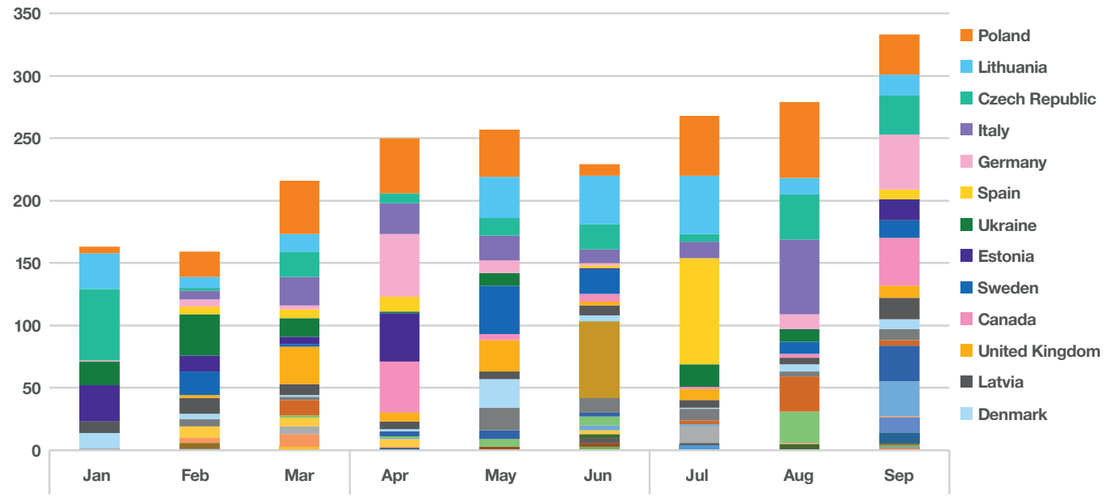
Ukraine Support Tracker

Top 20 countries offering support in $ billions



Victims of NoName057(16)

NoName057(16) victim countries in 2023



The institute began tracking government-to-government (bilateral) commitments to Ukraine in January 24, 2022 by at least 40 different governments; and continues doing so at the time of writing. This is explained in more detail in the data section.

The Ukraine support tracker shows that the United States has provided the most aid to Ukraine. In fact, they have committed (though not yet completely delivered) more support to Ukraine than all EU countries combined. This is notwithstanding the geography of the war, which is happening in Europe and thus not in the US' immediate neighbourhood.

Noteworthy, besides the documented aid provided by the respective countries listed, is that the paper published [141] alongside the Ukraine aid tracker database points out that the overall support given to Ukraine is comparatively small when compared to support given in other wars in history. As the paper states:

"The results show that governments in Europe did announce very large emergency funds in response to the war and energy price spike, but the bulk of the announced support was pledged to support their own households and firms rather than to support Ukraine. In total, the domestic energy support package commitments announced by EU countries amount to €570 billion, compared to €55 billion in total EU commitments to Ukraine."

This is particularly interesting considering the perceived high level of aid provided that is created by news outlets. The activities of NoName057(16) appear to track media trends and can seem disproportionate when this aid is put it into historic context.

So how does NoName057(16)'s victimology look in comparison to the level of support provided by governments as tracked by the Ukraine support tracker project?

As can be seen above, the victimology is very diverse in terms of which country is impacted. In total, since they became active, NoName057(16) has impacted 38 different countries.

The top 5 countries impacted are Poland, Lithuania, Czech Republic, Italy, and Spain. Ukraine is only at position # 6 in NoName057(16)'s list of victims, which is interesting given the fact that Ukraine is the target country in the actual war.

Let's explore whether we can find a reasonable explanation for NoName057(16)'s choice of victim countries in the Ukraine support tracker database. For this we conduct an experiment that looks at the countries that are noted by the Ukraine support tracker. We rank those countries by how much support (in terms of billions of USD) countries have promised to aid Ukraine (as visualized earlier). We then overlay this with the NoName057(16) country victim list, adding a ranking to reflect who has been attacked the most (as shown above). Using the ranking of countries in each list, we calculate the distance between the two rankings.

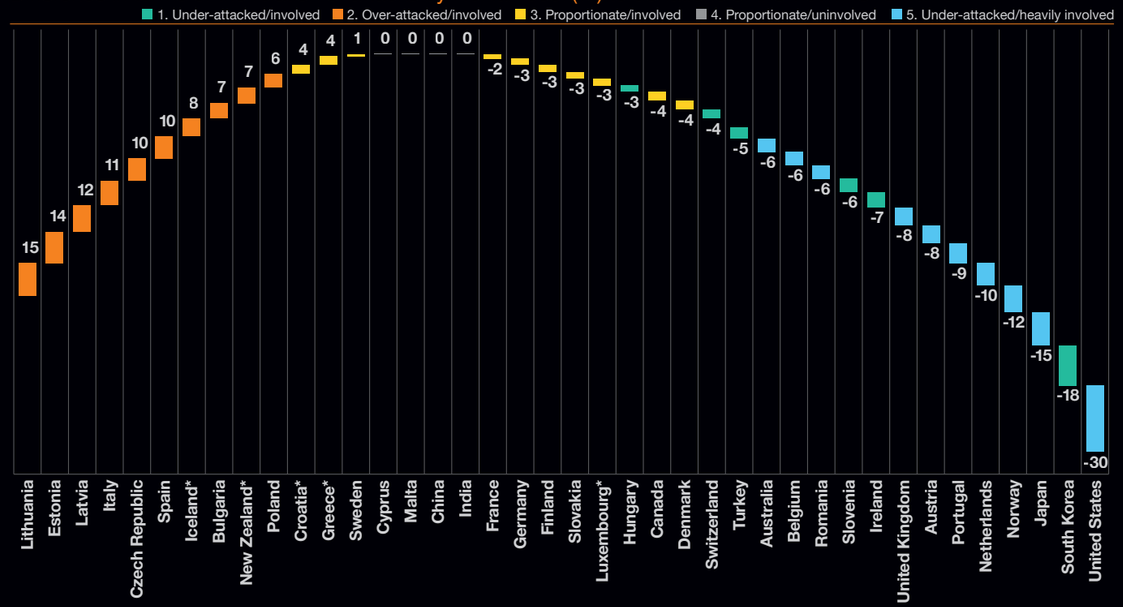
In our experiment, a distance of "0" could be considered to signal a politically "proportionate" response by NoName057(16), indicating that the country's ranking as a victim corresponds with its ranking in terms of level of support offered. We increase the radius to consider countries with distances between -4 and 4 as "proportionate" victims.

A negative distance tells us that those countries have made promises to support Ukraine but have not experienced correspondingly high numbers of attacks by NoName057(16). These countries are thus underrepresented in the NoName057(16) victim data. A positive distance suggests the opposite: These countries have been attacked many times by NoName057(16), but have not committed equivalently significant financial support to Ukraine. These countries are thus overrepresented in the NoName057(16) victim data.

If we look at examples of this logic at both extremes, we can identify the countries that appear "under-attacked", those that appear "over-attacked" with respect to the level of support they have promised Ukraine, and those where the level of attack could be viewed as political "proportionate" from the hacktivist perspective.

NoName057(16): victim rank vs. donations

Difference in terms of the relation of attacks by NoName057(16) to donations of the victim for Ukraine



There are other groups of countries that emerge from this insight:

1. Under-attacked and involved: Some countries have indeed committed to support Ukraine but were never impacted by attacks from NoName057(16).

2. Over-attacked: Some countries appear to have suffered a disproportionate level of attack relative to the amount of support they have offered. The countries include Lithuania, Estonia, Latvia, Italy and Czech Republic, Spain, and Bulgaria.
*Iceland and New Zealand also technically fall into this group, but their victim counts and promised support levels are so low that their position in our analysis is exaggerated.

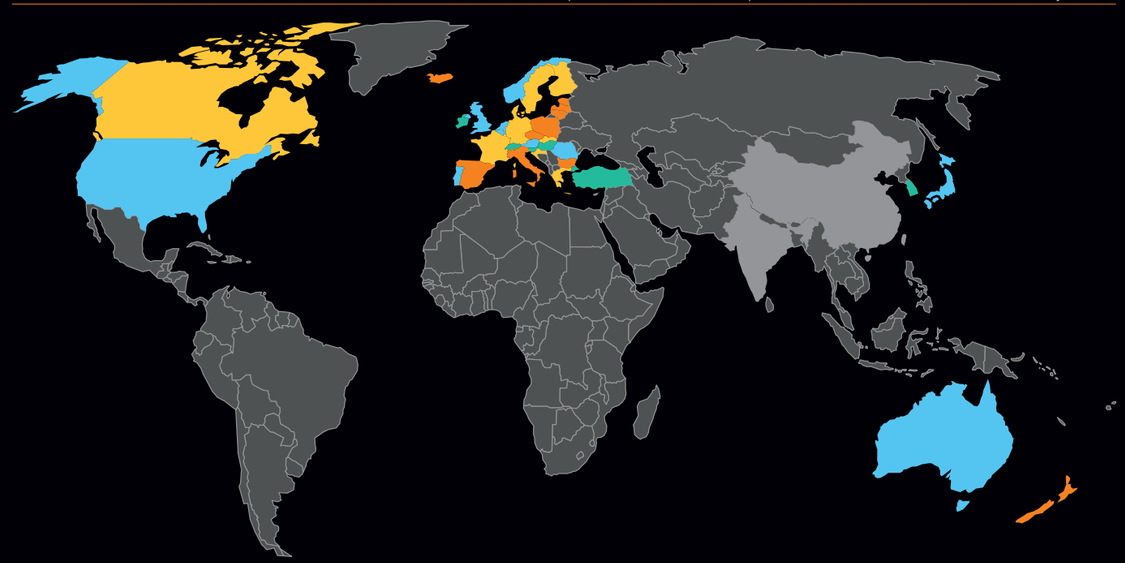
3. Proportionate and involved: Sweden, France, Germany, Finland, Slovakia, Canada, Denmark and Switzerland have all been heavily impacted by attacks, but the relative volume of attacks correlates logically with the relatively high level of aid provided to Ukraine. These countries could be thought of as the major 'front' in NoName's hacktivist war.
*The impact on Greece, Croatia and Luxembourg is also technically 'logical' in that it corresponds with the level of aid provided, but it should be noted that the levels of impact and the levels of aid are both substantially lower than the other countries in this group.

4. Proportionate but uninvolved: Some countries have not been impacted by attacks at all, and have not pledged to support Ukraine. These include Cyprus, Malta, China, and India. The impact on this group is politically "logical", but essentially irrelevant.

5. Under-attacked but heavily involved: The countries in this group include the United States, Japan, Norway, Netherlands, Portugal, Austria, the United Kingdom, Romania, Belgium and Australia. These countries have indeed been impacted by attacks, but the relative level of attacks they experience is low relative to the level of aid they have offered. The level of focus by NoName on this group is therefore also politically "disproportionate", with the United States standing far beyond others in this group from this perspective. The same analysis, but using percentage of GDP as the measure of aid given (rather than pure USD), would place Norway as the stand-out in this group.

NoName057(16): Heatmap

Countries more or less affected than expected as map



We observe that most of the over-attacked countries are geographically relatively close to the war, which could be the main reason for their apparent "unfair treatment". This aligns with the findings of the paper published with the Ukraine support tracker, in which the authors highlight that Eastern European countries stand out in terms of the help provided as a percentage of their GDP, especially when factoring the costs of hosting war refugees . Thus, geographical proximity and the appearance of "hands on" support could explain why some countries are impacted more than seems "proportionate". The exceptions here appear to be Spain and Italy, both of which suffer relatively high levels of attack despite relatively low levels of promised support but are not in close geographical proximity to the conflict.

Our qualitative observation of respective Telegram channels suggests that NoName057(16) has mostly been attacking Spain due to the military support and military training offered, along with the sanctions they've imposed.

Italy seems to be the victim of similar reasoning to Spain, in which they are apparently attacked due to military aid provided. There seems to be a misconception by NoName057(16) that Italy and Spain are large donors to Ukraine. As the Ukraine Support Tracker authors state: "In international comparison, it is puzzling why some rich Western European countries, like France, Italy, or Spain provide so little bilateral support".

Researcher notes – Data Source

Intel471: We thank Intel471 for their specialist contribution of data on overall activity & country distribution of pro-Russian hacktivist groups.

Telegram scraper: Orange Cyberdefense capabilities

According to the Ukraine Support Tracker paper and its described methodology:

- "We considered 2242 formal announcements of support between Dec 2021 and July 2023.
- Data included commitments from 41 donors, including G7 and EU member countries, plus Australia, New Zealand, Norway, South Korea, Switzerland, Turkey, India and China. Additionally, aids from EU institutions are traced, such as European Union institutions meaning the EU Commission and EU Council, but also via the European Peace Facility (EPF) and the European Investment Bank (EIB).
- The type of aid is classified in three types: military, humanitarian and financial.
- We removed entries that were not an official announcement but where support was mentioned by government officials (e.g. Minister of Foreign and European Affairs) during conferences, summits etc. We limited our analysis to official announcement that then caused a direct response by specific hacktivist groups. The official website of the Ukrainian Government describes additional financial aid, so that data was also considered but with a later time stamp. Support to NATO is not included in this dataset, which hacktivist also reacted on".

Summary

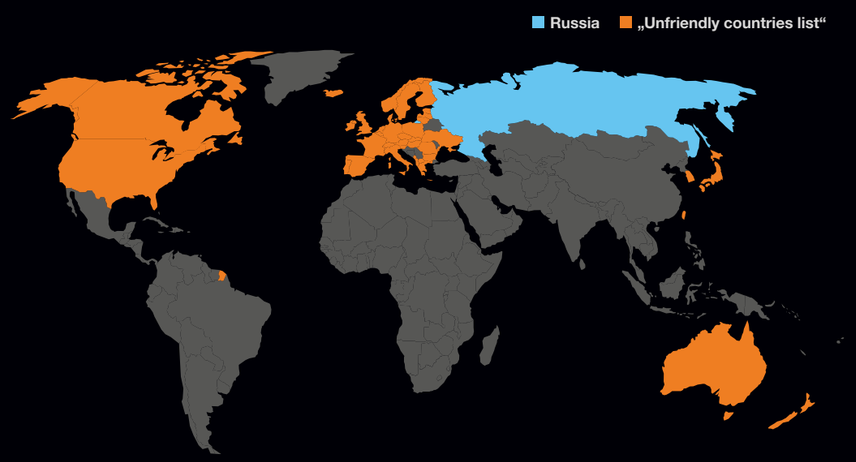
Hacktivism activity has seen a significant intensification since the war against Ukraine began. Hacktivism has become an impactful facet of modern warfare, as we have recently witnessed, not only in the war against Ukraine, but also in the most recent Hamas-Israel war. At the time of writing, our World Watch advisory service has reported that over 100 hacktivist groups are active in the war of Hamas against Israel. However, the sophistication seen in the first days of the war against Ukraine has not yet been seen in the Hamas-Israel war. In investigating two of the most active pro-Russian hacktivist groups, we discover major differences in the groups' modus operandi.

Anonymous Sudan has made many controversial statements regarding their origin. Given their connection to the KillNet collective, our assessment is that the group has close ties to Russia. However, we do believe that most of their members are based in Sudan, which is what they publicly claim. At first glance Anonymous Sudan seems to be a somewhat immature actor, indecisive on what they want to accomplish, switching between religious, political, and financial motivations, and even resorting to extorting victims - unsuccessfully. The group uses hyperbolic language to describe their efforts, exaggerating the impact of their attacks. During their short lifetime, they declared "cyber war" against countries or private organizations four different times. They attacked the social media platform Twitter / X in the apparent hope that Elon Musk would enable the Starlink satellite network in Sudan. Attacking someone they wanted help from is hardly characteristic of a mature player.

However, if we consider events in the Nordics, which began with Anonymous Sudan (as outlined in our timeline earlier), we see how powerful hacktivist activity can be in creating fear, uncertainty, and doubt (FUD). When viewed in terms of their impact, Anonymous Sudan has succeeded in this, especially in the Nordics. As we documented in the timeline, geopolitical tensions in the region escalated to the point that Sweden and Denmark had to introduce measures to preserve safety. Sweden raised their terror threat level after encountering heavy international unrest, in the "real" and cyber world. Denmark introduced a bill prohibiting the burning of religious scripts. This illustrates that it might be possible to destabilize countries and regions through these rather naive efforts. Anonymous Sudan seems inconsistent, but their actions have contributed to increasing tensions in an already tense geopolitical situation. On the other hand, NoName057(16), one of the most active pro-Russian hacktivist groups, has been behaving much more consistently – targeting organizations and countries that support Ukraine. Our analysis suggests that some countries have received attention from the group that is commensurate with the level of support they promise Ukraine, and thus constitute a "proportional" response.

Attacks on other countries appear less proportionate, as they are attacked more or less than their support for Ukraine would suggest is logical. This might have to do with their geographical location, or because their perception of who the "enemies" of Russia are, is shaped the Russian perspective. If we compare the map above with the depiction below of Russia's "unfriendly country list"[142], the similarities are apparent.

However, our analysis offers deeper insight by expanding on how well the level of activity experienced by victim countries corresponds with the level of support they promise Ukraine.



Conclusion

Hacktivism can be very noisy but still needs to be taken seriously. We have seen how impacts in cyber space (defacing websites, DDoS etc.) can intensify political tensions and have real impacts in the real world, showing that hacktivism has become a powerful tool.

An important thing to note is that we are seeing a continuous evolution towards 'cognitive' attacks, which seek to shape perception through technical activity. The impact has less to do with the disruptive effect of the attack or the value of the data or systems that are affected (e.g., stolen, leaked or destroyed) but with the impact that these attacks will have on societal perception.

Hacktivism is all about perception. The rage that triggers hacktivist activity emerges from a perception of threat or injustice, rather than cynical political calculus. The political effect of attacks exceeds the real technical impact because of the feelings of fear, uncertainty and doubt (FUD) they trigger. Hacktivists don't need to respect the real political calculus because FUD isn't logical. Since the impact is powered by the hacktivist's message, the actor can choose to make a political statement out of any apparently successful attack. Targeting can be highly opportunistic, which greatly exacerbates the technical asymmetry already faced by defenders in cyberspace. In 'conventional' cyberattacks, it's already said that "the attacker only has to be lucky once". This is even more true with hacktivism, where any successful technical operation can be turned in political collateral. Perception is contagious, so even the slightest technical success can spawn ballooning political consequences.

Hacktivist groups are mobilizing themselves into collectives to maximize their resources. We suggest that defenders need to do the same. The war against Ukraine has surfaced an intensification of hacktivist activity, but also spawned public-private collaborations to share intelligence and take collective defensive actions. We need to increase those efforts.

José Araujo
Global CTO
Orange Cyberdefense

Tatiana Chamis-Brown
SVP Global Marketing
Orange Cyberdefense

Security predictions

Prepare for nasty weather!

Once again, we are faced with the difficult exercise of anticipation. What will be the cybersecurity risks in the years to come? Should we prepare for new threats? Should we fear a significant increase in these threats, or have we reached a summit and if so, in what way? What will be the impact of major trends in the industry?

We had already considered last year some of the threats that we will have to face, covering the legal, economical, and technical aspects. Most of them remain relevant but certain technological and industry trends deserve to be explored in more depth.

This year we will focus on those which we believe will be causing lasting disruptions in the field of cyber security and associated risks.

Cloudy, with risk of rain

The perimeter is dead, long live the new perimeter!

We must no longer oppose perimeter security to the effectiveness of more global approaches, considering new usages and new services by all companies. We must ensure that data is secured in the best possible way, wherever it is stored, wherever it is consumed and regardless of how this data will be accessed and manipulated. We must review the security architectures put in place. They must consider Cloud services and the nomadism of users. The company's sensitive assets are now, most often, outside the company, within these departments. Users access it from anywhere and on terminals that must be secure.

Many security solutions have appeared in recent years, at the instigation of security solution publishers but also following concepts pushed by security consulting and research companies.

Zero Trust

The Zero Trust model appeared a few years ago and has become a target to achieve for a multi-year security roadmap. The migration of existing infrastructure but also the adoption of new security solutions (Multi Factor Authentication, Security Service Edge (SSE), Extended detection and Response (XDR), etc.) is essential and will become an even greater focus in the years to come because they will be the only actions able to combat the scale of the threat.

Outsmarting the machine: Artificial Intelligence (AI) cyberattacks are evolving

AI – Old ally, new enemy

Whilst AI has long been used in cybersecurity, it was mainly used to detect weak signals in large volumes of data or mixed sources. The performance of the algorithms used has greatly improved, thanks to today's storage and computing capacities. As such, results have changed the situation not only in terms of protection, but also in terms of the ability of attackers to take advantage of it.

Prepare for spam without spelling-mistakes

For phishing attacks, it will become increasingly complex to identify a fraudulent message by its form or content. AI enables attackers to write content in the victim's language, without syntax or grammatical errors and, above all, by adapting to their victims. In the future, these attacks will take other forms, such as vishing (phishing carried out by telephone or voice message), which is even more complex to combat.

Coding companion, for good and bad

In the creation of malware, generative AI will provide valuable assistance. It puts legitimate capabilities designed for developers within reach of cybercriminals. If today these technologies are not able to replace expertise, they facilitate and accelerate the software implementation work.

When it comes to implementing the exploitation of a newly discovered vulnerability, the risk of finding unprotected systems will be even greater. We must anticipate an increase in the use of this type of solution, especially since the level required to take advantage of it will become easier, as the reliability of these generative AI advances.

Eroding language barriers

Finally, we are already seeing the impact of these generative AIs on the increase in ransomware in certain geographic areas. Until now, the majority of targeted countries were English-speaking. We must now prepare for real-time, high-quality machine translation capabilities, as well as automation of the early phases of negotiation using AI technologies that will make it possible to target a wider variety of countries.

Laws and Regulations: When security becomes mandatory

Government policy and regulation at a turning point for defenders and attackers

We have seen new government policy and regulation developments this year which we expect will have a lasting effect on organizations' cyber security maturity.

In July, the US Securities and Exchange Commission (SEC) adopted rules requiring registrants to disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance. In Europe, we will see EU member states incorporating the NIS2 directive into national legislation by October 2024, requiring organizations in more sectors to establish a higher level of cybersecurity and resilience, and comply with incident reporting lead times.

As the first sanctions and charges are applied – as seen recently with SolarWinds - we anticipate it to be a turning point into elevating cyber security as a key focus in boardrooms.

Similarly, we foresee a potential turning point on Cyber Extortion activity driven by joint government policy. In a year where Cyber Extortion (Cy-X) activity level was the highest ever recorded by Orange Cyberdefense's Security Research Team, over 40 countries members of the International Counter Ransomware Initiative (CRI) have agreed a joint policy declaring that member governments should not pay ransoms demanded by cybercriminal groups. They also agreed a shared blacklist of wallets used by ransomware actors, commitment of pursuing actors responsible, amongst other initiatives. We are yet to see its impact on Cy-X statistics but anticipate this cooperation may damper the viability of Cy-X ecosystem.

One for all: Supplier consolidation

Security is consolidating, but never consolidated

Consolidation of cyber security products is not a new trend. From the first steps with unified threat management (UTM) devices to Next-Generation Firewalls (NGFW), and more recently with Extended Detection and Response (XDR), Secure Access Service Edge (SASE) and Cloud-Native Application Protection Platform (CNAPP), consolidation is a constant. With new attacks emerging, new solutions are required. And with an explosion of technology, consolidation promises efficient security operations and improved risk posture.

What seems to be at an inflection point is a 'consolidation of consolidations' – into single vendor platforms, or as multi-vendor composable modules that interoperate (what Gartner calls 'Cybersecurity Architecture Mesh'). We anticipate this to further ramp up in the next years.

Regardless of the model pursued, legacy technology compatibility, future-proofing from vendor lock-in and focusing on security outcomes rather than the technology itself are factors to be considered by organizations. In these aspects, consolidation via a security services provider may prove to be a compelling alternative.

Quantum threat, be prepared

Quantum threat refers to the risk that quantum computers, if they become sufficiently efficient, will impose on current cryptographic systems. Symmetric algorithms are less affected, but the public keys ones – currently used everywhere – will no longer be secure if such computers appear.

Many challenges must be addressed to develop such computers and we are still far from this "Q-day". However, to be prepared for a "Harvest-now, decrypt later" attack*, the scientific community is developing post-quantum cryptography algorithms. Thanks to their properties and their design, they should be resilient to such attack, at least we hope.

Recently, the scientific community have proposed new algorithms, supposedly post-quantum resistant, in which cryptography researchers have great confidence and which have been standardized. But, because they are recent, and we lack perspective, the precautionary principle requires us to adopt a hybrid approach. In Europe, we do not recommend to completely "shift" to quantum resistant cryptography but combining it with existing methods to use the best of both worlds. This hybrid approach guarantees continued protection by recognized public key algorithms and will, most likely, be prepared for this future type of attack.

Equipment and solutions embedding cryptographic algorithms should consider implementing these new mechanisms. Hybrid algorithm availability should be a key criterion when it comes to selecting a solution.

* This attack consists of recording communications that cannot be deciphered today to decrypt them later, when this type of computer appears.

A Quantum Security

Orange Cyberdefense and the MiDO academy

Building a safer digital society in Cape Town

From everything we know, and have seen, the rapid growth in tech advancement came with a paradigm shift in the way humans think, live and work. This was accelerated exponentially during the pandemic and subsequent lockdowns that were imposed due to Covid-19. This technical advancement, as well as the digital shift to remote working has birthed the need for a host of tech-related skills and tools to be able to fully partake in what's referred to as the 4th Industrial Revolution.

Roberto Arico, Senior Presales Consultant, **Orange Cyberdefense**

Bridging the 'digital divide'

When considering South Africa's current digital divide, due to the lack of access to quality digital enabling tools and the national need for youth upskilling for the future workplace, projects focusing on digital empowerment and upliftment become crucial to society.

MiDO Technologies has a mission to change the narrative around digital enabling tools on the continent of Africa and prepare African youth. As a result of what they do, individuals who would not normally be exposed to technology or the latest digital trends, will build confidence in the use of technology and digital skills that are imperative in the 4th Industrial Revolution. Here in South Africa, we have a dual challenge of high youth unemployment and cyber security skills shortage.

According to the Quarterly Labour Force Survey (QLFS) 2022, the unemployment rate in South Africa was 63.9% for those aged 15-24, while the current official national rate stands at 34.5%.

The digital chance

To this end, MiDO Technologies launched its first Cyber Security cohort through a new project - The MiDO Academy. The MiDO Academy was formed with a simple mission that enables a very real and impactful outcome: "To create pathways out of poverty and create viable employment opportunities for young people, while alleviating the pressures felt by business owners to upskill and integrate new talent".

The Academy's focus is on 21st century skills: soft skills, critical thinking, collaboration, creativity, innovation, cyber security awareness and cyber security training.

The programme facilitates workshops and guest lectures from industry representatives, as well as exposure to companies for job shadowing and internship opportunities, and there are weekly mentor group sessions. It will support 20 school leavers over 9 months, providing them with cyber, professional and life skills training.

There since the beginning

Since the very first days of our operations in South Africa as Sensepost in the year 2000, there has always been a fundamental belief that knowledge should be shared, and wisdom imparted to those who are willing and eager to learn. We have grown from an ethical hacking business of just 2 people in a shared space to a team over 100 that subsequently became Orange Cyberdefense South Africa. This Orange Cyberdefense South African team includes some of the world's most preeminent cybersecurity experts. We have helped governments and blue-chip companies both review and protect their information security and stay ahead of evolving threats. We are also a prolific publisher of leading research articles and tools on cybersecurity which are widely recognised and used throughout the industry and feature regularly at industry conferences including BlackHat and DefCon.

The ethos of Orange Cyberdefense South Africa is summed up succinctly by a quote from Dan Geer: "Work like Hell. Share all you know. Abide by your handshake. Have fun" Orange Cyberdefense South Africa continually strives to uplift those who have been marginalized and give back to the less fortunate communities in South Africa to uplift and empower them. There are few opportunities to support local initiatives that provide invaluable exposure, experience, and skills to those who wish to explore an interest in, start a career in, or simply upskill in the Cybersecurity space.

To this end, Charl van der Walt, Head of Security Research at Orange Cyberdefense and one of the original SensePost founders, felt it important to support the MiDO Foundation with their MiDO Academy.

> **I believe that the data science skills required for security research and analysis will be key to not only understanding threats today but will become an essential part of cybersecurity and the new digital world post the 4th Industrial Revolution."**
>
> **Charl van der Walt,**
> Head of Security Research at Orange Cyberdefense

Orange Cyberdefense team members – namely Charl, Wicus Ross and me, have provided a selection of learners with real-world threat actor data.

Learners are required to analyse the data, ensuring a high quality and attention to detail, and developing their Open-Source Intelligence (OSINT) skills, as well as Data Science and Analytics skills to classify and structure the data provided into meaningful information. With enough information, the learners are then tasked to interpret the results, and start to analyse and identify trends, patterns, and correlations. These patterns and trends must then be outlined and presented back to their classmates and facilitators for further scrutiny.

A change, a chance, a safer digital society!

Learners are gaining invaluable knowledge on real-world data and learning how to analyze, identify, structure and investigate data, while also keeping a big-picture view to perform a more detailed analysis.

This ensures that the MiDO academy will equip tomorrow's defenders and future cybersecurity experts with the skills and critical thinking needed to combat the challenges and threats they will face.

By sharing the Orange Cyberdefense methodology, tools, and processes we are striving to empower the next generation of cybersecurity professionals, fuelling a passion for knowledge and a hunger for understanding, while never forgetting to work like Hell, sharing all they know, abiding by their handshake and most importantly, having fun.

www.orangecyberdefense.com

Report summary

What have we learned?

Sara Puigvert
EVP Global Operations
Orange Cyberdefense

What a year!

Cyber threats have constantly been evolving with attackers trying to get past defenses to achieve their goals, be it for financial gain, political motives, or various other reasons.

The good news?

Our teams are always on the lookout for new and emerging trends. Let's summarize 4 main key take aways learnt from this past year.

Firstly, one of the most striking trends we notice is the rising number of ransomware victims. Unfortunately, Cyber Extortion (Cy-X) attacks are still highly profitable for criminals - though hopefully that will change as organizations find ways to be more resilient.

Hacker groups active since multiple years are still behind a large number of victims. However, and additionally, numerous new and younger groups have recently appeared in the ecosystem: they take advantage of ransomware strains that are leaked on cybercriminal forums. Thanks to that, they flourish quickly with much lesser effort.

We have noticed an uptick in international cooperation amongst security industry and Law Enforcement to try to take down such "historical" groups (Ragnar Locker, Qakbot, Snake -from Turla, to name but a few). In the cybersecurity world, without borders, international cooperation is key: without it, there's not much which can be done. Unfortunately, even when infrastructures are seized, it isn't uncommon to see the same group back in business a few weeks or months later under a new name.

We've even noticed more vigilante "group versus group" actions, as the example of the attack on the Trigona group, led by hacktivists from the Ukrainian Cyber Alliance. This politically driven attack successfully disrupted the illegal activities of the Russian-based ransomware gang. With the current geopolitical climate, it wouldn't be surprising to record similar attacks in the future.

A second persistent trend in 2023 : the number of detected vulnerabilities has continued to strongly increase. Hackers quickly exploit technical and human flaws (through phishing attacks for instance), so this increase is concerning. And what has been particularly true in 2023, is the increase of exploits using the infamous 0-days (with no patch or correction yet available from the software maker as they are unaware of their existence).

Unfortunately, the confirming trend is that vulnerabilities (among which 0-days) are used as attack vectors even more quickly and more intensively. The defender's patching response time is crucial in preventing a breach. And in the case of openly disclosed 0-days breaches, it is becoming increasingly important for solution providers to release security fixes as fast as possible.

The third trend in 2023 is related to hacktivism behavioral changes increasingly conflictual global geopolitical climate. Whereas 2022 was shaped by cyber hacktivism linked to the war against Ukraine, with a relatively easy to follow and political-only approach by belligerents on both sides, the Hamas-Israel war has sparked many individual, loose and moving, politically-driven initiatives across the globe, which will probably contribute to more disruptions in the cyber world in years to come. These actions are also increasingly aiming to promote fear or to influence public opinion with exceptional levels of disinformation flourishing online.

Moreover, cyberwarfare, another consequence of the world's conflictual evolution, has also evolved this year: sabotage, through wipers, to destroy an enemy's data is way less popular amongst nation-state threat actors, in favor of espionage operations. In some cases, attacks have been conducted to try to influence elections in other countries, and in others we can even notice alliances between nation-states (exchanging cyber expertise for weapons, for instance).

The picture which is drawn here might seem a bit bleak; but the silver lining is that this analysis is the fruit of years of gathering intelligence on the cyber threat – and in this world, knowledge is power.

The last and positive trend I would like to end this summary on is around the defenders' resiliency: cyber threat is growing and evolving but cyber defenders, as shown in this Security Navigator are also learning, adapting and innovating to meet these threats head on.

The fight against threats requires awareness and best practices adoption within your own organization.

Together, we (can) build a safer digital society.

»Cyber threat is growing and evolving but cyber defenders, as shown in this Security Navigator, are also learning, adapting and innovating to meet these threats head on.«

Sara Puigvert, EVP Global Operations Orange Cyberdefense

Contributors, sources & links

Sources

This report could not have been created without the hard work of many researchers, journalists and organizations around the world. We've gratefully used their online publications for reference or context.

Sources/links

[1] https://www.securityweek.com/goanywhere-mft-users-warned-of-zero-day-exploit/

[2] https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/

[3] https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/

[4] https://sec.okta.com/harfiles

[5] https://www.beyondtrust.com/blog/entry/okta-support-unit-breach

[6] https://blog.1password.com/okta-incident/

[7] https://blog.cloudflare.com/how-cloudflare-mitigated-yet-another-okta-compromise/

[8] https://www.regjeringen.no/no/aktuelt/presseinvitasjon/id2990098/

[9] https://forums.ivanti.com/s/article/CVE-2023-35078-Remote-unauthenticated-API-access-vulnerability?language=en_US

[10] https://forums.ivanti.com/s/article/CVE-2023-35081-Arbitrary-File-Write?language=en_US

[11] https://github.com/vchan-in/CVE-2023-35078-Exploit-POC

[12] https://forums.ivanti.com/s/article/CVE-2023-35082-Remote-Unauthenticated-API-Access-Vulnerability-in-Mobile-Iron-Core-11-2-and-older?language=en_US

[13] https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

[14] https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

[15] https://www.infosecurity-magazine.com/news/mandiant-russian-gru-cyber/

[16] https://www.reuters.com/world/uk/uk-electoral-commission-says-it-was-targeted-by-hostile-actors-cyberattack-2023-08-08/

[17] On August 11, 20223

[18] https://arstechnica.com/security/2023/08/how-an-unpatched-microsoft-exchange-0-day-likely-caused-one-of-the-uks-biggest-hacks-ever/

[19] https://www.globaltimes.cn/page/202308/1296226.shtml

[20] https://www.infosecurity-magazine.com/news/barracuda-zero-day-exploited/

[21] https://www.securityweek.com/cisa-analyzes-malware-used-in-barracuda-esg-attacks/

[22] https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf

[23] https://arstechnica.com/security/2023/09/with-0-days-hitting-chrome-ios-and-dozens-more-this-month-is-no-software-safe/

[24] https://www.techtarget.com/searchsecurity/definition/hacktivism

[25] https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia

[26] https://emerging-europe.com/news/ukraines-tech-warrior/

[27] https://www.zdnet.com/article/ukraine-is-building-an-it-army-of-volunteers-something-thats-never-been-tried-before/

[28] https://www.politico.eu/article/ukraine-digital-transformation-mykhailo-fedorov-russia-blockade/

[29] https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-assessment-iocta-2023

[30] https://www.reliaquest.com/blog/q1-2022-ransomware-roundup/

[31] https://www.darkowl.com/blog-content/dark-web-groups-turn-their-attention-to-israel-and-hamas/

[32] https://cert.gov.ua/article/2394117

[33] https://blog.google/threat-analysis-group/ukraine-remains-russias-biggest-cyber-focus-in-2023/

[34] https://therecord.media/hacker-group-anonymous-sudan-demands-three-million-from-sas

[35] https://socradar.io/ghostlocker-a-new-generation-of-ransomware-as-a-service-raas/

[36] https://twitter.com/vxunderground/status/1714476634781241583

[37] https://msrc-ppe.microsoft.com/blog/2023/06/microsoft-response-to-layer-7-distributed-denial-of-service-ddos-attacks/

[38] https://insights.sei.cmu.edu/library/historical-analysis-of-exploit-availability-timelines/

[39] J. Jacobs, S. Romanosky, I. Adjerid and W. Baker, "Improving vulnerability remediation through better exploit prediction," Journal of Cybersecurity, vol. 6, no. 1, 2020.

[40] https://www.first.org/epss/

[41] https://insights.sei.cmu.edu/library/historical-analysis-of-exploit-availability-timelines/

[42] J. Jacobs, S. Romanosky, I. Adjerid and W. Baker, "Improving vulnerability remediation through better exploit prediction," Journal of Cybersecurity, vol. 6, no. 1, 2020.

[43] https://arxiv.org/pdf/2302.14172.pdf

[44] https://www.first.org/epss/

[45] https://insights.sei.cmu.edu/library/historical-analysis-of-exploit-availability-timelines/

[46] https://www.first.org/epss/

[47] J. Jacobs, S. Romanosky, I. Adjerid and W. Baker, "Improving vulnerability remediation through better exploit prediction," Journal of Cybersecurity, vol. 6, no. 1, 2020.

[48] https://arxiv.org/abs/2302.14172

[49] https://www.first.org/epss/

[50] https://www.orangecyberdefense.com/global/white-papers/cy-xplorer-2023

[51] https://www.worldbank.org/en/country/india/overview

[52] https://minister.homeaffairs.gov.au/ClareONeil/Pages/australia-leads-global-task-force-to-fight-ransomware.aspx

[53] https://therecord.media/costa-rica-cyberdefense-ransomware-rodrigo-chaves

[54] https://www.census.gov/naics/?58967?yearbck=2022

[55] https://www.bleepingcomputer.com/news/security/meet-noescape-avaddon-ransomware-gangs-likely-successor/

[56] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2023/230614_CISA_Lockbit.html

[57] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

[58] https://en.wikipedia.org/wiki/Pareto_principle

[59] https://www.trendmicro.com/en_us/research/23/i/fbi-qakbot-takedown.html

[60] https://www.europol.europa.eu/media-press/newsroom/news/cybercriminals-stung-hive-infrastructure-shut-down

[61] https://cyberscoop.com/doj-cybercrime-disruption-ransomware/

[62] https://twitter.com/ValeryMarchive/status/1715351959111094717

[63] https://www.bleepingcomputer.com/news/security/new-hunters-international-ransomware-possible-rebrand-of-hive/

[64] https://analyze.intezer.com/analyses/5fd2d3fa-2344-4f95-b129-3d236eee7814

[65] https://therecord.media/ransomware-experts-laud-hive-takedown-but-question-impact-without-arrests

[66] https://therecord.media/whiteh-house-global-initiatives-information-sharing-ransomware-tracking

[67] https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/01/international-counter-ransomware-initiative-2023-joint-statement/

[68] https://twitter.com/vxunderground/status/1714476634781241583

[69] https://therecord.media/hacker-group-anonymous-sudan-demands-three-million-from-sas

[70] https://socradar.io/ghostlocker-a-new-generation-of-ransomware-as-a-service-raas/

[71] https://www.reliaquest.com/blog/q1-2022-ransomware-roundup/

[72] https://cert.gov.ua/article/2394117

[73] https://blog.google/threat-analysis-group/ukraine-remains-russias-biggest-cyber-focus-in-2023/

[74] https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/

[75] https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-assessment-iocta-2023
[76] https://www.ejiltalk.org/8-rules-for-civilian-hackers-during-war-and-4-obligations-for-states-to-restrain-them/
[77] https://cyberlaw.ccdcoe.org/wiki/Direct_participation_in_hostilities#cite_note-1
[78] https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/
[79] https://github.com/cert-orangecyberdefense/ransomware_map/blob/main/OCD_WorldWatch_Ransomware-ecosystem-map.pdf
[80] https://github.com/cert-orangecyberdefense/ransomware_map/blob/main/OCD_WorldWatch_Ransomware-ecosystem-map.pdf
[81] https://www.bleepingcomputer.com/news/security/blackcat-alphv-ransomware-linked-to-blackmatter-darkside-gangs/
[82] https://www.europol.europa.eu/media-press/newsroom/news/ragnar-locker-ransomware-gang-taken-down-international-police-swoop
[83] Industroyer2: Sandworm's Cyberwarfare Targets Ukraine's Power Grid Again (Robert Lipovsky & Anton Cherepanov, ESET, Black Hat USA, 2022): Industroyer2: Sandworm's Cyberwarfare Targets Ukraine's Power Grid Again
[84] BlackEnergy – What we really know about the notorious cyberattacks (Anton Cherepanov & Robert Lipovsky, ESET, 2016): https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Cherepanov-Lipovsky.pdf
[85] Analyzing PIPEDREAM - Challenges in Testing an ICS Attack Toolkit (Jimmy Wylie, DEF CON, 2022): DEF CON 30 - Jimmy Wylie - Analyzing PIPEDREAM - Challenges in Testing an ICS Attack Toolkit
[86] https://www.dragos.com/year-in-review/
[87] https://waterfall-security.com/ot-insights-center/ot-cybersecurity-insights-center/2023-threat-report-ot-cyberattacks-with-physical-consequences/
[88] https://www.orange-business.com/en/blogs/how-boost-ot-it-security
[89] https://www.orange-business.com/en/industries/manufacturing
[90] Miller, T., Staves, A., Maesschalck, S., Sturdee, M. and Green, B., 2021. Looking back to look forward: Lessons learnt from cyberattacks on industrial control systems. International Journal of Critical Infrastructure Protection, 35, p.100464.
[91] Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44, 588–608.
[92] https://www.nozominetworks.com/downloads/US/SANS-Survey-2022-OT-ICS-Cybersecurity-Nozomi-Networks.pdf
[93] https://arxiv.org/abs/2307.09549
[94] https://www.techtarget.com/searchsecurity/definition/hacktivism
[95] https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia
[96] https://emerging-europe.com/news/ukraines-tech-warrior/
[97] https://www.zdnet.com/article/ukraine-is-building-an-it-army-of-volunteers-something-thats-never-been-tried-before/
[98] https://www.politico.eu/article/ukraine-digital-transformation-mykhailo-fedorov-russia-blockade/
[99] https://therecord.media/russia-or-ukraine-hacking-groups-take-sides
[100] https://www.securityinfowatch.com/cybersecurity/article/53056804/did-the-russiaukraine-war-start-a-hacktivist-revolution
[101] https://engelsbergideas.com/essays/hacktivisms-cold-war-turns-hot/
[102] https://check-host.net/
[103] https://www.radware.com/cyberpedia/ddos-attacks/killnet/
[104] https://www.bbc.com/news/technology-66668053
[105] https://intelcocktail.com/anonymous-sudan-interview/
[106] https://flashpoint.io/blog/anonymous-sudan-ddos-timeline/
[107] https://www.scmagazine.com/news/hacktivist-anonymous-sudan-bear-wolf
[108] https://www.government.se/articles/2023/08/swedish-security-service-raises-terror-threat-level/
[109] https://www.blogarama.com/technology-blogs/1412280-cyber-express-blog/52063110-attacks-sweden-rises-opsweden-back-this-time-different-results
[110] https://www.cnbc.com/2023/01/24/quran-burning-in-sweden-enrages-turkey-threatens-nato-membership-path.html
[111] https://www.aljazeera.com/news/2023/1/23/erdogan-to-sweden-dont-expect-turkish-support-for-nato-bid
[112] https://www.government.se/press-releases/2023/06/twelfth-support-package-to-ukraine/
[113] https://apnews.com/article/turkey-sweden-nato-erdogan-quran-c69a3258e3bd60995561b5fbc87b8d12
[114] https://www.blogarama.com/technology-blogs/1412280-cyber-express-blog/52063110-attacks-sweden-rises-opsweden-back-this-time-different-results
[115] https://www.reuters.com/world/koran-burning-sweden-sparks-protest-baghdad-2023-06-29/
[116] https://www.politico.eu/article/protesters-sweden-embassy-baghdad-iraq-quran-burn/#
[117] https://www.sn.dk/danmark/rasmus-paludan-starter-koranafbraending/
[118] This is one example out of many that happened during this time, either attacking Sweden or other countries.
[119] https://socradar.io/an-ongoing-ddos-campaign-targeting-sweden/
[120] https://www.reuters.com/world/europe/protesters-burn-koran-front-egyptian-embassy-denmark-2023-07-25/
[121] https://www.nytimes.com/2023/08/25/world/europe/denmark-quran-burning.html
[122] https://thecyberexpress.com/air-france-cyberattack/
[123] https://therecord.media/hacker-group-anonymous-sudan-demands-three-million-from-sas
[124] https://therecord.media/microsoft-azure-outage-anomalous-traffic-spike-anonymous-sudan
[125] After the Qur'an burning at the end of January, several hacker groups condemned the burning and called out
[126] https://www.amnesty.org/en/latest/news/2023/08/sudan-war-crimes-rampant-as-civilians-killed-in-both-deliberate-and-indiscriminate-attacks-new-report/
[127] [128] https://www.amnesty.org/en/latest/news/2023/08/sudan-war-crimes-rampant-as-civilians-killed-in-both-deliberate-and-indiscriminate-attacks-new-report/
[129] https://en.wikipedia.org/wiki/Rapid_Support_Forces
[130] https://en.wikipedia.org/wiki/Timeline_of_the_war_in_Sudan_(2023)
[131] https://www.reuters.com/technology/musk-says-starlink-active-ukraine-russian-invasion-disrupts-internet-2022-02-27/
[132] https://www.state.gov/u-s-measures-in-response-to-the-crisis-in-sudan/
[133] https://intelcocktail.com/anonymous-sudan-interview/
[134] https://x.com/joetidy/status/1697174535026462787?s=20
[135] https://www.bbc.com/news/technology-66668053
[136] Plausible deniability is the ability to deny any involvement in illegal or unethical activities, because there is no clear evidence to prove involvement. https://politicaldictionary.com/words/plausible-deniability/
[137] https://intelcocktail.com/anonymous-sudan-interview/
[138] https://cip.gov.ua/services/cm/api/attachment/download?id=60068
[139] https://www.government.se/press-releases/2023/08/thirteenth-support-package-to-ukraine-focusing-on-ammunition-and-spare-parts/
[140] https://www.ifw-kiel.de/topics/war-against-ukraine/ukraine-support-tracker/
[141] https://www.ifw-kiel.de/topics/war-against-ukraine/ukraine-support-tracker/
[142] https://en.wikipedia.org/wiki/Unfriendly_countries_list

Disclaimer

A very special thanks
to all our experts including cyber hunters, researchers, analysts, engineers, ethical hackers and incident responders.

Why Orange Cyberdefense?

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group, providing managed security, managed threat detection & response services to organizations around the globe. As Europe's go-to security provider, we strive to build a safer digital society.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

Our organization retains a 25+ year track record in information security, 250+ researchers and analysts 18 SOCs, 14 CyberSOCs and 8 CERTs distributed across the world and sales and services support in 160 countries. We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

Orange Cyberdefense has built close partnerships with numerous industry-leading technology vendors.

We wrap elite cybersecurity talent, unique technologies and robust processes into an easy-to-consume, end-to-end managed services portfolio.

At Orange Cyberdefense we embed security into Orange Business solutions for multinationals worldwide. We believe strongly that technology alone is not a solution. It is the expertise and experience of our people that enable our deep understanding of the landscape in which we operate. Their competence, passion and motivation to progress and develop in an industry that is evolving so rapidly.

We are proud of our in-house research team and proprietary threat intelligence thanks to which we enable our customers to focus on what matters most, and actively contribute to the cybersecurity community. Our experts regularly publish white papers, articles and tools on cybersecurity which are widely recognized and used throughout the industry and featured at global conferences, including Infosec, RSA, 44Con, BlackHat and DefCon.

www.orangecyberdefense.com
X/Twitter: @OrangeCyberDef