Check Point
SOFTWARE TECHNOLOGIES LTD

CYBER SECURITY REPORT

2021

cp<r>
CHECK POINT RESEARCH

CONTENTS

"PREDICTION IS VERY DIFFICULT,
ESPECIALLY IF IT'S ABOUT THE FUTURE."

—Niels Bohr, Nobel Laureate in Physics

The year 2020 will be one that we will all remember for a very long time. Twelve months ago, very few of us could have foreseen the global disruption that would be caused by COVID-19, the worst pandemic in over a century. The seismic changes that affected our lives almost overnight continue to be felt, and will stay with us through 2021 and beyond.

With social distancing being critical to slowing the spread of the coronavirus, we needed to transform all aspects of the way we live, from working to shopping to interacting with our families and loved ones. The internet enabled us to keep our world running. Businesses globally surprised themselves with the speed and success of their digital initiatives: it is estimated that during 2020, digital transformation has accelerated and advanced by up to seven years. What was once thought to be almost impossible was achieved in just a few months.

Of course, this giant leap in connectivity and our growing reliance on technology in our everyday lives has created new challenges and problems. Just as organizations worldwide have transformed their ways of working, threat actors and cyber criminals also changed their tactics so that they could take advantage of the pandemic's disruption.

We saw huge spikes in attacks against organizations' new remote working capabilities. We witnessed surges in phishing attacks targeting home workers and consumers, aiming to steal their personal details. There were major increases in shameless ransomware exploits and sophisticated hacking attempts targeting hospitals, healthcare organizations, and the companies involved in making and shipping the critical COVID-19 vaccines.

And in December, we saw the massive Sunburst attacks which targeted many thousands of government and private-sector technology organizations worldwide via a backdoor embedded in their SolarWinds network management software. Check Point first predicted these types of multi-vector, fast-moving, large-scale Gen V attacks two years ago, and they are hitting organizations globally more frequently than ever before. All these attacks and threats continue to be on the rise today. This growing cyber pandemic has the potential to destabilize the new normal that we have carved out over the past year.

However, while COVID-19 has cast a dark cloud over the world, there are strong signs that this cloud will soon be lifting. The world's largest-ever vaccination campaign is now rolling out to protect populations against infection. This will in turn allow restrictions to be eased and enable us to take full advantage of the fantastic digital advances we made in 2020.

But to do this, we need to act now to stop the cyber pandemic spreading out of control. Just as the global vaccine roll-out will enable societies to safely emerge from lockdowns, we also need to vaccinate our hyper-connected networks to prevent the damaging cyber attacks and threats that cause so much disruption, and put security and safety at risk for all of us.

In this 2021 Cyber Security Report, we will review 2020's significant cyber threats, attacks and events, and the impact these have had on organizations worldwide. We will also look at what we expect to see in 2021's cyber landscape, to help organizations prepare themselves for what's to come and show how they can develop the strongest possible security posture. By preventing advanced cyber attacks, security is an enabler that unlocks innovation and helps to safeguard the future—for all of us.

Dr. Dorit Dor

Vice President of Products
Check Point Software Technologies

OVER **22 BILLION** RECORDS WERE EXPOSED IN DATA BREACHES WORLDWIDE IN 2020, FROM 730 PUBLICLY DISCLOSED BREACHES

—Tenable's 2020 Threat Landscape Retrospective Report

TIMELINE OF 2020'S MAJOR CYBER EVENTS

JAN

01

Travelex, a London-based foreign exchange company, had its operations crippled for weeks due to an attack by the Sodinokibi (aka REvil) ransomware gang. Travelex had entered into negotiations with the group, but refused to pay the ransom demand of $6M in exchange for the decryption keys. In retaliation, the attackers threatened to publish 5GB of customers' personal information that had been stolen and exfiltrated prior to the encryption. This was one of the highest-profile 'double extortion' ransomware attacks, in which attackers breach corporate networks, steal sensitive files, then encrypt data and demand a ransom to decrypt it, as well as threatening to publish data if the ransom demand is not met, to put additional pressure on victims.

Travelex

FEB

02

Estée Lauder, the New York-based cosmetics giant, accidentally exposed 440 million internal records to the public Internet, including internal emails, reports and documents. However, there was no evidence that customer records or payment details were put at risk.

ESTĒE LAUDER

MAR

03

The Marriott Hotels group disclosed a new data breach impacting 5.2 million hotel guests. The hotel chain discovered that a hacker had used the login credentials of two employees from one of its franchise properties to access customer information from the app's backend systems. The company informed guests via email and provided personal information monitoring services to those impacted by the breach.

Marriott

APR

04

As countries worldwide started implementing lockdowns and restrictions to slow the spread of Covid-19, a Check Point survey showed that 71% of security professionals reported an increase in security threats and attacks since the start of the coronavirus outbreak. The leading threat cited was phishing attempts (cited by 55% of respondents), followed by malicious websites claiming to offer information or advice about the pandemic (32%), followed by increases in malware (28%) and ransomware (19%).

Microsoft warned Kubernetes users of a large-scale hacking campaign that targets Kubeflow, a machine learning toolkit. The campaign aims to infect internet-facing Kubernetes instances and use them for crypto-mining at the victims' expense, using the XMRig crypto-mining malware.

Microsoft

MAY

05

Budget airline EasyJet was hacked, impacting 9 million customers and exposing the details of over 2,000 credit and debit cards. EasyJet said it has been the target of a "highly sophisticated" attacker, which gained access to and stole customers' email addresses and travel details.

easyJet

JUN

06

The University of California paid $1 million ransom to unscramble COVID-19 research data after being hit by ransomware. The attack impacted the University's School of Medicine, encrypting data on a "limited number of servers" according to a UCSF statement. The University added that although it believed no patient records were exposed by the Netwalker ransomware attack, "we made the difficult decision to pay some portion of the ransom, approximately $1.14 million, to the individuals behind the malware attack in exchange for a tool to unlock the encrypted data and the return of the data they obtained."

UCSF

JUL

07

Microsoft patched the 17-year-old SIGRed exploit that could be used to hijack Microsoft Windows Servers. The vulnerability, discovered by Check Point Research (CPR) and fixed in Microsoft's regular Patch Tuesday cycle, was awarded the highest severity rating of 10.0. The vulnerability is of particular importance to enterprises as it is wormable —or self-propagating— and as such, is able to jump across vulnerable machines without any user interaction, potentially compromising an entire organization's network of PCs in the process, making it as significant as the 2017 EternalBlue exploit, which led to the global WannaCry and NotPetya cyberattacks.

SIGRed

AUG

08

The operators of the Maze ransomware published tens of gigabytes of internal data from the networks of business giants LG and Xerox following two failed extortion attempts. The hackers leaked 50.2GB of data they claimed to have stolen from LG's internal networks, and 25.8GB of data from Xerox. This example underlines the very real threat posed by double extortion ransomware.

LG

xerox

SEP

09

A hospital patient in Germany died after being redirected from a hospital that was hit by a ransomware attack. The patient, who needed urgent medical care, died after being re-routed to a hospital in the city of Wuppertal, more than 30 km away from her initial intended destination, the Duesseldorf University Hospital, which had been hit by the attack. Germany's Federal Agency for Security in Information Technology said that the attackers breached the hospital by exploiting a flaw in Citrix software that had not been patched, despite the patch being available for several months.

CITRIX®

OCT

10

Universal Health Services (UHS), a healthcare provider with over 400 facilities in the US, UK and Puerto Rico, was hit by the Ryuk ransomware. The attack crippled its entire IT infrastructure and phone system in the US, resulting in a transition to all-paper systems.

A voter database in Hall Country, Georgia, used to verify voter signatures, was breached by ransomware, alongside other government systems, making it perhaps the first official election resource to be hit by ransomware. The 'DoppelPaymer' gang claimed responsibility for the attack.

NOV

11

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS) released a warning of an increase in Ryuk ransomware attacks on US hospitals. Check Point Research showed that the healthcare sector was the most targeted industry in the US, with a 71% increase in attacks in November compared to the previous month. Attacks increased again during December 2020.

DEC

12

On the week of December 13th, US Government offices disclosed that they had been targeted by a series of mega cyber attacks, allegedly related to state-sponsored threat organizations. The attacks targeted many government and private-sector technology organizations worldwide. This series of attacks, dubbed 'Sunburst', was made possible when hackers were able to embed a backdoor into the SolarWinds network management software. Over 18,000 companies and government offices downloaded what seemed to be a regular software update on their computers, but was in fact a Trojan. By leveraging the common IT practice of software updates to insert malware on organizations' networks, the attackers utilized the backdoor to compromise the assets of victims, both cloud and on premise, enabling them to spy on network traffic and access its data.

SUNBURST

EVERY DAY, THE WORLD FACES OVER **100,000** MALICIOUS WEBSITES AND **10,000** MALICIOUS FILES, ALL SEEKING TO STEAL, CAUSE DISRUPTION OR DAMAGE

87% OF ORGANIZATION HAVE EXPERIENCED AN ATTEMPTED EXPLOIT OF AN ALREADY-KNOWN, EXISTING VULNERABILITY

FROM ON-PREMISE TO CLOUD ENVIRONMENTS—THE SOLARWINDS SUPPLY-CHAIN ATTACK

In December 2020, just when we thought the year could not bring any more bad news, the SolarWinds attack was discovered, which swiftly took the title of the most significant cyberattack of the year. The first sign of the attack was the disclosure on December 8 by cyber security firm FireEye, who publicized that they had been breached by a highly capable APT group, during which FireEye Red Team cyber-assessment tools were stolen.

The scope of the incident became clearer several days later when Microsoft, FireEye, SolarWinds, and the US government all admitted they suffered an attack made possible by a hack to SolarWinds' core IT management software. Further investigation revealed that the attackers added a backdoor, called 'Sunburst', to a component of the SolarWinds Orion system, which was then distributed to SolarWinds customers via an automatic software update. That granted remote access to multiple high-profile organizations—making it one of the most successful supply-chain attacks ever observed.

46% OF ORGANIZATIONS HAVE HAD AT LEAST ONE EMPLOYEE DOWNLOAD A MALICIOUS MOBILE APPLICATION WHICH THREATENS THEIR NETWORKS AND DATA

AVI REMBAUM
Vice President,
Security Solutions

"Supply-chain attacks, like that involving SolarWinds, show the potential impact of previously unknown threat vectors. Core security practices, such as least privilege and segmentation, remain relevant in helping to limit the likelihood of initial breach as well as the potential for lateral expansion.

The novelty of the recent incident also informs us of the need to consider new approaches to cyber security. Application developers should consider ways of embracing DevSecOps methodologies and integrating security controls into code as well as the software development lifecycle. Security professionals should explore opportunities for implementing automated, real-time protections for identified exploits as well as extending threat prevention and hunting capabilities across all environments: network, endpoint, cloud and mobile."

The scale of the attack is huge: documents filed by SolarWinds to the U.S. SEC reveal that approximately 18,000 customers downloaded the compromised Orion software update, among them 425 companies on the Fortune 500 list. However, evidently not all customers who received the compromised update became active targets—the attackers only chose high-value entities whose network and data was actually breached. It appears that the threat actors focused primarily on technology companies, government agencies, and consultancy firms across the US, Europe, Asia and the Middle East. The victim list includes the US departments of State, Energy (DOE) and Homeland Security (DHS), the National Institutes of Health (NIH), Cisco and Microsoft, among many others.

The threat actors behind the attack, believed to be of Russian origin and with ties to the Russian Intelligence services, demonstrated top-notch capabilities. While it is not certain how SolarWinds was infected in the first place, it is suspected that the company was breached via its Office 365 accounts. The threat actors were able to forge a token for a highly privileged account in Azure Active Directory and gain admin privileges using compromised credentials. Essentially, the actor gained significant access to the on premise network of SolarWinds customers via the compromised update, and then moved laterally to the cloud environment to facilitate long-term access to the victim and obtain information, such as email files stolen via Microsoft Office 365.

"Vishing attacks are a growing cyber threat. They give the attacker control of the information channel and put additional psychological pressure on the target. Because of this, we're seeing that more and more multi-staged cyber attacks are incorporating vishing calls as part of their infection chains. Organizations should educate their employees to not overshare sensitive details such as user credentials or bank details, and to verify the authenticity of whoever they find themselves on the phone with."

LOTEM FINKELSTEEN
Manager of
Threat Intelligence

A key innovation in this attack lies in the way the attackers obtained access to cloud-based services. It seems that cloud-based services were a key objective in the supply-chain attack, and access to those was obtained via authentication systems on the compromised networks, which allowed them to penetrate these services without raising suspicions. This attack vector is fully adapted to the currently-common hybrid on-premises-cloud environments.

Organizations wishing to respond to the attack need to review both their on-premises network as well as their cloud-based services, and take the necessary steps to protect their authentication infrastructure and establish monitoring procedures to detect such attacks.

VISHING—THE NEW OLD-SCHOOL

In 2020, we saw the unwelcome return of an old social engineering method in a new guise, one well suited to the current dynamic work arrangement. Vishing, or voice phishing, is an attempt to gain access to private or corporate information or systems through fraudulent voice calls. During the phone call, the attacker leverages social engineering techniques to get the victim to open a malicious document, share sensitive information, or give the caller access to private devices.

MAYA HOROWITZ
Director,
Threat Intelligence
& Research

"Ransomware attacks have ramped up again in 2020, with the double-extortion technique putting more pressure on organizations to give in to the hackers' demands. It's estimated that ransomware has cost businesses globally $20 billion in 2020, up from $11.5 billion in 2019. To avoid being a ransomware victim, organizations must adopt a strategy of threat prevention and not rely on detection or remediation alone. They should deploy dedicated anti-ransomware solutions, virtually patch relevant vulnerabilities such as RDP, and educate employees about the risks of malicious emails that can carry the malicious payload."

Throughout 2020, a surge in successful attacks incorporating voice phishing revealed that vishing attacks are no longer limited to simple tech support scams that are easily detected by people with cyber threat awareness. Vishing can be sophisticated attacks, tailored to the victim's background and occupation. With research and a caller with good language skills, it can be used to obtain access to a corporate network.

A recent article revealed that a professional cybercriminal group was offering vishing attacks for hire, for clients seeking to access specific companies. These attacks target employees who work from home, and attempt to obtain their VPN credentials and thus gain access to the company network. One-on-one phone calls, in which the caller impersonates a helpdesk employee and demonstrates knowledge of the company and employee position, give the attacker credibility.
In August 2020, the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI issued a joint advisory warning of a wave of vishing attacks targeting U.S. private sector companies, luring employees into providing their corporate credentials.

While independent attackers or small cybercriminal groups may be behind such attacks, recently we witnessed APT groups integrating vishing into their arsenal. Groups like the Iranian Charming Kitten and the North Korean Lazarus were reported to use vishing as part of complex phishing schemes.

Advanced cybercrime groups such as the financially motivated Evilnum also adopted vishing as a more efficient and controlled tactic to ensure the success of the phishing phase.

Vishing can also be used to bypass the Two-Factor Authentication (2FA) security mechanism. In some cases, attackers used the victim's phone for authentication while attempting to access a private account. They then requested the user's 2FA code over a phone call, pretending to be a support representative. The code granted the attacker full access to the account. This technique was recently used in a campaign to take over WhatsApp accounts and leverage the victim's account to target all of the victim's contacts.

A key example was July 2020's attack on Twitter in which hackers gained access to dozens of Twitter's most high-profile accounts, including those belonging to Joe Biden and Jeff Bezos, and tweeted demands for ransom in Bitcoin that yielded more than $100K in several hours. It was later discovered that the attack was initiated by a vishing attack that convinced Twitter employees to grant access to internal tools. In November, a similar attack hit GoDaddy, the world's largest domain name registrar.

These attacks hint at the nature of the current wave of phishing attacks—sophisticated, well-planned attacks targeting specific users at high-profile organizations. Extensive reconnaissance work is probably done prior to the call to choose the employees most likely to cooperate, gather personal information about them and obtain their phone numbers. We can soon expect vishing attacks to incorporate 'deep phishing' techniques, such as a deepfake sound recording, which enables an attacker to choose the voice used in the call and mimic any person of interest, or even the face used in a video conference. Imagine receiving a call that appears to be from your workplace CEO, and follows up on a business deal, including ordering a transaction.

DOUBLE EXTORTION RANSOMWARE RAMPS UP

While conventional ransomware continues to cause disruption in organizations worldwide, threat actors introduced a new tactic in late 2019: double extortion. This is a multi-stage ransomware attack, which combines the traditional encryption of the victim's files with exfiltration of data. The attacker then threatens to release the breached data publicly unless the ransom payment is paid within the designated timeframe. This puts additional pressure on victims to meet the attackers' demands, as well as exposing the victim to penalties from data watchdogs, and the need to alert affected customers, partners and consumers whose data was breached.

RESEARCH SHOWS THAT IN **Q3 2020**, NEARLY HALF OF ALL RANSOMWARE CASES INCLUDED THE THREAT OF RELEASING STOLEN DATA, AND THE AVERAGE RANSOM PAYMENT WAS **$233,817—UP 30%** COMPARED TO **Q2 2020**.

During 2020, double extortion attacks have ramped up. The data center giant Equinix was hit by the Netwalker ransomware. The threat actor behind that attack was also responsible for the attack against K-Electric, the largest power supplier in Pakistan, demanding $4.5 million in Bitcoin for decryption keys and stopping the release of stolen data. The business model of double extortion attacks has proved so efficient that traditional ransomware techniques do not compare.

Other companies known to have suffered such attacks include the French system and software consultancy Sopra Steria, with major financial and healthcare sector customers; the Japanese game developer Capcom; the Italian liquor company Campari Group; the US military missile contractor Westech; the global aerospace and electronics engineering group ST Engineering; travel management giant CWT, who paid $4.5M in Bitcoin to the Ragnar Locker ransomware operators; and business services giant Conduent, who was hit by the Maze ransomware, possibly via a vulnerable Citrix server.

And that's just the average ransom paid. In a recent attack using the prominent Ryuk ransomware, the victim paid the remarkable ransom of 34 million USD, or 2200 Bitcoin (BTC). And of course, even when ransom demands are met, there is still no guarantee that the attackers will honor their promise to release the files.

Attackers are also refining double extortion techniques to put extra pressure on the companies who are unwilling to pay. The Ragnar Locker ransomware group, for example, utilizes hacked accounts to run Facebook ad campaigns, stating that large amounts of sensitive customer data was indeed collected, refuting the statements often released by targeted companies.

Going forward, some attackers already realized that the threat of data leakage might be even greater than the ransomware stage, and skipped the ransomware altogether—as was the case with Vastaamo, a Finnish psychotherapy clinic with over 40,000 patients. For over a year, the hackers managed to collect information belonging to tens of thousands of patients. In a unique twist, the hackers sent direct email to both the clinic and the patients, threatening to release the data. Approximately 530,000 USD in BTC were demanded from the healthcare provider, while a sum of 200-500 USD in BTC was requested from the patients to prevent the release of their therapist session notes. The medical records of 300 patients were released to expedite the payment. Involving customers in extortion processes guarantees that the incident becomes public knowledge at a very early stage, putting additional public pressure on the victimized organization, forcing it to follow regulations and alert law enforcement agencies as well as affected personnel.

'HELLCARE'—HAVE HEALTHCARE ATTACKS GONE TOO FAR?

In March 2020, as the extent and severity of the global COVID-19 pandemic became clear, several threat groups, including Maze and DoppelPaymer, pledged to refrain from attacking healthcare institutions, which were struggling to keep up with the increasing work load, researching the virus and dealing with an overwhelming number of patients. Some of the groups even went so far as promising to provide free decryption services for institutions who were mistakenly attacked. Among these groups was the prominent Maze ransomware group, who committed to the following statement: *"We also stop all activity versus all kinds of medical organizations until the stabilization of the situation with virus."*

As 2020 progressed, it became increasingly obvious that such promises hold no substance. In fact, in 2020, attacks targeting healthcare facilities, medical institutions and pharma research centers, were executed at an unprecedented rate. In early April, Hammersmith Medicines Research Ltd. (HMR), a research firm that was at the time on standby to perform trials of COVID-19 vaccines in humans, suffered a data breach caused by the Maze ransomware. The investigation revealed that the breach occurred on March 14, almost in parallel to the Maze group's pledge. As HMR decided not to pay the ransom, the data was published on Maze's designated web page.

MONTHLY CYBER ATTACKS PER HEALTHCARE ORGANIZATION
JAN 2020 - JAN 2021

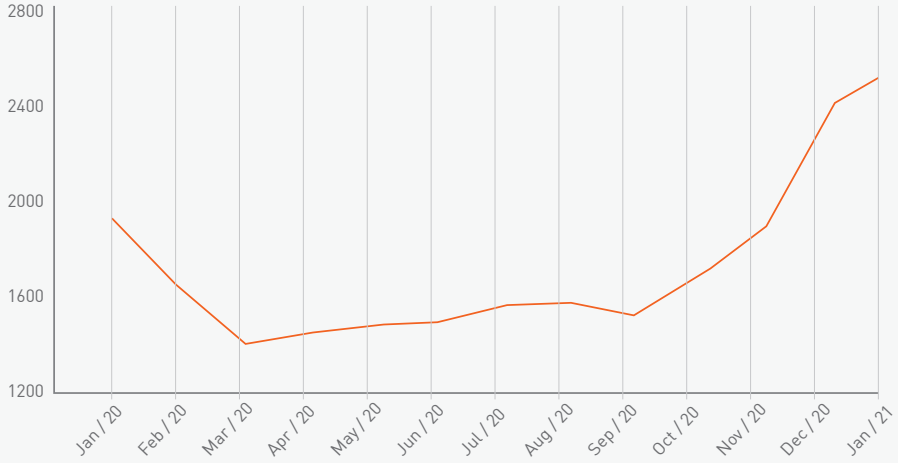


Figure 1: March 2020 Ransomware groups pledged to avoid attacking healthcare institution. In reality, healthcare attacks increased sharply towards the end of the year.

Shortly afterward, we observed an escalation in healthcare-related attacks, as threat actors began focusing on medical facilities working to mitigate the coronavirus contagion, as well as pharmaceutical institutions working to develop a vaccine. This activity continued through 2020.

Recent Check Point Research from October shows that healthcare is currently the most targeted industry in the US, with a 71 percent increase in attacks compared to September. The chart above shows the sharp increase of healthcare-sector attacks compared to the global increase. In November and December 2020 there was an increase of over 45 percent in the amount of attacks targeting healthcare organizations globally—double the global increase of attacks seen in the same time period across all industry sectors (22 percent).

This chart demonstrates the increase in attack rate per healthcare organization throughout 2020 and the beginning of 2021.

Towards the end of October, the U.S. CISA, FBI, and HHS released a warning about an increase in Ryuk ransomware attacks on U.S. hospitals, mentioning the prominent Trickbot multi-purpose malware which is used to deploy Ryuk in the victim's network.

We also saw nation-sponsored APT groups, including the North Korean Lazarus Group and Russian Fancy Bear, targeting institutions involved in COVID-19 treatment and vaccine development. Spear-phishing based on pandemic-related themes are the most commonly used tactic. It seems that both hackers and state-related groups, looking to promote their national interests and make a

"Cyberattacks on the global healthcare sector are getting out of control, because criminals view hospitals as being more willing to meet their demands and actually pay ransoms—and the events of 2020 proved this. The usage of Ryuk ransomware emphasizes the trend of having more targeted and tailored ransomware attacks rather than using a massive spam campaign, which allows the attackers to make sure they hit the most critical parts of the organization and have a higher chance of getting their ransom paid."

OMER DEMBINSKY
Manager of Data Research

global impact, decided to focus on institutions promoting the global fight in the pandemic, thus putting countries' citizens in the front line of their attacks.

THREAD HIJACKING—YOUR OWN EMAILS COULD BE USED AGAINST YOU

One of the cornerstones of good security today is cyber security awareness training for company employees. This should include an extensive list of do's and don'ts in a corporate environment. One common golden rule is to suspect any email attachments that weren't sent from your colleagues or trusted partners. But what happens when you receive a reply to an old corporate thread with an update attached? Do you open it as a matter of course, or should you be suspicious?

Emotet, originally a banking malware and now one of the largest botnets in the cyber landscape, has consistently topped the malware rankings at Check Point Research for several months, targeting almost 20% of global organizations in the past year.

One of the keys to the astonishing success of Emotet's spam campaigns, is a simple yet sophisticated phishing technique called thread hijacking. Once a single victim is infected, the attackers leverage that person's old email conversations for malware distribution, forwarding the last email of the thread and adding malicious files as attachments. This makes it easier to trick new victims that are within the victim's social and professional domain, as from their perspective they're receiving an email from a trusted colleague concerning a known subject.

EMOTET, ORIGINALLY A BANKING MALWARE AND NOW ONE OF THE LARGEST BOTNETS IN THE CYBER LANDSCAPE, HAS CONSISTENTLY TOPPED THE MALWARE RANKINGS AT CHECK POINT RESEARCH FOR SEVERAL MONTHS, TARGETING ALMOST **20%** OF GLOBAL ORGANIZATIONS IN THE PAST YEAR

In the case of Emotet, email threads, often chosen for their engagement in wire transfers or sensitive proprietary information, are hijacked by the attackers and sent to their C&C servers. The attackers then spoof one of the email addresses used in the thread and impersonate a reply to the hijacked email. Targeted users can be part of the original conversation, or new users within the organization. Sometimes, legitimate files stolen from the network are attached to the phishing email in addition to the malicious file. The thread hijacking technique has even been utilized in an Emotet attack targeting Quebec's Department of Justice and successfully infected dozens of users. This technique, together with Emotet's large distribution proved to be so effective that the French Interior Ministry reacted by blocking all Office documents (.doc) from being delivered via email.

Recently another prominent malware variant added thread hijacking to its arsenal: the Qbot banking malware, also called Qakbot. The new version of the malware, released at the end of July and analyzed by Check Point Research, features a module called 'email collector' which is capable of hijacking Microsoft Outlook email threads. The module extracts all email conversations from the victim's client, uploads them to a remote server, and uses them in malicious spam campaigns. Observed stolen emails include subjects related to COVID-19, tax payment reminders and job recruitments. The Qbot campaign was distributed worldwide, but focused on US users and on the government and military sectors.

More creative implementation of the thread hijacking technique has also been observed this year. Check Point Research recently came across an incident in which hackers managed to gain access to a user's WhatsApp account and distribute malware to the victim's contact by replying to existing WhatsApp correspondences. The attackers used vishing to obtain the 2FA password provided to the victim via SMS.

YANIV BALMAS
Head of Cyber Research

"Even older forms of malware can be updated with new features to make them a dangerous and persistent threat. The threat actors behind Qbot and Emotet invest heavily in development to enable data theft on a massive scale from organizations and individuals. We strongly recommend organizations educate employees to watch their emails closely for signs that indicate a phishing attempt—even when the email appears to come from a trusted source. They should also use an email security solution."

Both Emotet and Qbot are more than just prominent malware in the cyber landscape—their ongoing success has turned them into trend setters. We therefore estimate that the thread hijacking technique will quickly be adopted by other threat actors across the spectrum from state-backed espionage groups to financially motivated hackers.

REMOTE ACCESS VULNERABILITIES

As the coronavirus spreads worldwide, the social distancing policies enacted due to the pandemic shifted a substantial number of employees from corporate offices to home working. Network admins had to rapidly adjust to the requirements of working remotely and implement remote access platforms within their organizations. Unfortunately, these often resulted in misconfigurations and vulnerable connections, allowing attackers to leverage these flaws to access corporate information.

As a result, the first half of 2020 saw an increase in attacks against remote access technologies such as Remote Desktop Software (RDP) and VPN, as well as a sharp rise in brute force attacks on RDP servers. In fact, several researchers found that in the first half of the year, RDP was the most popular intrusion vector, as well as the greatest ransomware delivery platform, surpassing phishing emails. Another report concluded that during the first months of the pandemic, almost a million attack attempts against RDP connections were observed every day.

"Attackers will always look for organizations that have vulnerable, unpatched systems so that they can get easy access, like a car thief looking for an unlocked car. To prevent hackers having an easy ride, we strongly recommend users patch their servers regularly to prevent exploitation of such vulnerabilities. IPS prevents attempts to exploit weaknesses in vulnerable systems or applications, protecting you in the race to exploit the latest breaking threat, and comprehensive endpoint protection is crucial to avoid security breaches."

ADI IKAN
Network Research & Protection Group

In the second half of the year, attackers embraced a more calculated approach, aiming to ensure that even after organizations implement their remote access platforms properly and minimize their misconfiguration incidents, remote connection services will continue to enable corporate attacks. Instead of searching for misconfigured servers, they began exploiting vulnerabilities in remote access services, fueled by a large number of newly disclosed vulnerabilities in perimeter and remote access devices. This list includes IBM WebSphere Application Server, Oracle WebLogic, Microsoft Remote Desktop Gateway, Citrix NetScaler Gateway, Citrix ADC, Cisco ASA & Firepower, Oracle iPlanet Web Server, and more.

This bumper crop of new vulnerabilities is the direct result of the increasing adoption of these devices amid the COVID-19 pandemic's 'new normal' and the increased interest of security researchers in remote access platforms. Nation-backed threat groups running long-term espionage operations also leveraged both old and newly discovered remote access vulnerabilities to gain initial footholds in their target networks.

The Iranian Fox Kitten group, which was observed targeting organizations from the oil and gas, aviation, government IT and security sectors throughout the past three years, exploits known vulnerabilities in systems with unpatched VPN and RDP services as their

INCREASE IN ATTACKS EXPLOITING VULNERABILITIES IN REMOTE ACCESS PRODUCTS 2019-2020

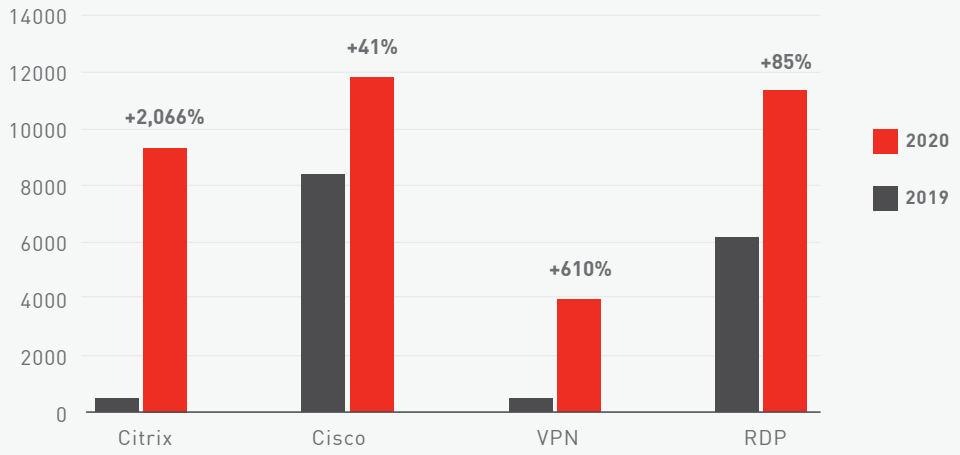


Figure 2: APT Groups Integrate New and Old Remote Access Vulnerabilities to Gain Initial Foothold.

primary infection vector. The China-affiliated group APT 41 exploited vulnerabilities in Cisco and Citrix applications in a campaign focused on the industrial, telecommunications, financial, and healthcare sectors.

In October 20, the NSA published a detailed report listing the top 25 vulnerabilities currently being leveraged and exploited by Chinese threat actors. The flaws that made the list were exploited 7 times more than other vulnerabilities in 2020. The above chart displays the increase in attacks exploiting vulnerabilities in remote connection products.

Check Point Research's top 20 most exploited vulnerabilities, as collected by our Intrusion Prevention System (IPS) sensor net, includes 8 vulnerabilities for remote access devices. Among these vulnerabilities are **Cisco Unified IP Conference Station 7937G Denial of Service (CVE-2020-16139), Citrix XenMobile Server Directory Traversal (CVE-2020-8209)** and **Citrix ADC Reflected Cross Site Scripting (CVE-2020-8191).**

While researchers continued their work of investigating and identifying vulnerabilities in remote access platforms, skilled and not-so skilled attackers alike used the time frame between vulnerability disclosure and the actual patching of systems to unleash attacks and to strengthen their hold on corporate targets worldwide.

ISAAC DVIR
Director,
Mobile Solutions

"As we rely more on our mobile devices to stay connected and manage our lives, attackers are increasingly targeting them via sophisticated malware, malicious apps and trying to exploit vulnerabilities. Enterprises need to adopt mobile security that can seamlessly protect unmanaged devices from these advanced cyber threats, and users should be careful to use only apps from official app stores to minimize their risk."

MOBILE—FROM COVID-19 TO ZERO-CLICK ATTACKS

COVID-19 dominated the mobile cyber-threat landscape as it did every other aspect of life in 2020. As well as the introduction of several malicious applications masquerading as legitimate coronavirus-related apps, there was increasing concern over data privacy issues in the official tracking applications developed by national governments.

The increased use of mobile devices during lockdown and social distancing may also be responsible for the substantial growth in banking Trojan malware families. The Guildma threat actor introduced Ghimob, which is capable of performing transactions on accounts with financial institutions in Brazil, Paraguay, Peru, Portugal, Germany, Angola and Mozambique. The newly discovered EventBot focuses on targets in the U.S. and Europe while ThiefBot aims at Turkish users. The list continues with BlackRock, Wroba, TrickMo and others, all of which show the increase in baking Trojans' activity.

Advanced Persistent Threat (APT) activity through mobile devices continued, spreading MRATs (Mobile Remote Access Tools) and continually refining their capabilities. In some cases, like that of Iranian Rampant Kitten APT, the threat actor used a combination of fake mobile applications, Windows infostealers, and Telegram phishing pages to utilize stolen Two-Factor Authentication (2FA) codes to spy on Iranian expat citizens. Both espionage and financially-motivated groups targeted MFA mechanisms as a prime objective in their surveillance activity.

"Check Point's CloudGuard has been key in enabling us to add new cloud workloads and services without needing to constantly review or deploy new security infrastructure. This means we can focus on the critical public-facing tasks where we can add real value. Right now we are building our vaccination management systems, and our cloud-first approach gives us the agility and scalability we need to roll it out nationally while being sure that data and services are secured."

DERYCK MITCHELSON
Chief Information Security Officer, NHS Scotland

NHS SCOTLAND

Major vulnerabilities reported this year in mobile hardware and popular applications may mark a shift in attack strategies, which are currently based on disguised malicious applications or OS vulnerabilities. Previously, in most cases the attackers gained an initial foothold through malicious applications or OS flaws, but in 2020 we saw an increase in reports of vulnerabilities in mobile hardware and popular applications.

The Achilles family of vulnerabilities revealed more than 400 weaknesses in a Qualcomm chip that affects a large portion of the entire mobile market. Zimperium pointed at additional weak points in Android phone hardware that can be exploited to result in a full takeover. The most popular apps were found to expose their users to potential exploitation. Instagram was reported to have an RCE zero-click vulnerability in its JPEG decoder. Apple's 'sign in' system vulnerability can allow remote attackers to bypass authentication and take over targeted accounts. Additional vulnerabilities were detected in WhatsApp, Facebook, and more.

TSION (TJ) GONEN
Head of
Cloud Product Line

"The rate of cloud migrations and deployments has raced ahead of security teams' abilities to defend them against attacks and breaches. Over 80% of organizations say their traditional security solutions either don't work at all, or only provide limited functions in cloud environments—creating a great opportunity for threat actors targeting the cloud. To close these security gaps, enterprises need to get holistic visibility across all their public cloud environments, and deploy unified, automated cloud-native protections. This way, they can keep pace with business demands while ensuring continuous security and compliance."

PRIVILEGE ESCALATION IN THE CLOUD

The COVID-19 pandemic has driven a systematic shift in corporate network architecture. The urgent need for remotely administered, agile, and scalable networks has accelerated moves to a cloud infrastructure, which allows flexibility in scale and resource management, and is accessible from anywhere. A recent study shows that the cloud market increased by almost 40 percent in the first quarter of 2020 alone, and reveals the growing popularity of hybrid cloud networks. By 2025, it is predicted that the market will exceed more than twice its current value.

Attackers have taken note of this massive migration to hybrid cloud technologies. Dark Halo, the threat actor behind the notorious SolarWinds supply chain compromise which breached 18,000+ organizations, has heavily relied on the hybrid cloud model to access sensitive information and establish persistence on targeted organizations. Once an organization is compromised, the attacker moves laterally from the organization's SolarWinds server to the on-premise Active Directory Federation Services (ADFS) server —a service responsible for the organization's Single Sign On to access cloud services like Office 365. At this point, the attacker utilizes a previously published technique to create a so-called "Golden SAML," which gives the attacker persistent and hard to detect full access to the victim's cloud services.

Overall, in the past year we saw a change in the nature of cloud misconfigurations, their root causes and their consequences, as identity and access management (IAM) misconfigurations began making headlines. These targeted cloud account attacks, sometimes caused by flaws in the provider's permissions or trust policy logic, could allow an attacker to gain privilege escalation and move laterally within the corporate's cloud environment, thus obtaining certificate private keys, sensitive information and database credentials.

Essentially, there is a shift to attacking cloud accounts instead of cloud resources. This new way of using the cloud has opened the door for attack vectors based on role assumption —the ability to obtain short-term permissions to authorized resources—that often enables vast operations within the environment, including data theft. According to researchers, Identity and Access Management (IAM) roles can be abused by 22 APIs found in 16 Amazon services. Privilege escalation exploits based on permission settings can also be found on Salesforce, which unlike AWS, is a SaaS (Software as a Service).

This new class of privilege escalation attacks, leveraging structural components of the cloud infrastructure, can often be achieved by chaining several vulnerabilities and misconfigurations together. Initial access can be obtained via a vulnerable cloud-hosted application, and used by the attackers to obtain the token required to gain elevated permissions and move laterally within the different segments of the environment, gradually escalating privileges. These attacks rely on understanding the components, architecture, and trust policy of both IaaS (Infrastructure-as-a-Service, such as Amazon) and SaaS providers to construct sophisticated multi-stage attacks, unlike the previously-common data breaches, which mostly relied on misconfigured settings such as publicly exposed S3 buckets.

WHILE 2020 HAS BEEN A YEAR MANY WOULD RATHER FORGET, WE HAVE ALSO SEEN MANY SUCCESSFUL ACTIONS BY GLOBAL LAW ENFORCEMENT ORGANIZATIONS, SUPPORTED BY THE CYBER SECURITY COMMUNITY, IN TRACKING DOWN AND INDICTING NUMEROUS INDIVIDUALS AND THREAT GROUPS INVOLVED IN CYBER-CRIME AROUND THE WORLD.

SILVER LININGS IN 2021

> In October, the notorious 'Trickbot' cyber-crime infrastructure of over a million infected machines globally was taken down in coordinated action by vendors and law enforcement. This example and others show how close co-operation between security researchers, software vendors, law enforcement and government agencies can mitigate and even eliminate major cyber-threats and disruptive attacks which can impact all of our lives. Based on these successes, we are optimistic that 2021 will offer many more positive examples of how cyber-threats are being overcome.

Countries cooperated in extraditing cybercriminals to stand trial in foreign countries, achieving high levels of international cooperation. Europol headed several of these investigations, including the DisrupTor operation in which 179 vendors of illicit goods on Dark Web forums were arrested and seized illegal goods including drugs, cash and cryptocurrencies, and weapons.

Actions against individual hackers resulted in arrests as in the case of the 17-year-old Florida resident behind the celebrity Twitter hack. A Check Point Research report to the Brazilian law authorities exposing the identity of 'VandaTheGod,' who operated a 7-year website defacement and infostealing campaign against governments around the globe, ended up with his arrest. The GandCrab affiliate who used the notorious MaaS to extort victims in more than 100 countries was arrested in Belarus.

The global effort to expose individuals behind APT and state cybercrime activity continued. Germany issued arrest warrants for a Russian military intelligence officer suspected of hacking servers in the German parliament. U.S. authorities arrested a member of the Fin7 hacking group, who was connected to the theft of more than $1 billion. Six Russian nationals, members of the GRU, were accused of masterminding the Sandworm attacks on Ukrainian infrastructure and French elections, as well as the NotPetya ransomware outbreak and the Olympic Destroyer attack.

The U.S. government also filed charges against five Chinese nationals, part of the APT41 Chinese group, for hacking into more than 100 companies. Two Malaysian businessmen were arrested by local authorities for cooperating with APT41 activity. Concluding a three-year investigation, the U.S. Department of Justice charged four Chinese military-backed hackers in the Equifax breach which affected nearly half of all Americans.

It isn't just groups and individual threat actors that have been pursued. In many cases, cyber agencies targeted and successfully shut down criminal operations' infrastructure. In October, Microsoft, together with several federal agencies, took down the infrastructure behind the Trickbot botnet. Notorious for its malicious partnerships with other malware groups, which often resulted in ransomware deployment, it was marked as a major threat to the U.S. 2020 elections. This was not the first Microsoft-led effort of the year. In March, it acted against the Necurs botnet, breaking its DGA mechanism and blocking future domain registration.

COVID-19 has pushed various forces to unite in an effort to battle cyber attacks. The British NCSC (National Cyber Security Centre) increased its takedown service abilities and recruited the public in an effort to shutdown coronavirus-related scams, resulting in more than 22,000 malicious COVID-19 related URLs that were taken down. The pandemic brought together efforts like the Cyber Threat Coalition (CTC), uniting the efforts of thousands of security professionals to collect, analyze and share COVID-19 related IoCs. The CTI League established a global volunteer response community to protect life-saving sectors related to the pandemic.

Governments are actively scanning networks for weaknesses and alerting CISOs accordingly. The British NCSC reported it had scanned one million NHS (National Health Service) IP addresses with 51,000 IoCs shared.

Another area showing positive results is vulnerability reporting and information sharing, and especially zero-day investigations. Zero-day exploits are unknown to software vendors and thus can be exploited by threat actors. Check Point Research found and reported a 10.0 CVE score vulnerability in Microsoft Azure, allowing Microsoft to patch it and protect users from malicious cloud takeovers. Similarly, Check Point Research reported SIGRed, a 10.0 vulnerability in Windows DNS servers. Cross-industry alerts promoted patching against the Pulse Secure VPN vulnerability, the F5 BIG-IP exploitation, and more. Malware itself is not free of vulnerabilities and an Emotet buffer overflow bug acted as a kill switch and allowed researchers to stop its activity for a six months period in 2020.

This pause in Emotet activity was followed in January 2021 by the news that an international operation by police in several countries had succeeded in bringing down the Emotet botnet, which for many years had been regarded as one of the world's most dangerous malware variants.

This example and others show how close co-operation between security researchers, software vendors, law enforcement and government agencies can mitigate and even eliminate major cyber-threats and disruptive attacks which can impact all of our lives. Based on these successes, we are optimistic that 2021 will give many more positive examples of how cyber-threats are being overcome.

THE DATA PRESENTED IN THE FOLLOWING SECTIONS OF THIS REPORT ARE BASED ON FINDINGS DRAWN FROM THE CHECK POINT THREATCLOUD CYBER THREAT MAP BETWEEN JANUARY 1ST AND DECEMBER 31ST 2020.

5 GLOBAL MALWARE STATISTICS

CYBER ATTACK CATEGORIES BY REGION

GLOBAL

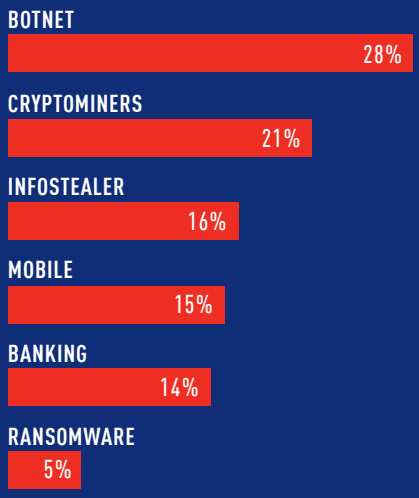


Figure 3: Percentage of corporate networks attacked by each malware type.

AMERICAS

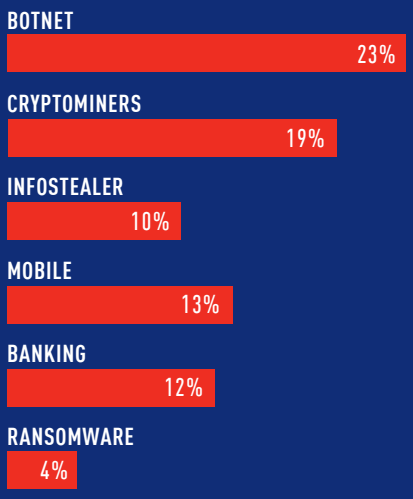


Figure 4: Percentage of corporate networks attacked by each malware type.

CYBER ATTACK CATEGORIES BY REGION

EMEA

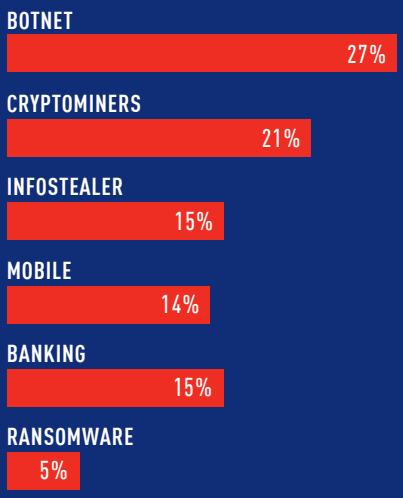


Figure 5: Percentage of corporate networks attacked by each malware type.

APAC

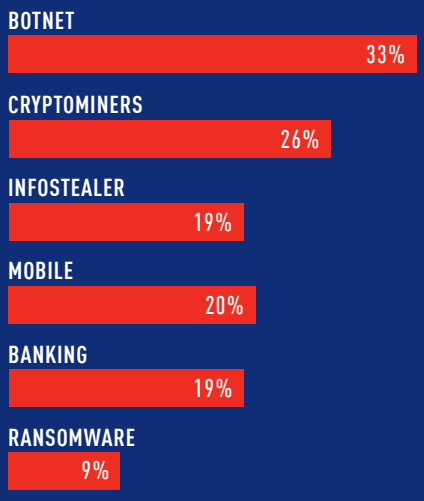
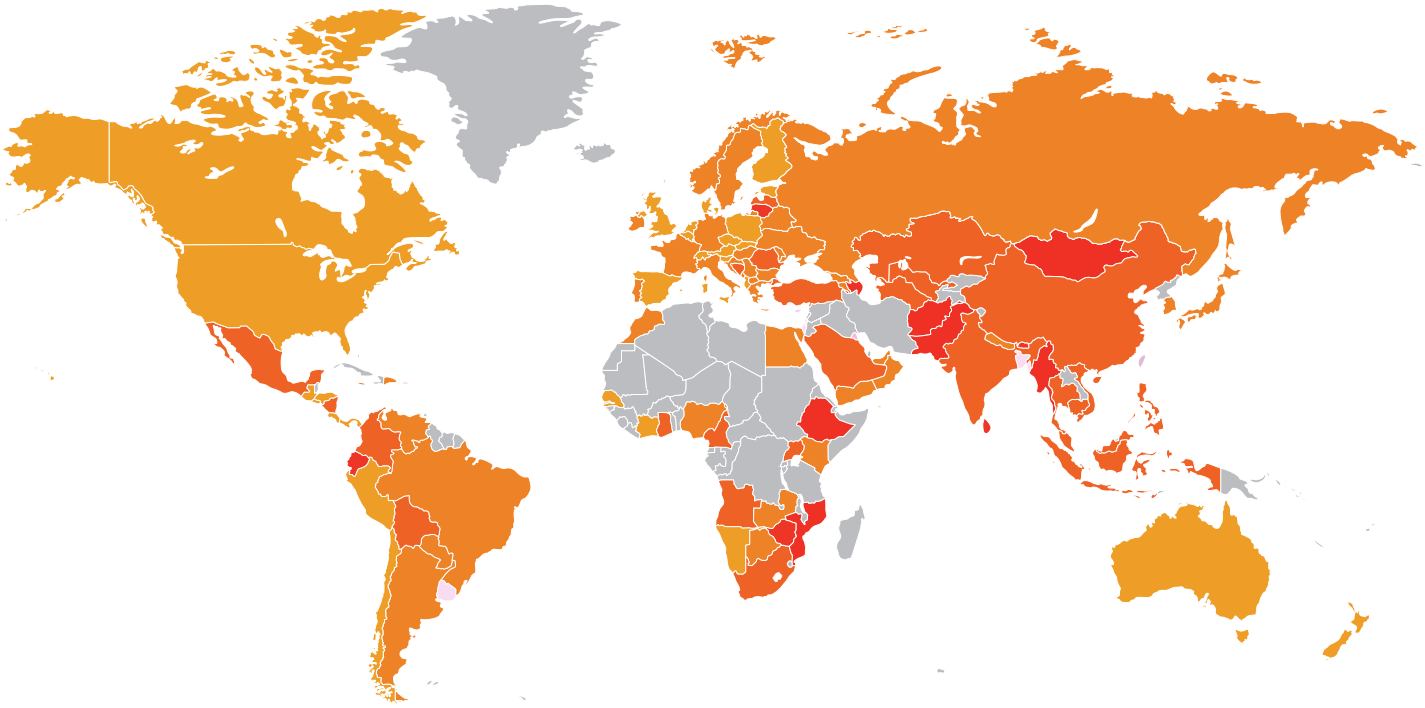


Figure 6: Percentage of corporate networks attacked by each malware type.

GLOBAL THREAT INDEX MAP

The map displays the cyber threat risk index globally, demonstrating the main risk areas around the world.*



* Darker = Higher Risk
Grey = Insufficient Data

Figure 7.

TOP MALICIOUS FILE TYPES – WEB VS. EMAIL

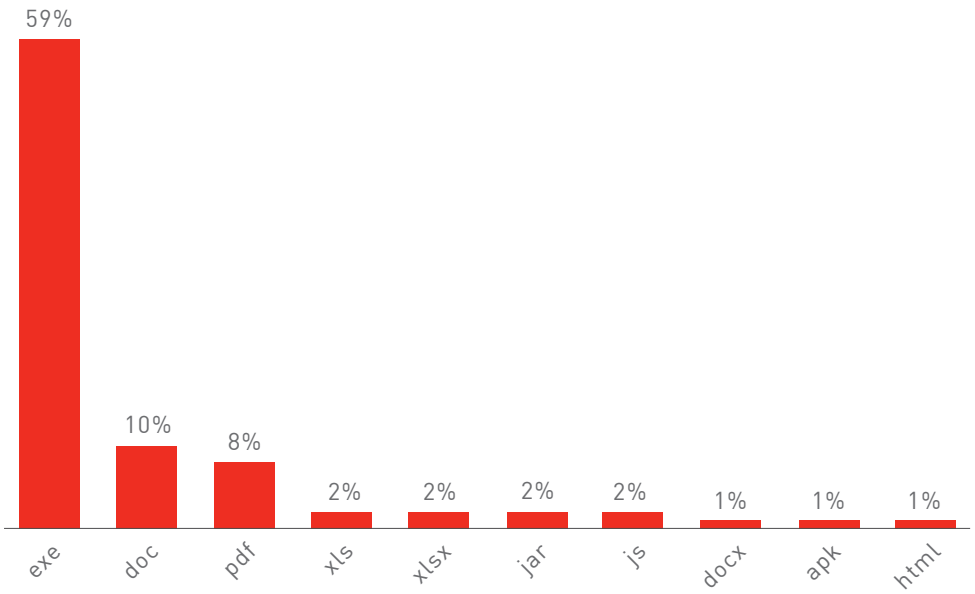


Figure 8: Web—Top Malicious File Types.

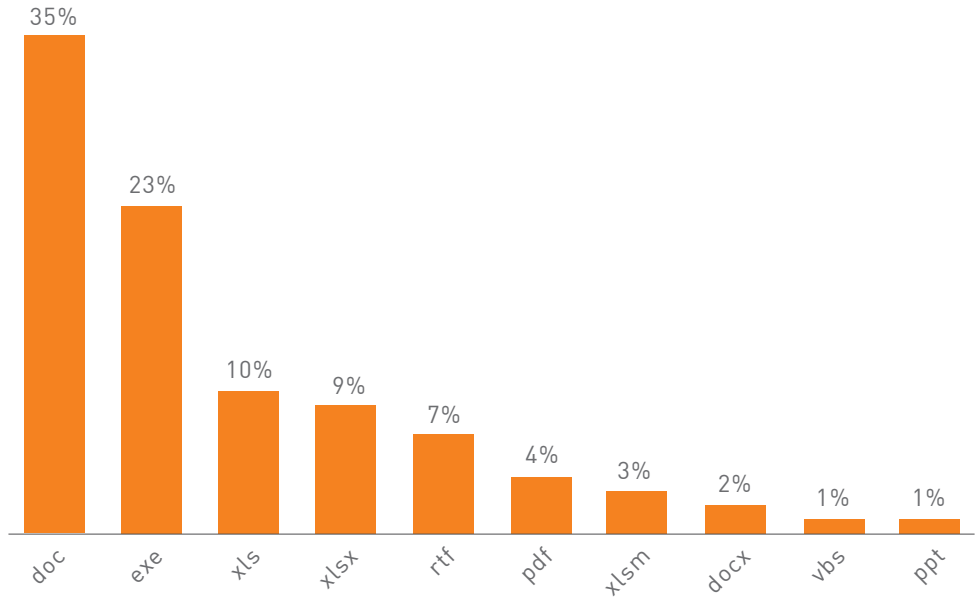


Figure 9: Email—Top Malicious File Types.

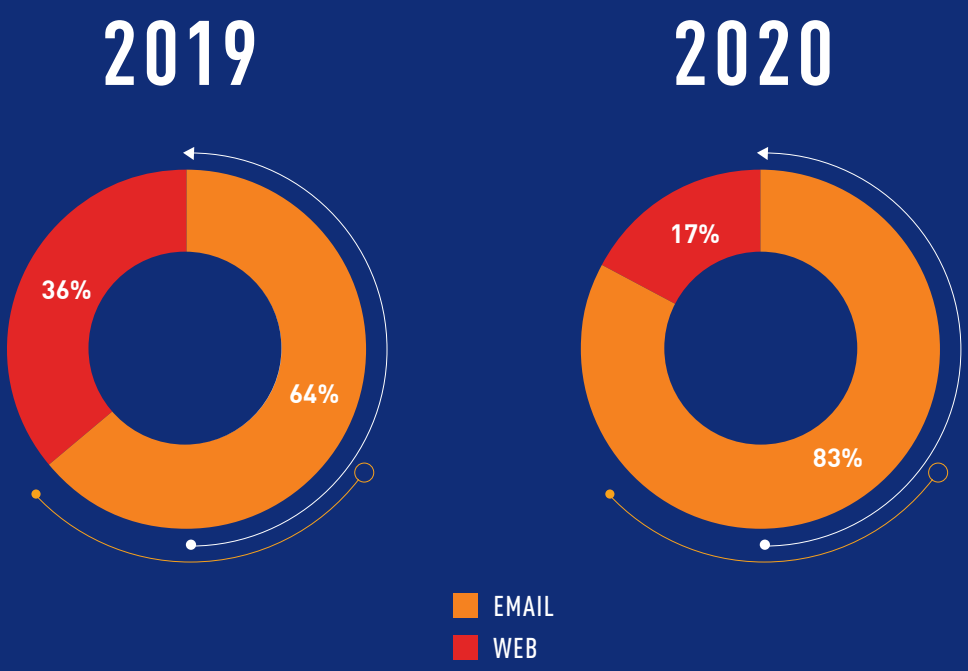


Figure 10: Distribution Protocols—Email vs. Web Attack Vectors in 2019 and 2020.

The chart above shows a significant increase of almost 20% in the distribution of email-based attacks compared to web attack vectors. The spike is in line with the 2020 event timeline and the end of life for Flash Player that made exploit kits less effective. The COVID-19 pandemic alone, that has been creatively leveraged by attackers since its inception, led to a 220% increase in the phishing email attack rate.

Other current events that were heavily exploited by cybercriminals and threat groups include Black Lives Matters, the 2020 presidential election and global shopping days.

GLOBAL MALWARE STATISTICS

Data comparisons presented in the following sections of this report are based on data drawn from the Check Point ThreatCloud Cyber Threat Map between January and December 2020.

For each of the regions below, we present the most prevalent malware.

TOP MALWARE FAMILIES

GLOBAL

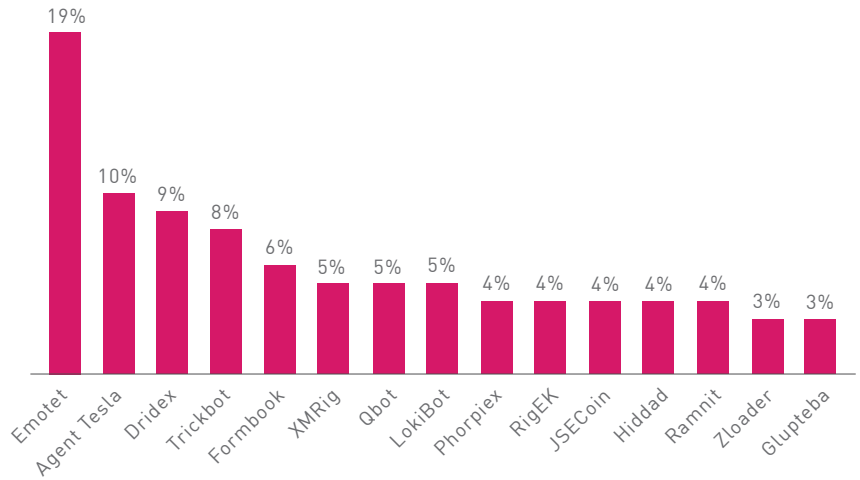


Figure 11: Most Prevalent Malware Globally.
Percentage of corporate networks attacked by each malware family.

AMERICAS

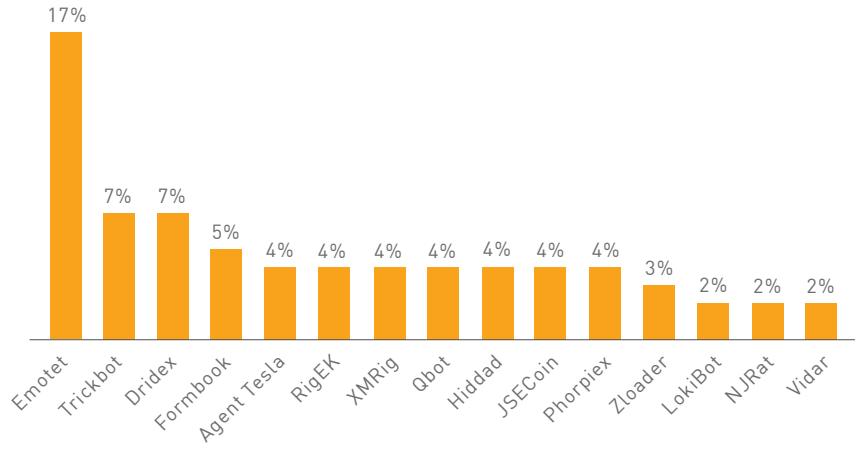


Figure 12: Most Prevalent Malware in the Americas.

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

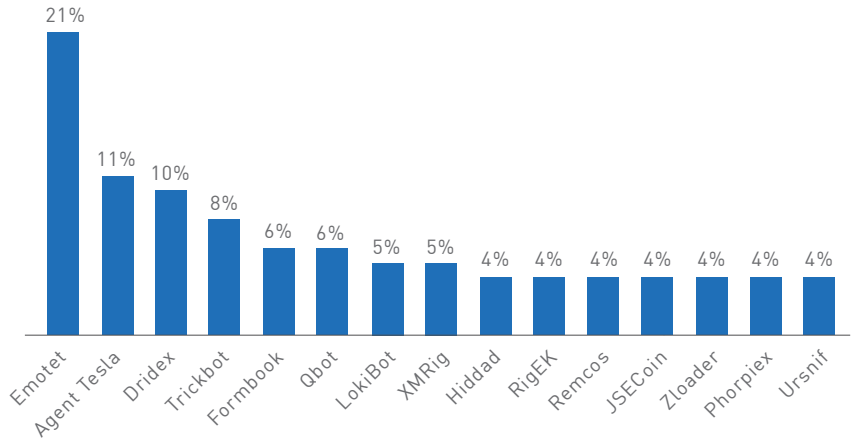


Figure 13: Most Prevalent Malware in EMEA.

ASIA PACIFIC (APAC)

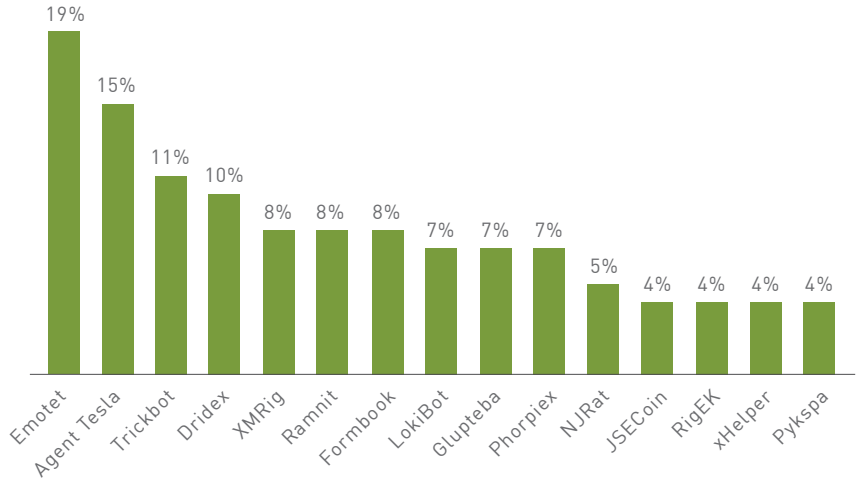


Figure 14: Most Prevalent Malware in APAC.

IN THE FINAL WEEK OF JANUARY 2021, INTERNATIONAL LAW ENFORCEMENT AGENCIES SEIZED CONTROL OF THE EMOTET INFRASTRUCTURE, AND IS IN THE PROCESS OF DISMANTLING IT: A MAJOR VICTORY IN THE ONGOING BATTLE AGAINST MALWARE.

GLOBAL ANALYSIS OF TOP MALWARE

Many malware families were able to maintain their global rank from 2019, with only slight movements up or down. Agent Tesla and Formbook, two commodity infostealers, climbed from the lower ranks to the top five. Drive-by cryptominers like Cryptoloot, moved down or dropped from the top 10 altogether.

Emotet, a botnet responsible for the distribution of Trickbot, Qbot and more, in some cases resulting in a ransomware attack, was the most heavily distributed malware family in 2019 and 2020. The yearly statistics reflect the botnet's prominent share of the threat landscape despite periodic months-long activity breaks. The longest "break" took place between February to July 2020, and reduced Emotet's impact on the first half of the year.

Emotet also leveraged the United States 2020 Presidential elections in a spam campaign distributing letters allegedly from the Democratic National Convention's Team Blue initiative. Emotet has missed out on prime months early in the pandemic during its break, but its return in July still allowed it to capitalize fully. After another two-month break, Emotet resumed its attack activities on Christmas Eve, in a campaign targeting over 100,000 users per day. The botnet updated its payloads, improved detection evasion capabilities and changed its malicious macro document to disguise the payload installation flow.

TOP MOBILE MALWARE

GLOBAL

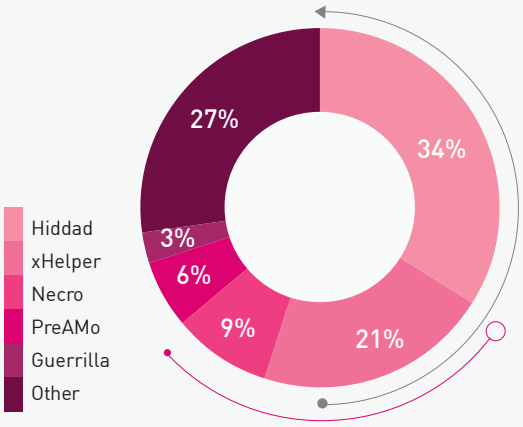


Figure 15: Top Mobile Malware Globally

AMERICAS

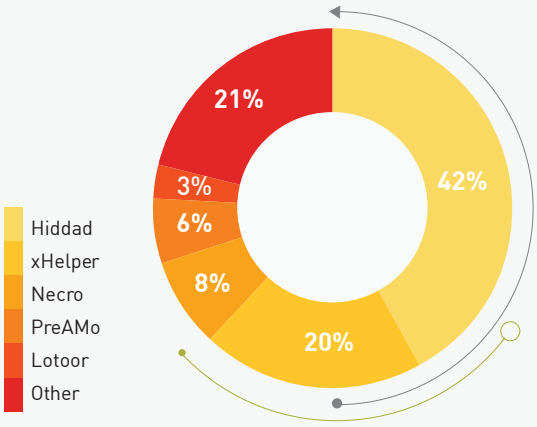


Figure 16: Top Mobile Malware in the Americas

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

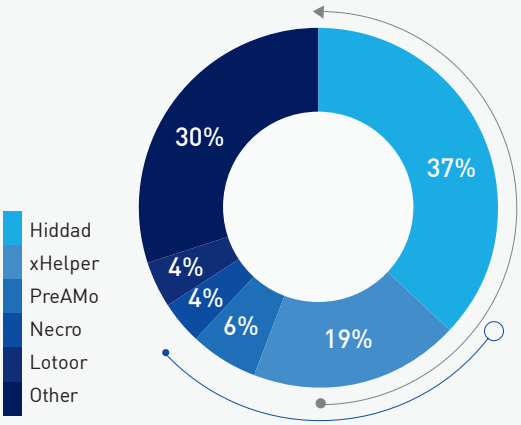


Figure 17: Top Mobile Malware in EMEA

ASIA PACIFIC (APAC)

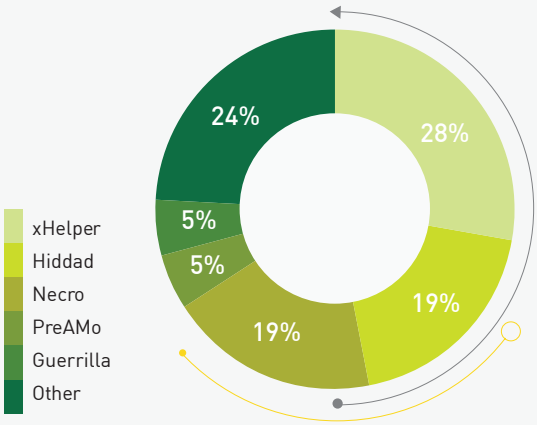


Figure 18: Top Mobile Malware in APAC

MOBILE MALWARE GLOBAL ANALYSIS

Hiddad, short for 'Hidden Ad', rose from 4th place in 2019 to the top of the global chart this year. The malware, designed to display ads and collect system information, features simple, yet clever ways to keep itself on the victim's device —it hides its icon from the app launcher, and masquerades as other apps post-installation, such as "Google Play Service" and "Google Play Store." This year, the malware joined the COVID-19 trend, and disguised itself as a coronavirus information app for Arab speakers. Upon infection, the malware displays heavy, full-screen advertisements on a timely basis.

TOP BOTNETS

GLOBAL

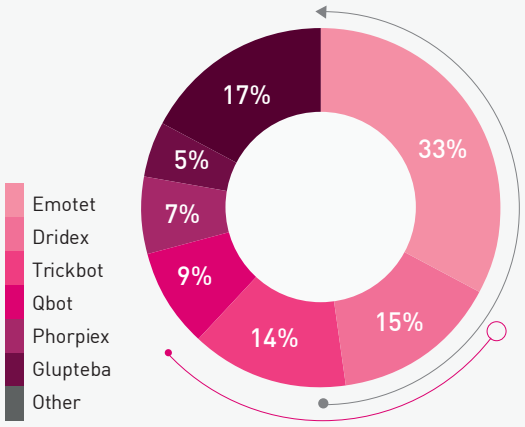


Figure 19: Most Prevalent Botnets Globally

AMERICAS

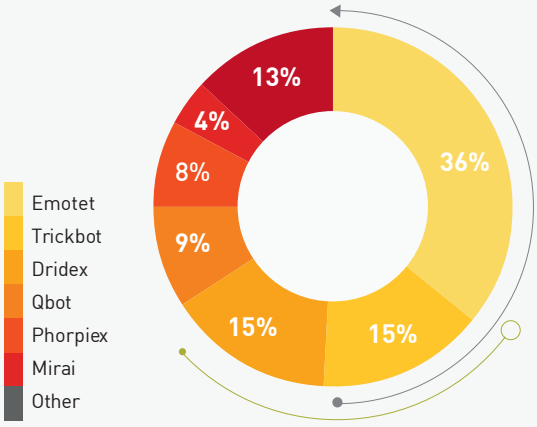


Figure 20: Most Prevalent Botnets in the Americas

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

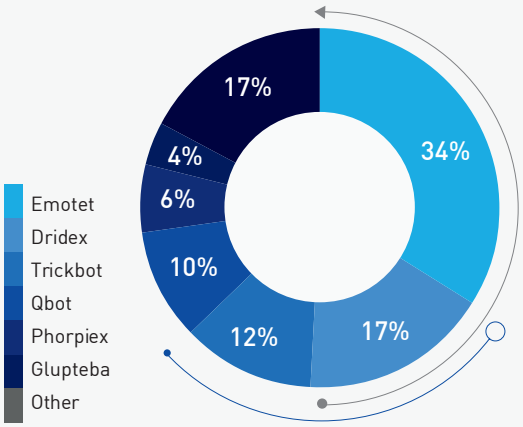


Figure 21: Most Prevalent Botnets in EMEA

ASIA PACIFIC (APAC)

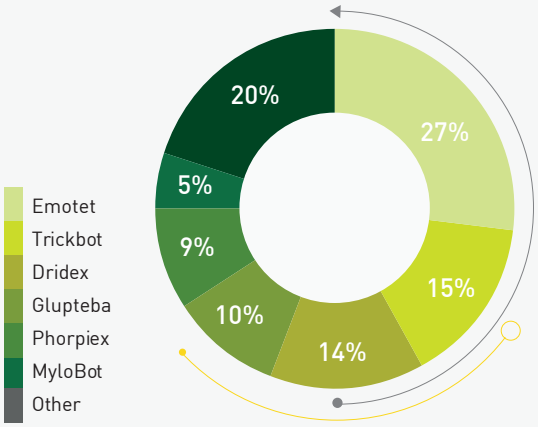


Figure 22: Most Prevalent Botnets in APAC

BOTNET GLOBAL ANALYSIS

The botnet arena remains in control of several prominent botnets, including Emotet, Trickbot and Mirai-based variants. Unlike 2019, this year Dridex entered our top ranks, fueled by numerous spam campaigns. Dridex first emerged as a banking Trojan in 2012, and gained prominence in 2015 due to its credential theft capabilities. Around 2016, the malware began functioning as a botnet, distributing noticeable malware such as the Locky ransomware. Today, it powers targeted ransomware attacks utilizing the DoppelPaymer ransomware.

In September, Emotet and Trickbot were involved in one of the most memorable attacks of 2020, demonstrating the strength and potential of botnet collaboration —the Universal Health Services (UHS) incident. UHS is one of the largest healthcare providers in the US, with over 400 facilities mostly in the US and UK, and serves 3.5 million patients per year.

UHS suffered an attack by the Ryuk ransomware, leading to the lockdown of computers, databases and phone systems across all UHS facilities in the US for almost a month. Employees and medical staff were instructed to work solely with paper documentation. Reports claimed that hospitals were forced to divert all ambulances to smaller centers, and treatments were delayed as lab results could not be delivered to the staff.

Investigators found that both Emotet and Trickbot were involved in the attack. Emotet probably gained access to the UHS network in the form of a malicious attachment to a phishing email. Emotet then installed Trickbot, to detect and harvest valuable information from the system, and then delivered the Ryuk ransomware.

TOP INFOSTEALER MALWARE

GLOBAL

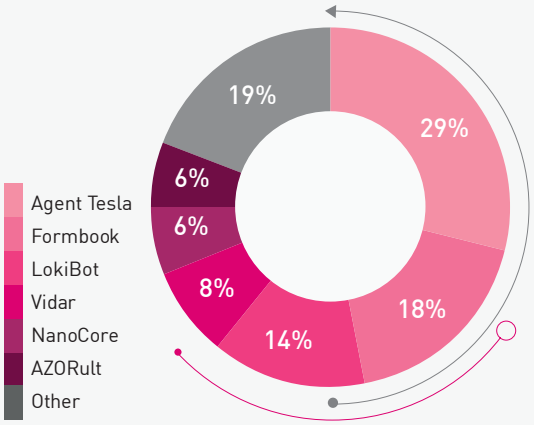


Figure 23: Top Mobile Malware Globally

AMERICAS

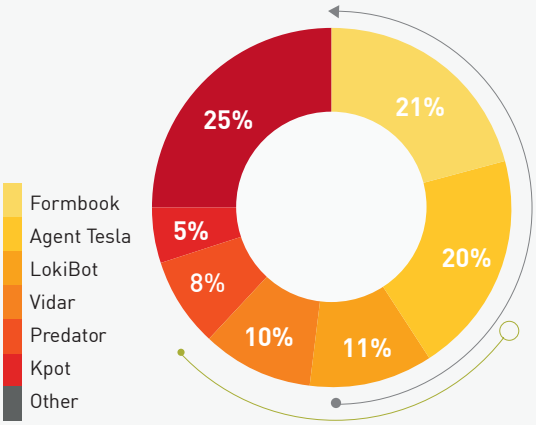


Figure 24: Top Mobile Malware in the Americas

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

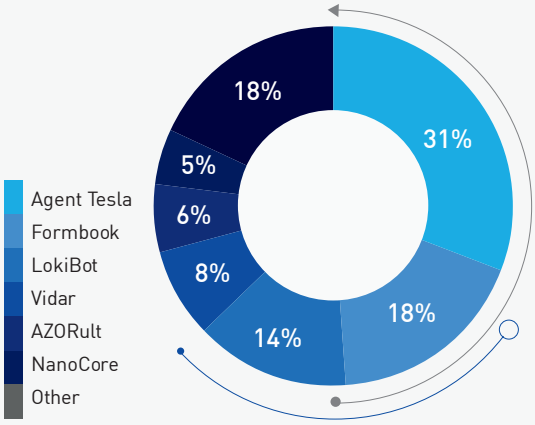


Figure 25: Top Mobile Malware in EMEA

ASIA PACIFIC (APAC)

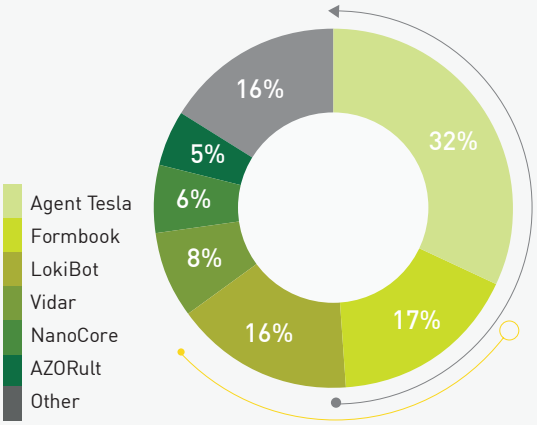


Figure 26: Top Mobile Malware in APAC

INFOSTEALER MALWARE GLOBAL ANALYSIS

The infostealer top ranks did not see significant changes since last year. The infostealer arena is dominated by three prominent commodity malware families: Agent Tesla, LokiBot and Formbook. Commodity malware, available for purchase or download, is often fueled by mass spam campaigns that can be operated by less skilled attackers. The NanoCore RAT, that was missing from the charts during the first half of the year, is also a commodity malware.

The attackers who utilize these malware families still employ new tricks to avoid detection, like migrating their infrastructure to the cloud, and hosting its payloads on well-known cloud services such as Dropbox and Google Drive via seemingly-legitimate accounts. In April, a LokiBot campaign leveraging the pandemic was observed targeting users in the US, Turkey, Portugal, Germany, and Austria. Another infostealer that exploited the COVID-19 outbreak is AZORult. In March, AZORult was distributed via a weaponized application of a coronavirus heat map. While the app displayed the map, the Infostealer was collecting information in the background.

TOP BANKING TROJANS

GLOBAL

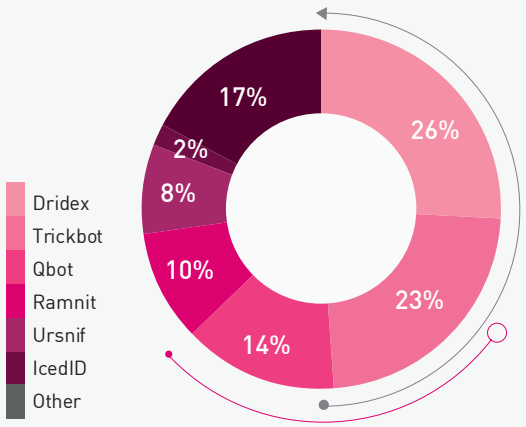


Figure 27: Most Prevalent Banking Trojans Globally

AMERICAS

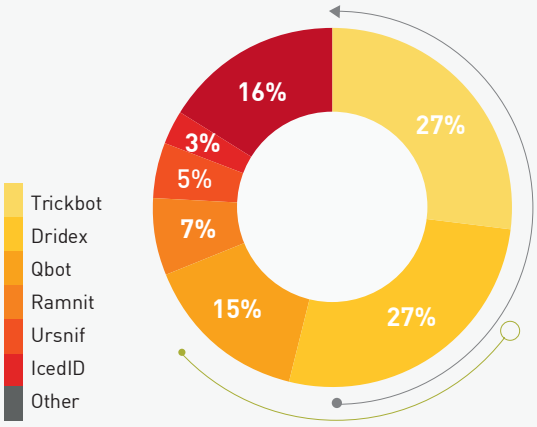


Figure 28: Top Most Prevalent Banking Trojans in the Americas

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

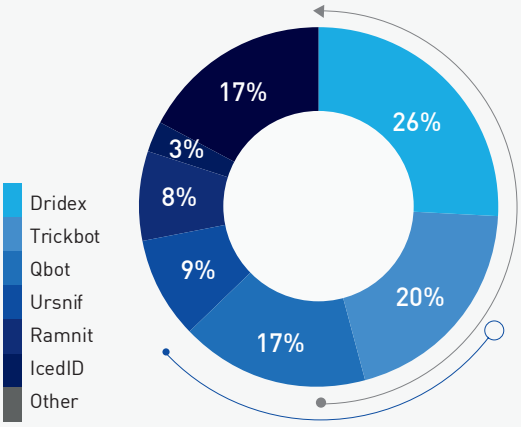


Figure 29: Most Prevalent Banking Trojans in EMEA

ASIA PACIFIC (APAC)

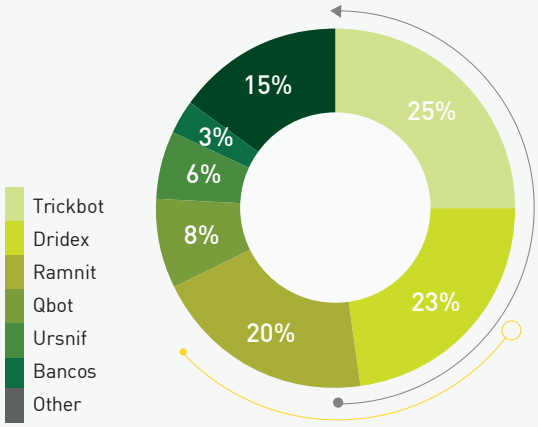


Figure 30: Most Prevalent Banking Trojans in APAC

BANKING TROJANS GLOBAL ANALYSIS

Dridex and Trickbot continue to dominate the bankers' arena. Financial institutions reported a significant increase in the rate of phishing emails that pretend to be sent by prominent banks. Many of these campaigns leverage changes wrought by the COVID-19 crisis, namely financial struggles, the changing job market and remote, solitary work from home. The phishing emails allegedly offer financial support, flexible loans and credit deferrals.

In this year's top banking malware chart, **Qbot** makes an appearance. The malware first appeared in 2008, and was designed to steal users' banking credentials and keystrokes and spread mainly via spam email campaigns. However, Qbot is an ever-evolving malware, constantly adding new features and capabilities, both for data exfiltration and stealth. Its first campaign in 2020 took place between March and the end of June, and was followed by a brief halt for further development. Qbot quickly resumed activity in July, alongside Emotet, and was installed by Emotet in multiple malspam campaigns. The latest trick in its arsenal is thread hijacking.

IcedID, another up-and-coming banking Trojan which was heavily targeting the Americas region, also cracked the region's top banking malware chart. Relatively new, IcedID was first revealed in 2017, and targeted banks, credit card companies, payroll services and e-commerce websites, mainly in the US. In 2020, its latest version featured extensive evasion tools, modified code injection tactics and steganography.

TOP CRYPTOMINING MALWARE

GLOBAL

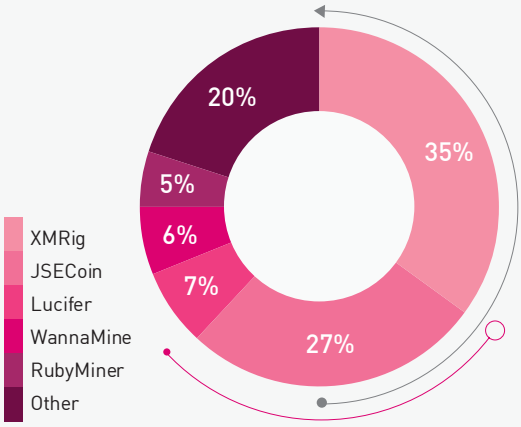


Figure 31: Top Cryptomining Malware Globally

AMERICAS

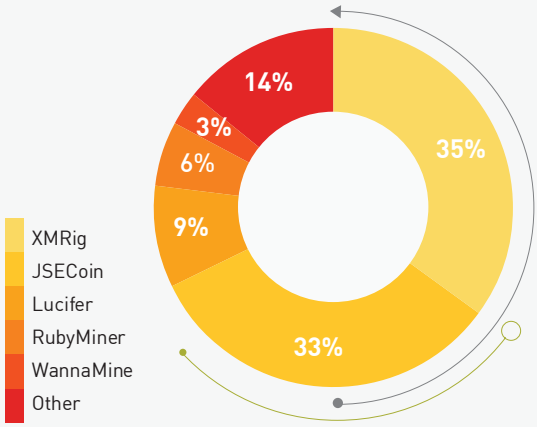


Figure 32: Top Cryptomining Malware in the Americas

EUROPE, MIDDLE EAST AND AFRICA (EMEA)

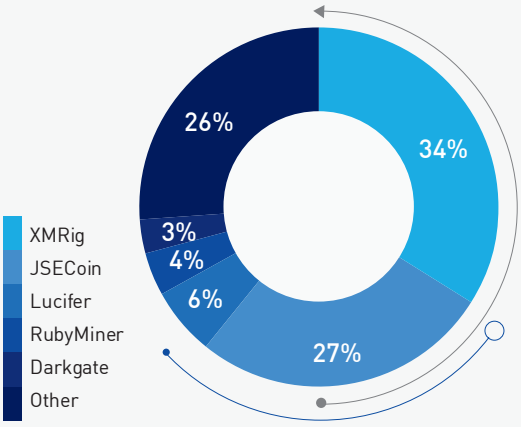


Figure 33: Top Cryptomining Malware in EMEA

ASIA PACIFIC (APAC)

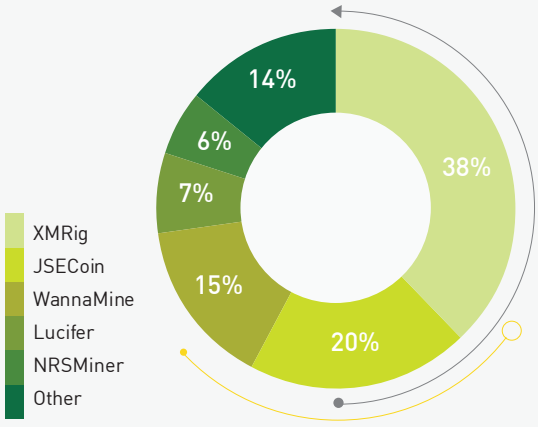


Figure 34: Top Cryptomining Malware in APAC

CRYPTOMINERS GLOBAL ANALYSIS

XMRig, originally a legitimate open-source mining tool that was leveraged by attackers for malicious purposes, is now at the top of the cryptominer chart, despite a year-long decrease from 46 percent (in H1) to 35 percent. Since 2019, we have been witnessing a steady decline in drive-by cryptominers, which were the dominant type for the past few years. The decline, which is aligned to the diminishing value of drive-by mining profitability, was hastened by the shutdown of Coinhive in March 2019 and JSECoin in April 2020.

A rising cryptominer making its first appearance on the chart is the Lucifer family. Lucifer is a self-propagating, multi-platform malware that targets Linux and IoT devices, as well as Windows web servers. Interestingly, it is also a hybrid malware, integrating multiple types of DDoS attacks, malware downloads, remote code execution and Monero cryptocurrency mining.

THE FOLLOWING LIST OF TOP VULNERABILITIES IS BASED ON DATA COLLECTED BY THE CHECK POINT INTRUSION PREVENTION SYSTEM (IPS) AND DETAILS SOME OF THE MOST POPULAR AND INTERESTING ATTACK TECHNIQUES AND EXPLOITS OBSERVED BY **CHECK POINT RESEARCHERS IN 2020**

DRAYTEK VIGOR COMMAND INJECTION (CVE-2020-8515)

Draytek is a Taiwan-based manufacturer of networking equipment and management systems such as Firewall, VPN devices and routers. Draytek Vigor is a series of VPN routers designed to build site-to-site VPN with other routers and fit into an organization's network infrastructure. In January, the Draytek Vigor router product line was found to be vulnerable to a critical remote code execution vulnerability that allows an unauthenticated attacker to execute arbitrary code as root via shell metacharacters. This high-profile vulnerability was listed in the NSA's Top 25 vulnerabilities exploited in the wild by Chinese state-sponsored threat actors. It was also heavily leveraged by cyber attackers: **according to Check Point Research, approximately 27 percent of organizations were affected by exploitation attempts of the Draytek Vigor vulnerability in 2020.**

F5 BIG-IP REMOTE CODE EXECUTION (CVE-2020-5902)

F5's BIG-IP is a popular multi-purpose networking device designed around application availability, access control, and security solutions. In June, a critical flaw was discovered in the Traffic Management User Interface (TMUI), also called the Configuration Utility, of several versions of BIG-IP devices by F5. This remote code execution vulnerability allows any user with remote access to the TMUI to execute system commands and gain complete control over a vulnerable system. Attackers can easily access the TMUI if it is exposed to the internet. Researchers were quick to release an exploit for the flaw, and although an update was released a month after the exposure, attackers rapidly responded by targeting unpatched devices. The vulnerability has been leveraged to install IoT malware and cryptominers, and the US-CERT urged organizations to install the patch as the flaw is likely continue to be exploited by cybercriminals. The vulnerability was listed in the NSA's Top 25 vulnerabilities exploited in the wild by Chinese state-sponsored threat actors.

CITRIX ADC AUTHENTICATION BYPASS (CVE-2020-8193)

A high-profile vulnerability was found in several Citrix products, and was heavily exploited by cybercriminals because of its great relevance to the professional 'new normal' due to the COVID-19 pandemic. Citrix products allow corporate employees to collaborate remotely regardless of the network or device. The bug is the result of an improper access control and input validation, and it allows unauthenticated access to certain URL endpoints as well as information disclosure to low-privileged users. Citrix released a patch to address the flaw and researchers published a scanner for exploits in the wild. The vulnerability was leveraged by threat actors a single day after its disclosure; it further made it to the NSA's top 25 vulnerabilities exploited by Chinese state-sponsored actors.

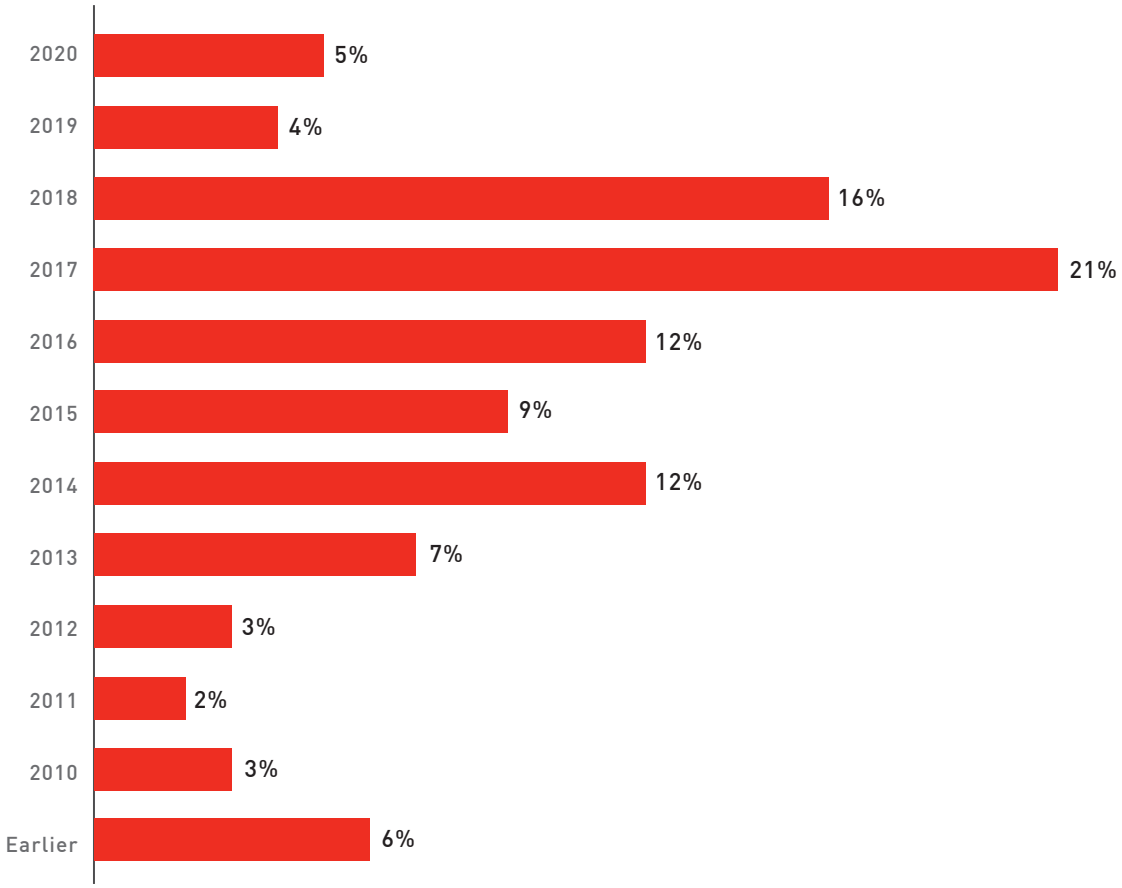


Figure 35: Percentage of Attacks Leveraging Vulnerabilities by Disclosure Year in 2020.

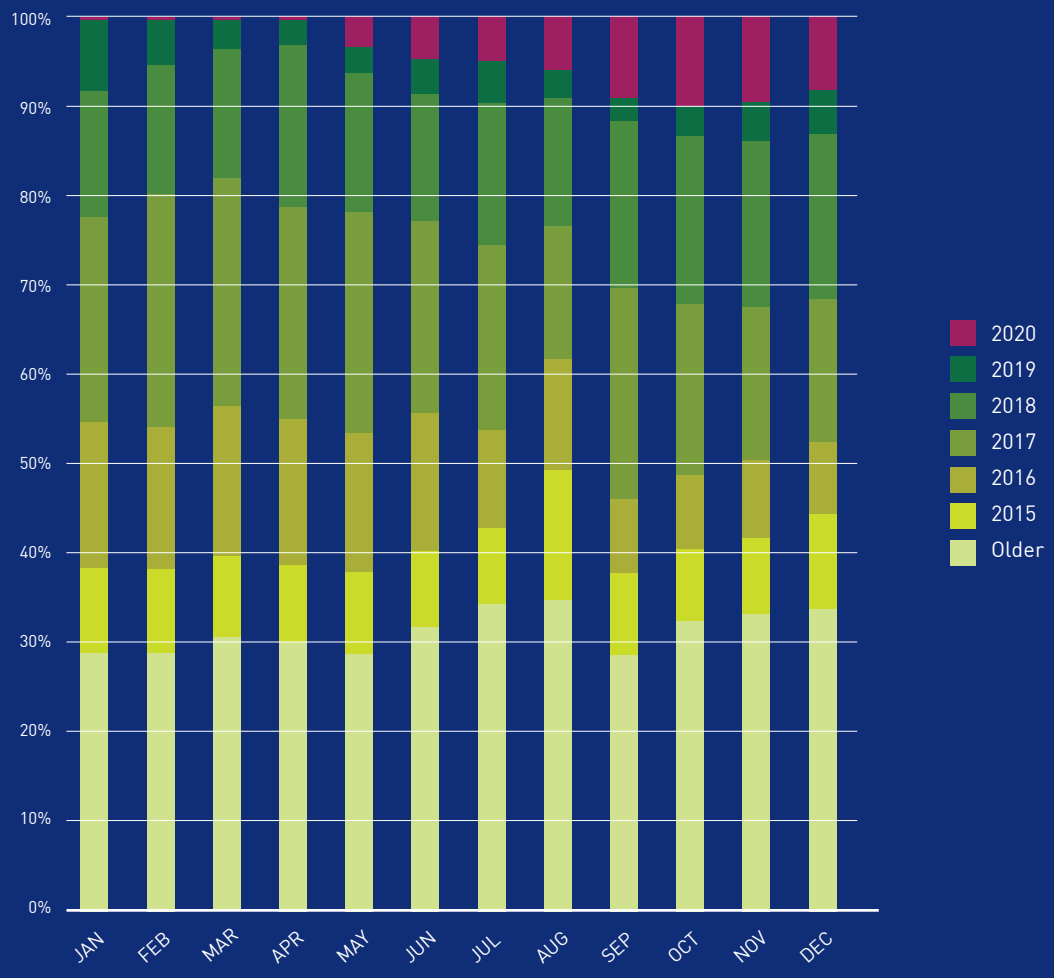


Figure 36: Percentage of Attacks Leveraging Vulnerabilities by Disclosure Year per Month.

The chart above shows the integration of new vulnerabilities in exploit chains during the year, and reveals how 2020 CVEs were increasingly exploited by attackers throughout the year.

Approximately 80 percent of the attacks observed throughout 2020 utilized vulnerabilities reported and registered in 2017 and earlier. The most prominent year in the chart—in which 21 percent of the vulnerabilities exploited this year were revealed—is 2017. This leads us to the conclusion that on average, it takes a vulnerability three years to reach its prime rate exploit. While many exploits are developed by skilled actors or threat groups for personal use, the most heavily exploited vulnerabilities are the ones who have easily available POC code or were integrated into a popular exploit toolkit and offered for sale or hire on underground forums.

IN 2020, THE AVERAGE TIME TAKEN TO IDENTIFY AND CONTAIN A CYBER-BREACH WAS **280 DAYS**, AND THE AVERAGE COST OF A BREACH IN TERMS OF LOSSES AND REMEDIATION WAS NEARLY **US$4 MILLION**.

THAT'S WHY PREVENTION IS BETTER THAN DETECTION.

RECOMMENDATIONS TO PREVENT THE NEXT CYBER PANDEMIC

By Jony Fischbein,
CISO for Check Point Software

REAL-TIME PREVENTION

As we've learned in healthcare, vaccination to prevent infection is far better than treatment after infection. The same applies to your cyber security. Real time prevention places your organization in a better position to defend against the next cyber pandemic.

Organizations that stress the prevention of unknown, zero-day threats can win the cyber security battle. Attacks from unknown threats pose critical risks to businesses, and unfortunately, they're also the hardest to prevent. That's why many businesses resort to detection-only protection. Some rely on event monitoring and threat hunting by Security Operations Center (SOC) teams to detect them after breaching their systems. But this is a far less effective strategy. The strategic imperative for organizations is to prevent cyber attacks before they breach enterprise systems.

SECURE YOUR EVERYTHING

Every part in the chain matters. The new normal introduced during the response to COVID-19 requires that you revisit and check the security level and relevance of all your network's infrastructures and processes, as well as the compliance of connected mobile and endpoint devices, and your growing IoT device estate.

The increased use of the cloud also demands an increased level of security, especially in technologies that secure workloads, containers, and serverless applications on multi- and hybrid-cloud environments.

CONSOLIDATION AND VISIBILITY

Dramatic changes in your company's infrastructure presents a unique opportunity to assess your security investments. Are you really getting what you need and are your point solutions protecting the right things? Are there areas you've overlooked?

The highest level of visibility across your network estate, reached through consolidation, will guarantee you the security effectiveness needed to prevent sophisticated cyber attacks. Unified management and risk visibility fill out your security architecture. This can be achieved by reducing your point product solutions and vendors, and your overall costs.

ABSOLUTE ZERO TRUST SECURITY

With cyber-threats existing inside and outside the security perimeter, it has become essential to adopt a Zero Trust security approach in order to keep business data protected, anywhere. Across the industry, security professionals are shifting to a Zero Trust Security state-of-mind: no device, user, workload or system should be trusted by default, neither inside or outside the security perimeter.

However, designing or rebuilding your security infrastructure around a Zero Trust approach using point solutions often leads to complexities in deployment and management, and inherent security gaps. Build a practical and holistic approach to implement Zero Trust, based on single consolidated cyber security architecture that consolidates a wide range of security functions and solutions that enable you to implement all of the seven principals of the Extended Zero Trust Security model: zero trust networks, workloads, people, data, devices, visibility and analytics, automation and orchestration.

KEEP YOUR THREAT INTELLIGENCE UP TO DATE

Malware is constantly evolving, making threat intelligence an essential tool for almost every company to consider. When an organization has financial, personal, intellectual, or national assets, a more comprehensive approach to security is the only way to protect against today's attackers. And one of the most effective proactive security solutions available today is threat intelligence. Threat intelligence combines information from multiple sources, providing a more effective protection screen for your network. Organizations are quickly understanding the need for adopting a tool such as threat intelligence into their security architecture.

To prevent zero-day attacks, organizations first need incisive, real-time threat intelligence that provides up-to-the-minute information on the newest attack vectors and hacking techniques. Threat intelligence must cover all attack surfaces including cloud, mobile, network, endpoint, and IoT, because these vectors are commonplace in an enterprise. To maintain business operations, you need comprehensive intelligence proactively stop threats, management of security services to monitor your network, and incident response to quickly respond to and resolve attacks. Malware is constantly evolving, making threat intelligence an essential tool for almost every company to consider in order to better protect themselves.

APPENDIX

MALWARE FAMILY DESCRIPTIONS

Agent Tesla

Agent Tesla is an advanced RAT which functions as a keylogger and password stealer and has been active since 2014. Agent Tesla can monitor and collect the victim's keyboard input and system clipboard, and can record screenshots and exfiltrate credentials for a variety of software installed on a victim's machine (including Google Chrome, Mozilla Firefox and Microsoft Outlook email client). Agent Tesla is sold on various online markets and hacking forums.

AZORult

AZORult is a Trojan that gathers and exfiltrates data from the infected system. When the malware is installed on a system, it can send saved passwords, local files, crypto-wallets, and computer profile information to a remote C&C server. The Gazorp builder, available on the Dark Web, allows anyone to host an AZORult C&C server with moderately low effort.

Cerberus

First seen in the wild in June 2019, Cerberus is a Remote Access Trojan (RAT) with specific banking screen overlay functions for Android devices. Cerberus operates in a Malware-as-a-Service (MaaS) model, taking the place of discontinued bankers like Anubis and Exobot. Its features include SMS control, keylogging, audio recording, location tracking, and more.

Clop

Clop is a ransomware that was first discovered in early 2019 and mostly targets large firms and corporations. It was used in an attack on the Dutch University of Maastricht which some researchers linked to the Russian cybercrime group TA505. During 2020, Clop began exercising a double extortion strategy, where in addition to encrypting the victim's data, the attackers also threatened to publish stolen information unless ransom demands were met.

Coinhive

Coinhive is a now defunct, once popular cryptomining service, designed to perform unauthorized online mining of Monero cryptocurrency when a user visits a particular web page. The implanted JavaScript uses a large amount of the end user machines' computational resources, thus impacting performance.

Danabot

Danabot is a modular banking Trojan written in Delphi that targets the Windows platform. The malware, which was first observed in 2018, is distributed via malicious spam emails. Once a device is infected, the malware downloads updated configuration code and other modules from the C&C server. Available modules include a "sniffer" to intercept credentials, a "stealer" to steal passwords from popular applications, a "VNC" module for remote control, and more.

DarkGate

DarkGate is a multifunction malware active since December 2017 which combines ransomware, credential stealing, and RAT and cryptomining abilities. Targeting mostly the Windows OS, DarkGate employs a variety of evasion techniques.

DoppelPaymer

DoppelPaymer is a variant of the BitPaymer ransomware discovered in 2019. It was involved in several high-profile targeted attacks including attacks against the city of Florence, Alabama, and Bretagne Télécom. It is usually delivered as the final stage after a successful intrusion into the victims' network. DoppelPaymer targets mostly middle to large businesses and demands high ransoms. In 2020, the operators of DoppelPaymer began exercising a double extortion strategy, where in addition to encrypting the victim's data, they also threatened to publish stolen information unless ransom demands were met.

Dridex

Dridex is a banking Trojan that targets the Windows platform. It is delivered by spam campaigns and Exploit Kits, and relies on WebInjects to intercept and redirect banking credentials to an attacker-controlled server. Dridex contacts a remote server, sends information about the infected system, and can also download and execute additional modules for remote control.

Emotet

Emotet is an advanced, self-propagating and modular Trojan. Emotet was once used as a banking Trojan, and now is used as a distributer for other malware or malicious campaigns. It uses multiple methods for maintaining persistence and evasion techniques to avoid detection. In addition, Emotet can also be spread through phishing spam emails containing malicious attachments or links.

Formbook

Formbook is an Infostealer targeting the Windows OS and was first detected in 2016. It is marketed as Malware-as-a-Service (MaaS) in underground hacking forums for its strong evasion techniques and relatively low price. Formbook harvests credentials from various web browsers, collects screenshots, monitors and logs keystrokes, and can download and execute files according to orders from its C&C.

Glupteba

Known since 2011, Glupteba is a backdoor which gradually matured into a botnet. By 2019 it included a C&C address update mechanism through public Bitcoin lists, an integral browser stealer capability and a router exploiter.

Guerrilla

Guerrilla is an Android Trojan found embedded in multiple legitimate apps and is capable of downloading additional malicious payloads. Guerrilla generates fraudulent ad revenue for the app developers.

Hawkeye

Hawkeye is an infostealer malware for Windows, active since 2013, which is designed primarily to steal users' credentials from infected devices and deliver them to a C&C server. In recent years, Hawkeye gained the ability to take screenshots, spread via USB, and more, in addition to its original functions of email and web browser password stealing and keylogging. Hawkeye is often sold as a MaaS (Malware-as-a-Service).

Hiddad

Android malware which repackages legitimate apps and then releases them to a third-party store. Its main function is displaying ads, but it also can gain access to key security details built into the OS.

IcedID

IcedID is a banking Trojan which first emerged in September 2017. It spreads by mail spam campaigns and often uses other malwares like Emotet to help it proliferate. IcedID uses evasive techniques like process injection and steganography, and steals user financial data via both redirection attacks (installs a local proxy to redirect users to fake-cloned sites) and web injection attacks.

JSECoin

Web-based cryptominer designed to perform unauthorized online mining of Monero cryptocurrency when a user visits a particular web page. The implanted JavaScript uses a large amount of the computational resources of the end users' machines to mine coins, thus impacting the performance of the system. JSECoin stopped its activity in April 2020.

KPOT

KPOT is a Trojan that targets the Windows platform. This malware steals personal information from various sources such as web browsers, Microsoft accounts, instant messengers, FTP, email, VPN, RDP, cryptocurrency, and gaming software, and sends the collected information to the remote server. In addition, this malware takes screenshots and retrieves system information from the infected computer and sends it to a remote server.

Reports in late 2020 suggest that the source code of the KPOT was acquired by the REvil ransomware group in an auction held on a hacker forum.

LokiBot

LokiBot is commodity infostealer for Windows. It harvests credentials from a variety of applications, web browsers, email clients, IT administration tools such as PuTTY, and more. LokiBot has been sold on hacking forums and is believed to have had its source code leaked, thus allowing for a range of variants to appear. It was first identified in February 2016.

Lotoor

Lotoor is a hacking tool that exploits vulnerabilities in the Android operating system to gain root privileges on compromised mobile devices.

Lucifer

Lucifer is a crypto miner and DDOS hybrid malware that exploits Windows vulnerabilities. The malware also uses brute force attacks to gain login credentials and invade Windows servers and PCs.

Lucifer originally targeted the Windows system, but recently evolved into a multi-platform and multi-architecture malware targeting Linux, and IoT devices, and has separate ARM and MIPS versions.

Maze

Maze is a ransomware first discovered in mid-2019 and was the first ransomware to practice the double extortion strategy. Maze operators opened a dedicated webpage where, in addition to encrypting victim's data, they started publishing stolen sensitive information from victims who refused to pay the ransom. Many other threat groups followed this strategy.

Mirai

Mirai is an infamous Internet-of-Things (IoT) malware that tracks vulnerable IoT devices, such as web cameras, modems and routers, and turns them into bots. The botnet is used by its operators to conduct massive Distributed Denial of Service (DDoS) attacks. The Mirai botnet first surfaced in September 2016 and quickly made headlines due to some large-scale attacks including a massive DDoS attack used to knock the entire country of Liberia offline, and a DDoS attack against the Internet infrastructure firm Dyn, which provides a significant portion of the United States internet's infrastructure.

MyloBot

MyloBot is a sophisticated botnet that first emerged in June 2018 and is equipped with complex evasion techniques including anti-VM, anti-sandbox, and anti-debugging techniques. The botnet allows an attacker to take complete control of the user's system, downloading any additional payload from its C&C.

NanoCore

NanoCore is a Remote Access Trojan that targets Windows operating system users and was first observed in the wild in 2013. All versions of the RAT contain basic plugins and functionalities such as screen capture, cryptocurrency mining, remote control of the desktop and webcam session theft.

Necro

Necro is an Android Trojan Dropper. It can download other malware, show intrusive ads and fraudulently charge for paid subscriptions.

NRSMminer

NRSMiner is a cryptominer that surfaced around November 2018, and was mainly spread in Asia, specifically Vietnam, China, Japan and Ecuador. After the initial infection, it uses the famous EternalBlue SMB exploit to propagate to other vulnerable computers in internal networks and eventually starts mining the Monero (XMR) cryptocurrency.

Phorpiex

Phorpiex is a botnet (aka Trik) that has been active since 2010 and at its peak controlled more than a million infected hosts. It is known for distributing other malware families via spam campaigns as well as fueling large-scale spam and sextortion campaigns.

PreAMO

PreAMo is a clicker malware for Android devices, first reported in April 2019. PreAMo generates revenue by mimicking the user and clicking on ads without the user's knowledge. Discovered on Google Play, the malware was downloaded over 90 million times across six different mobile applications.

Predator the Thief

Predator the Thief is a sophisticated infostealer which was identified in mid-2018. It started as coding experiments in malware development but later evolved into a full-fledged menace. Predator can extract passwords, access the victim's camera and steal information from cryptocurrency wallets.

Pykspa

Worm that spreads itself by sending instant messages to contacts on Skype. It extracts personal user information from the machine and communicates with remote servers by using a Domain Generation Algorithm.

Qbot

Qbot AKA Qakbot is a banking Trojan that first appeared in 2008. It was designed to steal a user's banking credentials and keystrokes.

Often distributed via spam email, Qbot employs several anti-VM, anti-debugging, and anti-sandbox techniques to hinder analysis and evade detection.

Ragnar Locker

Ragnar Locker is a ransomware first discovered in December 2019. It deploys sophisticated evasion techniques including deployment as a virtual machine on targeted systems to hide its activity. Ragnar was used in an attack against Portugal's national electric company in a double extortion act where the attackers published sensitive data stolen from the victim.

Ramnit

Ramnit is a modular banking Trojan first discovered in 2010. Ramnit steals web session information, giving its operators the ability to steal account credentials for all services used by the victim, including bank accounts, and corporate and social networks accounts. The Trojan uses both hardcoded domains as well as domains generated by a DGA (Domain Generation Algorithm) to contact the C&C server and download additional modules.

Remcos

Remcos is a RAT that first appeared in the wild in 2016. Remcos distributes itself through malicious Microsoft Office documents, which are attached to spam emails, and is designed to bypass Microsoft Windows UAC security and execute malware with high-level privileges.

RigEK

The oldest and best known of the currently operating Exploit Kits, RigEK has been around since mid-2014. Its services are offered for sale on hacking forums and the TOR Network. Some "entrepreneurs" even resell low-volume infections for those malware developers not yet big enough to afford the full-fledged service. RigEK has evolved over the years to deliver anything from AZORult and Dridex to little-known ransomware and cryptominers.

RubyMiner

RubyMiner was first seen in the wild in January 2018 and targets both Windows and Linux servers. RubyMiner seeks vulnerable web servers (such as PHP, Microsoft IIS, and Ruby on Rails) to use for cryptomining, using the open source Monero miner XMRig.

Ryuk

Ryuk is a ransomware used by the Trickbot gang in targeted and well-planned attacks against several organizations worldwide. The ransomware was originally derived from the Hermes ransomware, whose technical capabilities are relatively low, and includes a basic dropper and a straightforward encryption scheme. Nevertheless, Ryuk was able to cause severe damage to targeted organizations, forcing them to pay extremely high ransom payments in Bitcoin. Unlike common ransomware, systematically distributed via massive spam campaigns and Exploit Kits, Ryuk is used exclusively in tailored attacks.

Sodinokibi

Sodinokibi is a Ransomware-as-a-Service which operates an "affiliates" program and was first spotted in the wild in 2019. Sodinokibi encrypts data in the user's directory and deletes shadow copy backups to make data recovery more difficult. In addition, Sodinokibi affiliates use various tactics to spread it, including through spam and server exploits, as well as hacking into managed service providers (MSP) backends, and through malvertising campaigns that redirect to the RIG Exploit Kit.

Trickbot

Trickbot is a modular Banking Trojan that targets the Windows platform, and is mostly delivered via spam campaigns or other malware families such as Emotet. Trickbot sends information about the infected system and can also download and execute arbitrary modules from a large array of available modules, including a VNC module for remote control and an SMB module for spreading within a compromised network. Once a machine is infected, the threat actors behind this malware utilize this wide array of modules not only to steal banking credentials from the target PC, but also for lateral movement and reconnaissance on the targeted organization itself, prior to delivering a company-wide targeted ransomware attack.

Ursnif

Ursnif is a variant of the Gozi banking Trojan for Windows, whose source code has been leaked online. It has man-in-the-browser capabilities to steal banking information and credentials for popular online services. In addition, it can steal information from local email clients, browsers and cryptocurrency wallets. Finally, it can download and execute additional files on the infected system.

Valak

Known since 2019, Valak was originally a malware dropper and was enhanced to include infostealing capabilities. The malware spreads through malspam campaigns, often by replying to email threads from a compromised account. Valak is often delivered alongside other malware like Ursnif.

Vidar

Vidar is an infostealer that targets Windows operating systems. First detected at the end of 2018, it is designed to steal passwords, credit card data and other sensitive information from various web browsers and digital wallets. Vidar is sold on various online forums and used as a malware dropper to download GandCrab ransomware as its secondary payload.

WannaMine

WannaMine is a sophisticated Monero crypto-mining worm that spreads the EternalBlue exploit. WannaMine implements a spreading mechanism and persistence techniques by leveraging the Windows Management Instrumentation (WMI) permanent event subscriptions.

xHelper

xHelper is an Android malware which mainly shows intrusive popup ads and notification spam. It is very hard to remove once installed due to its reinstallation capabilities. First observed in March 2019, xHelper has now infected more than 45,000 devices.

XMRig

XMRig is open-source CPU mining software used to mine the Monero cryptocurrency. Threat actors often abuse this open-source software by integrating it into their malware to conduct illegal mining on victims' devices.

Zeus

Zeus is a widely distributed Windows Trojan which is mostly used to steal banking information. When a machine is compromised, the malware sends information such as the account credentials to the attackers using a chain of C&C servers.

Zloader

Zloader is a banking malware which uses webinjects to steal credentials and private information, and can extract passwords and cookies from the victim's web browser. It downloads VNC that allows the threat actors to connect to the victim's system and perform financial transactions from the user's device. First seen in 2016, the Trojan is based on leaked code of the Zeus malware from 2011. In 2020, the malware was very popular among threat actors and included many new variants.

Check Point's Global Threat Impact Index and its ThreatCloud Map is powered by Check Point's ThreatCloud intelligence, the largest collaborative network to fight cybercrime which delivers threat data and attack trends from a global network of threat sensors. The ThreatCloud database inspects over 3 billion websites and 600 million files daily, and identifies more than 250 million malware activities every day.

cp<r>
CHECK POINT RESEARCH

CONTACT US

WORLDWIDE HEADQUARTERS

5 Ha'Solelim Street, Tel Aviv 67897, Israel
Tel: 972-3-753-4555 | Fax: 972-3-624-1100
Email: info@checkpoint.com

U.S. HEADQUARTERS

959 Skyway Road, Suite 300, San Carlos, CA 94070
Tel: 800-429-4391 | 650-628-2000 | Fax: 650-654-4233

UNDER ATTACK?

Contact our Incident Response Team:
emergency-response@checkpoint.com

CHECK POINT RESEARCH PODCAST

Tune in to cp<radio> to get CPR's latest research,
plus behind the scenes and other exclusive content.
Visit us at https://research.checkpoint.com/category/cpradio/

WWW.CHECKPOINT.COM