



INSIGHTS
DRIVEN BY DATA 

2021 Global Threat Intelligence Report

Technical Report

Together we do great things
hello.global.ntt

The 2021 Global Threat Intelligence Report reminds us that in a world of evolving cyberthreats, we need to stay ahead of the curve to secure the next horizon of cyber resilience. Success lies in rethinking what you need to accommodate new ways of working; engaging with your ecosystem of partners and customers to entrench trust across the supply chain; and securing all elements of your infrastructure to drive business value and transformation.

We're here to keep you secure by design with our intelligence-driven cybersecurity.

Contents

Executive summary	4
Impact of COVID-19	6
Global analysis	10
Global highlights	13
Targeted technologies	17
Regional analysis	18
The Americas	19
Europe, Middle East and Africa	20
Asia Pacific	22
Focus on industries	24
Finance	25
Manufacturing	29
Healthcare	32
Education	35
Technology	38
Malware and threats – research and observations	42
Trickbot	43
Emotet	43
APT41: A threat actor with global reach	44
Best practices	47
Cyber-resiliency and agility	48
Trust, the supply chain and how it affects business	50
Privacy, governance, risk and compliance	54
2020 Olympics threat landscape	60
Conclusions	62
NTT global data analysis methodology	64
NTT resource information	66
Global Threat Intelligence Center	66
NTT-CERT	66
Contributors	67

Executive summary

NTT designs and implements cybersecurity solutions to address challenges impacting clients across many industries. In our 2021 Global Threat Intelligence Report, we identify the threats organizations faced globally over the last year, and provide operational, tactical and strategic recommendations they should consider implementing to manage risk.

In this year's Report, we continue reinforcing the concepts of 'cyber-resilience' and 'secure by design' solutions, but also include discussions related to trust. Organizations can no longer simply assign blind trust to new alliances, partners or vendors. It is also not wise to trust unvetted access to your organization's data. We devoted an entire section of this year's Report to discussing trust and briefly review the 'cyber-resiliency' and 'secure by design' concepts.

As in previous years, we continue our analysis of attacks against several industries. This includes looking at finance, healthcare, education, manufacturing and technology. We share our findings for each industry and look closely at where we observed changes in nefarious cyberattack activity.

This Report shares insights that empower cybersecurity leaders and defenders to make informed decisions on where to focus when making investments in and improvements to their security capabilities. The Report will also enable them to evaluate threats which may impact their environments and help them identify where risks can be reduced as well as where detection and response capabilities may be improved.

It is noteworthy that, in a year where the COVID-19 pandemic profoundly altered the tactics of threat actors, 88% of cybersecurity professionals said that risks have increased in the last six months.



Kazu Yozawa

CEO, Security Service division, NTT Ltd.

Kazu has more than 40 years' experience in the ICT sector, with 12 years in managed security services. He was appointed Chief Executive Officer of NTT Security in April 2021. Prior to his appointment as CEO, Kazu held the position of CTO for NTT's broader cybersecurity team in Global R&D for Managed Security Services and CEO of NTT Security Japan.

Some of our most notable findings include:



Industries in the line of fire; amplified attacks on finance, manufacturing and healthcare

Attacks against manufacturing increased from 7% last year to 22%; healthcare increased from 7% to 17%; and finance is up from 15% to 23%. Attackers continue to focus on these industries with the combined percentage of attacks against the top three targeted industries being 62% in 2020.



Changing face of malware: miners and Trojans replace spyware as most common malware family globally

Malware continues to evolve and become more diverse with the growth of multi-function malware. The use of worm functionality has increased, miners experienced a surge, ransomware evolved and attackers leveraged a variety of banking and remote access Trojans. Although malware is becoming more commoditized in features and functionality, the use of certain variants of malware against specific industries continues to evolve.



Cryptocurrency miners soar to new heights

Coin miners represented a staggering 41% of malware detected in 2020, with XMRig being the most common variant representing nearly 82% of all coin miner activity. Coin miners accounted for 23% of all malware in the US and 74% in Europe, the Middle East and Africa (EMEA). Miners were the most detected form of malware in the UK and Ireland (UK&I) (87%), Germany (65%) and Benelux (89%).



COVID-19 emboldens advanced persistent threat (APT) groups to intensify espionage, sabotage and cybercriminal operations

Cybercriminal groups such as the Ozie Team, Agent Tesla and TA505, along with nation-state actors like Vicious Panda, Mustang Panda and Cozy Bear were very active in 2020. Organizations in multiple industries saw attacks related to the COVID-19 vaccine and associated supply chains.



Work-from-home and remote access are magnifying web and application attacks

Organizations continue to race to make their organizations more virtual, increasing their use of client portals as well as mobile and web-enabled applications. Application-specific and web-application attacks continued to rise and remained the top types of attacks observed. Application-specific attacks accounted for 35%, and web-application attacks accounted for 32%, resulting in a combined total of 67% of attacks (up from 55% in 2019 and 32% in 2018). The top three detections (application-specific attacks, web-application attacks and reconnaissance activity) accounted for 87% of all activity in 2020.



A year of privacy and protection in the 'new normal'

The ongoing fallout following the Schrems II decision invalidated the EU-US Privacy Shield and placed additional obligations on organizations transferring personal data from the EU to third countries. Data localization strategies are rising on the agenda as new laws and regulations place increasing obligations, restrictions, or limitations on the ability to transfer personal data to other countries. Brazil, New Zealand, South Africa, Singapore and California all enacted new laws or updates to laws regarding privacy and protection; India also has an upcoming bill related to these concerns.



Impact of COVID-19

Throughout 2020, the COVID-19 pandemic wreaked havoc and concerns forced operational changes in many industries. Recurring global lockdowns to mitigate the spread of the disease continue to impact businesses dynamically.

CONNECTING AUTHORISED
HOLO1 TO BUSINESS NETWORK

36°

Nearly five in six organizations (83%) completely re-thought their IT security to accommodate new ways of working brought about by the pandemic, research for NTT's 2020 Intelligent Workplace Report found.

83%

of organizations have **completely rethought their IT security** to accommodate new ways of working brought about by the pandemic

31%

are still **assessing the impact of COVID-19** on their security and governance posture

Today, organizations must place a higher priority on:

- managing risk
- addressing cybersecurity issues related to supporting their online presence
- optimizing and securing work-from-home arrangements
- preparing to defend against supply chain attacks

Increased COVID-19 and COVID-19 vaccine-related phishing campaigns are a continuing threat.

As threat actors advance their tactics, techniques and procedures, organizations have a greater need to ensure that they and their associates can withstand a breach and recover from an attack in a timely manner. No amount of insurance can hedge against the reputational damage suffered after a breach becomes public.

Remote working has become a mainstay of the business environment. Some employees may never permanently return to an in-office working environment. This was illustrated in the NTT 2020 Intelligent Workplace Report, which showed that more than half of surveyed organizations (54%) would never return to their pre-pandemic operating model or would pursue a hybrid operating model with expanded flexible working.

54%

of organizations said they would never return to their pre-pandemic operating model or would pursue a hybrid operating model with expanded flexible working

This is a business model with which some organizations have had limited experience. It creates demand for employee equipment, additional networking and VPN support and backing for a culture that provides for limited hands-on management of employees. Irrespective of their work location, employees must be able to accomplish their tasks and effectively communicate with colleagues while adhering to organizational policies and procedures designed to keep all data safe. Organizations must adapt and maintain a secure network to allow uninterrupted business continuity. This has become increasingly difficult as security professionals have often been redirected to serve the additional demand for more general ICT support, effectively deprioritizing security initiatives.

Defending against supply chain attacks has taken on a new level of urgency. Depending upon the threat actor's goal, a supply chain attack on COVID-19 vaccine manufacturing and cold storage facilities could stop vaccine production and distribution. This would impact treatment and possibly cause patient deaths. Exfiltrating vaccine formulas and manufacturing processes would benefit nation-state threat actors whose countries have yet to produce a highly effective treatment for the virus. Sowing discord via vaccine delays could also provide attackers with additional attack vectors for follow-on attacks.

Threat actors and phishing campaigns

We've been actively tracking many cybercriminal and advanced persistent threat (APT) group campaigns that have been exploiting the pandemic to further their activities. While cybercriminal groups have exploited the pandemic to spread malware for financial gain, APT groups have leveraged pandemic-related concerns to define targets and establish footholds in victims' systems. Attackers have:

- distributed malicious PDF, RTF and Word documents
- disseminated spyware, keyloggers and other malware
- used specific COVID-19 related phishing lures
- targeted education or healthcare institutions involved in COVID-19 patient care and vaccine research, development and distribution

Specifically, NTT tracked multiple APT groups involved in either cybercrime, corporate espionage or sabotage operations related to COVID-19 exploitation, including Cozy Bear (APT29), Gamaredon, Sofacy (APT28), TA505, Wizard Spider, Emissary Panda (APT27), Judgement Panda (APT31), Mustang Panda, Sneaky Panda (APT17), Vicious Panda, KimSuky, Lazarus Group, DarkHotel, Charming Kitten (APT35), OceanLotus (APT32), TA412, TA505, Mummy Spider (TA542), Bamboo Spider (TA544) and more.

Next, we'll explore more about two of these groups, Ozie Team (cybercriminal) and TA505 (APT), as well as a widespread phishing campaign (Agent Tesla). We'll also briefly discuss the common attacker technique of domain name impersonation, which has seen significant use during COVID-19 related exploitation attempts.

The Ozie Team: Business email compromise (BEC) activity increased during the COVID-19 pandemic. One notable example is the BEC campaign launched by the Ozie Team, which we've been tracking since mid-2019. The Ozie Team is a Nigerian threat actor group specializing in BEC that uses commodity malware distributed via malspam. Once the victim opens the malicious attachment, FormBook injects itself into its desired running process or Windows Explorer. Once FormBook is uploaded, threat actors can see details of the user's activity from the FormBook web interface, including keystrokes and filled web forms.

On 6 April 2020, our analysts observed correspondence between two members of the Ozie Team discussing targeting a manufacturer of N95 masks. Tracking this correspondence led to the discovery of a transaction of over USD 550,000 in an account controlled by the Ozie Team.

COVID-19 phishing campaigns have spanned the globe and targeted organizations

studying the effects of the virus, those researching a vaccine and possibly The Vaccine Alliance's Cold Chain Equipment Optimization Platform program.

Agent Tesla: Around May 2020, threat actors deployed Agent Tesla, an advanced remote access Trojan that gives attackers access to an infected device. Agent Tesla is delivered via a compressed file attachment. It can steal data from web browsers, email, and FTP and VPN clients. The Agent Tesla Trojan was used during a phishing campaign that offered personal protective equipment as a lure. Once downloaded, the malware logged keystrokes on the infected device, stole sensitive information from the user's AppData folder and sent it to the command-and-control server via SMTP.

TA505: TA505, the threat actor group linked to Locky ransomware and the Dridex banking Trojan, has been using COVID-19-related lures to deliver malware to their victims' computers. Once delivered, attackers can download additional types of malware including banking Trojans and ransomware. As COVID-19-related cyberattacks increase worldwide, it's highly likely that TA505 could extend their attack surface to include a wider variety of employees working from home.

Domain name impersonation: Threat actors are using domain name impersonation, also known as 'cybersquatting' or 'typo-squatting', to trick people into visiting the threat actor's malevolent site. This tactic is the practice of registering domain names for well-known organizations by changing a letter or feature in a legitimate domain name. Victims then visit this malicious domain by accident and infect their systems with malware. Cybercriminals may attempt to sell their impersonated domain to the legitimate organization, which would allow them to remove the fake domain name from the internet. This tactic is commonly being used to lure victims to fake sites promising COVID-19 information.

COVID-19 vaccine and supply chain attacks

COVID-19 phishing campaigns have spanned the globe and targeted organizations studying the effects of the virus, those researching a vaccine and possibly The Vaccine Alliance's Cold Chain Equipment Optimization Platform program. Any disruption to the temperature-controlled storage facilities or transportation vehicles endangers the integrity of vaccines with cold-storage requirements, possibly endangering lives by contributing to increasing infection rates if people cannot get vaccinated.

As with all disasters, threat actors exploit opportunities to launch attacks. Industrious cybercriminals have had prolonged opportunities to launch various COVID-19-related attacks, particularly pandemic-themed phishing attacks and vaccine phishing campaigns.

Summary

Managing risk should be inherent in the operations of organizations in every industry. While each industry has its specific set of threats, all are subject to additional common threats. Among others, these include threats related to third-party vendor risk, supply chain attacks and the reputational damage incurred from public disclosure of client-sensitive data loss or intellectual property theft, along with fines for non-compliance. Specifically, with COVID-19:

- Manufacturing runs the risk of having processes, machinery designs and manufactured products being stolen either physically or via a breach.
- Threats to technology follow suit, as two of its greatest threats are intellectual property theft and data theft.
- Protection of Personal Identifiable Information (PII) is paramount in healthcare and finance.
- In the US, exfiltration of PII in healthcare violates the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which can incur steep fines on healthcare institutions.
- The finance industry is governed by regulations to protect client data which include penalties varying by region or country.
- Education, especially education institutions that conduct COVID-19 vaccine research, have come under attack by APTs, and are in danger of loss of computing resources, as well as research data.
- Unfortunately, the effects of the pandemic appear to have left some strategic misalignment, with only 53% of organizations saying that their security strategy is fully aligned with their business strategy needs. Indeed, 31% of organizations said they were still assessing the impact of the pandemic on their security and governance posture.

COVID-19 continues to evolve, affecting industries, businesses and human interactions around the globe. We must continue to seek ways to manage risk in all forms related to the pandemic and adjust our strategies, focusing on changing operations and providing continued support for clients and employees, as well as COVID-19 related research and vaccine distribution. These are highly complex issues that only serve to complicate the operations and security profiles of affected organizations. As a result, all organizations must continue to innovate and create resilient solutions for a more secure human and cyber environment.



Global analysis

Globally, organizations faced much of the same types of attacks, though attackers often targeted different technologies.

Organizations in the finance, manufacturing and healthcare industries experienced greater impact than other industries. Malware went through somewhat of a renaissance as multi-function malware continued to make its mark felt. A small number of malware saw wide adoption, but much of those observed appeared to be used in a more targeted manner. Attackers had their preferences depending on the industry being targeted, just like the technology being targeted. New threats made their way into industries and regions. Organizations adapted to embrace the new business models required due to the COVID-19 pandemic and increased their reliance on web-based infrastructure.

Figure 1 shows comparisons between 2018, 2019 and 2020's benchmark scoring using NTT's Cybersecurity Advisory (CA) consulting service. The CA score is based on a 0-6 scale which defines the maturity of the organization's security program in several areas (with a higher number indicating a more mature program).

Industry	2018 baseline	2019 baseline	2020 baseline
Technology	1.66	1.64 ↓	1.64 —
Finance	1.71	1.86 ↑	1.84 ↓
Business and professional services	1.31	1.54 ↑	1.79 ↑
Education	1.21	1.02 ↓	1.04 ↑
Manufacturing	1.45	1.32 ↓	1.21 ↓
Healthcare	1.03	1.12 ↑	1.02 ↓

Figure 1: Comparisons between 2018, 2019 and 2020's benchmark Cybersecurity Advisory scores | Arrow indicators show change versus the previous year.

Baseline scores (measured against the organization's current maturity) have largely remained within the same range as the previous year. Finance continues to show the highest benchmark score for the third consecutive year. Small decreases in baseline scores likely result from challenges in prioritization, which potentially affected allocation of resources and did not allow the organization's program to mature. This is not unexpected in healthcare. The industry faced challenges in keeping up with infrastructure issues during the pandemic. Manufacturing organizations experienced a three-year decline in scores, most likely due to changes in the operating environment, evolution of attacks and a greater inclination to benchmark their overall cybersecurity posture.

Maturity scale	Non-existent 0.00–0.99	Initial 1.00–1.99	Repeatable 2.00–2.99	Defined 3.00–3.99	Managed 4.00–4.99	Optimized 5.00–5.99
Process	No process costs	Ad-hoc and informal	Some basic templates or checklists exist	Formally documented processes are consistent	Formal integrated workflows	Mature and automated workflows
Metrics	No metrics exist	Ad-hoc reporting	Basic metrics, informal reporting	Formally documented metrics, manual reporting	Advanced metrics and semi-automated reporting	Fully automated reporting
Tools	No technology control exists	Planning underway	Basic functionality implemented with only elemental capabilities	Functionality implemented and aligned to policies	Integrated logging, manual correlation	Integrated platform, automated correlation

Figure 2: Maturity levels as defined in the Cybersecurity Advisory

The maturity of security programs in the business and professional services industry increased three years in a row. Improvements during 2020 are likely reflective of the industry's ability to continue managing priorities and make good investments in both strategy and implementations in response to COVID-19.

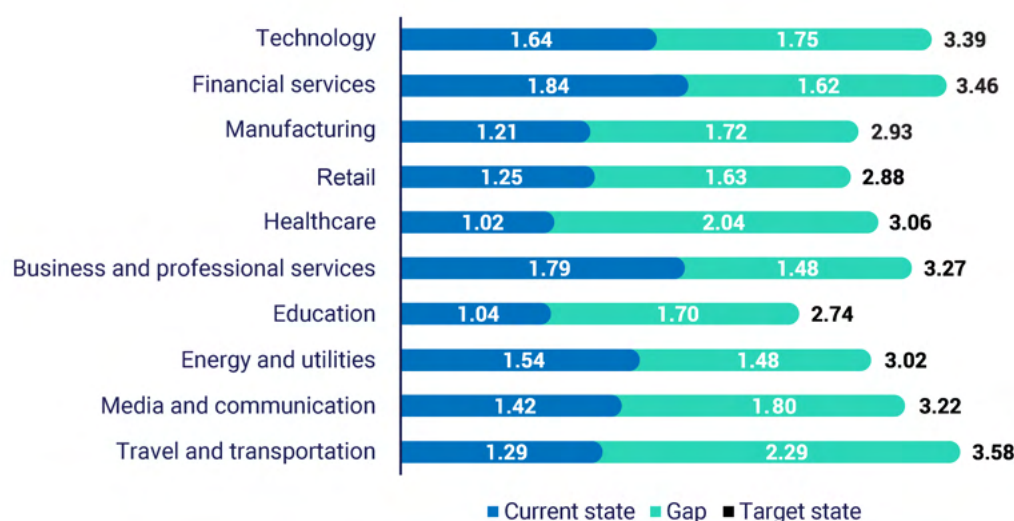


Figure 3: Current and target maturity levels and the gap between them, by sector

For this Report, we commissioned Jigsaw Research to undertake 1350 online interviews of technology and business decision-makers in large organizations in 15 sectors and 21 countries, including 1046 IT and cybersecurity professionals. The survey included a series of questions about the importance of key business and security issues relevant to secure cyber-operations.

Figure 3 illustrates the gap between the current and desired state of several industries. Industries seeking to close the gap must maintain a constant focus on tools, executive support and the maturity of underlying processes. However, various factors such as cost, compliance and the availability of resources can result in industries not achieving their desired goals. We commissioned a survey of 1350 technology and business decision makers, including 1046 IT and cybersecurity professionals, to determine what business and technology issues are key focus areas. Our research found a gap between organizations' perception of their cybersecurity posture and their actual score.

While the results of the research indicated organizations believed their cybersecurity posture averaged 3.16 (17% of organizations believed their posture is optimized, and CEOs believed their cybersecurity posture was higher, at 3.44) the average of all initial CA scores was 1.35, indicating organizations may not have a true understanding of the strength of their security programs.

The target state does not necessarily indicate where an industry needs to be. It indicates a goal state as defined by the organizations in each industry. Typically, active compliance with more stringent regulations, and motivations to protect more sensitive public or client information can help encourage organizations to strive for a higher maturity goal. A commitment to a higher goal which executive stakeholders support can lead directly to improved prioritization of security initiatives and better outcomes.

Global highlights

Finance was the most attacked industry, accounting for 23% of all attacks during 2020. Application-specific attacks continued to dominate finance, accounting for 42% of all attacks. Together, application-specific and web-application attacks make up more than 73% of all attacks on finance.

Industry and percent of global attacks	Percent of attack types for industry
Finance – 23%	Application-specific – 42% Web-application – 31% Reconnaissance – 12%
Manufacturing – 22%	Application-specific – 49% Reconnaissance – 24% Web-application – 20%
Healthcare – 17%	Web-application – 59% Application-specific – 38% Known bad source – 1%
Business and professional services – 10%	Reconnaissance – 53% Application-specific – 13% Brute force – 12%
Education – 6%	Web-application – 24% Application-specific – 22% Reconnaissance – 21%

Figure 4: Percent of attacks and percent of attack types per industry globally

The list of the most attacked industries in 2020 includes industries which were all in the top seven most attacked in 2019. However, there was a significant movement in the top five this year. Much was due to actual attack volume changes among the analysed industries, as both healthcare and business and professional services are new to the top five for 2020.

Industry	2018	2019	2020
Finance	#1 – 17%	#2 – 15%	#1 – 23%
Manufacturing	#6 – 7%	#5 – 7%	#2 – 22%
Healthcare	#7 – 7%	#6 – 7%	#3 – 17%
Business and professional services	#3 – 12%	#7 – 7%	#4 – 10%
Education	#4 – 11%	#4 – 10%	#5 – 6%

Figure 5: Percentage of overall attack volume by industry in 2018, 2019 and 2020

Finance emerged as the most attacked industry, on the strength of a 50% increase in attack volume. Manufacturing jumped from the fifth most targeted in 2019 to the second most targeted in 2020. The volume of attacks against manufacturing targets increased nearly threefold.

Healthcare was the sixth most attacked in 2019 and ended 2020 as the third most attacked, after experiencing an attack volume which more than doubled from the previous year.

Targeted industries experienced a shift in attacks towards the most attacked, with the top three industries accounting for 62% of all attacks. In 2019, the top three industries were targeted in 51% of all attacks. This appears to indicate a trend of attackers concentrating their efforts on more desirable targets, or at least more desirable industries. Nearly every other industry experienced fewer attacks than the previous year.

	2018	2019	2020
Percent of attacks focusing on the top three industries	46%	51%	62%

Figure 6: Percent of attacks against the top three industries in 2018, 2019 and 2020

Regardless of the specific industries being targeted, rates for application-specific and web-application attacks saw a rise. These attack types continued their combined impact on global industries, accounting for 67% of all attacks, up from 55% in 2019 and 32% in 2018.

They were followed by reconnaissance. No other types of hostile activity had as significant an impact on global attacks than these three attack categories. This is due to the types of vulnerabilities being uncovered, exploits being weaponized in tools, worms, botnets and other malware.

The biggest contributor is likely the increased use of web applications and infrastructures as organizations accelerated cloud adoption. Simply put, hostile threat actors are attacking the technology and functionality newly deployed by organizations. This accelerated during COVID-19 as organizations raced to become digital, increasing their use of client portals and cloud technologies, as well as mobile and web-enabled applications.

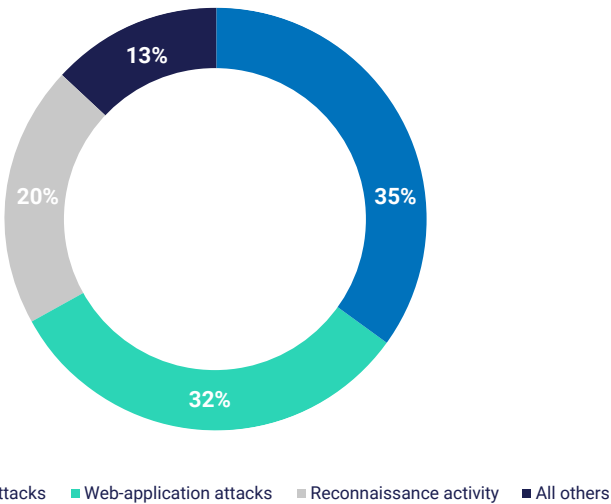


Figure 7: Breakdown of global attack types

	2018	2019	2020
Share of combined application-specific and web-application attacks	32%	55%	67%
Share of combined top three attack types	48%	69%	87%

Figure 8: Share of top attack types in 2018, 2019 and 2020



of organizations say they're **not prepared** for web and other application threats

Analysis of security tests on applications suggest some industries are simply better at managing application security. Based upon a dynamic vulnerability assessment, we established the average number of vulnerabilities per site across many industries and sub-industries.

Utilities showed the highest number of vulnerabilities, with an average of 10 per site. Of the primary industries evaluated for this Report, manufacturing showed the highest average number of vulnerabilities, with nine per site. Finance had the lowest number of average vulnerabilities per site at four. The more vulnerabilities an organization's site has, the more susceptible to attack they are from hostile actors. These vulnerabilities cover a wide range of issues and potential exposures, such as SQL injections, cross-site scripting vulnerabilities, directory indexing and data leakage.

Analysis of security tests on applications suggest some industries are simply better at managing application security.

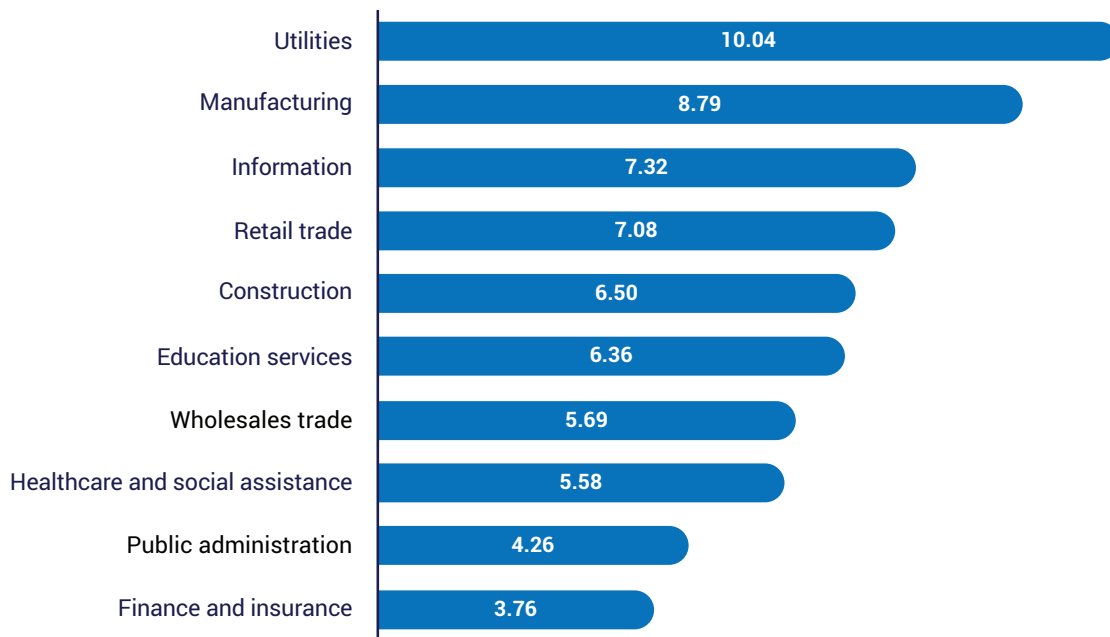


Figure 9: Average number of vulnerabilities per site by industry

While attack types have generally narrowed, malware has become more diverse. The use of worm functionality has multiplied; coin miners experienced a surge; ransomware continued to evolve; and attackers made use of a variety of Trojans, including banking Trojans and Remote Access Trojans (RATs).

Malware is the most commonly cited threat facing organizations in the next 12 months

58%

of organizations say **they're not prepared** for a malware attack

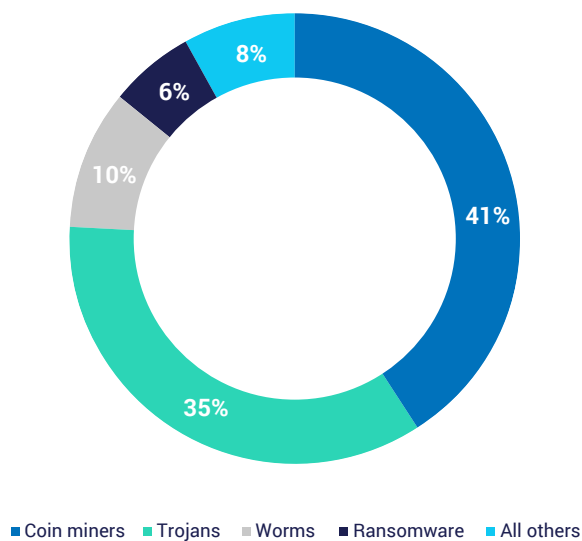


Figure 10: Breakdown of global malware detections by malware family

Coin miners replaced spyware as the most common type of malware globally. The most common malware was the XMRig miner, which showed the most detections of any single malware – about five times as many detections as the next most common malware, NetSupport Manager. XMRig accounted for 33% of all specific malware detections, and nearly 82% of all miner activity globally.

Malware	Malware family	Percent of malware
XMRig	Coin miner	33%
NetSupport Manager	RAT	6%
Morto	Worm	6%
Emotet	Trojan	5%
NetWalker	Ransomware	4%

Figure 11: Five most commonly detected malware globally

In reality, NetSupport Manager is not malware. It is a Windows-centric, cross-platform remote access tool. But it can serve a dual purpose. It was originally designed and used as a tool to provide remote support from a centralized location, such as for a distributed workforce. It can be used to gain full control of the target machine, including downloading and installing additional software. NetSupport Manager has also been widely adopted for nefarious purposes by hostile threat actors and is often identified as malware when used in such ways.

XMRig is a coin miner, which is a type of program that uses hardware resources to generate cryptocurrencies, such as Bitcoin, Monero, or Ethereum. Attackers can compromise an organization's resources and install coin miners, which may lead to a degradation in reliability as the coin miner uses system resources. XMRig mines the Monero cryptocurrency.

Attackers distribute NetSupport Manager via email attachments, online advertising and social engineering. One common technique was fake notifications which informed the user 'You are using an older version of Chrome' and prompting for a download which actually installed NetSupport Manager. It's widely used in schemes like fake Microsoft tech-support contacts. Once the attacker gets the user to click on a link or download the tool, the attacker uses the download and management capabilities to get full control of the targeted device and install additional malware.

While globally, only about 6% of malware was detected as NetSupport Manager, these attacks tend to be very successful and provide attackers with robust access to the end user's system.

Remote software was not the only malware that experienced success in 2020. Ransomware continues to account for less than 6% of all malware. However, in previous years, this number has hovered at near 4%. While the overall numbers have been relatively consistent, use of NetWalker surged in 2020 and accounted for over 79% of all ransomware detections.

While XMRig was the single most common malware detected in the education industry, every industry was different. Moreover, no malware appeared in every industry's top 10 list. Worms were the most common malware in finance and manufacturing. Healthcare was led by a RAT, education was led by a coin miner, and technology by ransomware.

Industry	Specific malware	Malware family
Finance	Conficker – 14%	Worm
Manufacturing	Morto – 34%	Worm
Healthcare	NetSupport Manager – 57%	RAT
Education	XMRig – 62%	Miner
Technology	NetWalker – 71%	Ransomware

Figure 12: Top globally detected malware by industry

Although some specific malware dominated several industries, every industry experienced all the major families of malware and a wide variety of specific named malware. Targeted technologies and applications also varied widely, often depending on the industry being targeted.

Targeted technologies

While attackers continue to target content management systems (CMSs), it wasn't at the level observed during 2019. Instead, attacks against ThinkPHP dominated the list of targeted technologies. In nearly 30% of all attacks targeting identified technology, ThinkPHP was the single most attacked technology globally. It was also the most attacked application in finance, manufacturing and technology, and was in the top 10 targeted technologies in every industry analysed.

One contributor to the widespread targeting of ThinkPHP is the fact that exploits have been implemented into multiple botnets for propagation and distributed denial-of-service (DDoS) attacks. This helped make attacks targeting ThinkPHP automatic, simple and more commonplace.

Targeted application or technology	Technology use	Percent of attacks 2020
ThinkPHP	Web-application development framework based on PHP; vulnerabilities are often related to NoneCMS or ECShop, among others	30%
Zeroshell Net Services	Small, open-source Linux distribution for servers and embedded systems	6%
PHPUnit	Testing framework for PHP, supports web-enabled services, especially CMS like WordPress and Drupal	5%
OpenSSL	Cryptography library often embedded in systems, operating systems or equipment to protect electronic communications	4%
D-Link devices	Network devices like routers or VPN servers	3%

Figure 13: Top targeted technologies globally

One contributor to the widespread targeting of ThinkPHP is the fact that exploits have been implemented into multiple botnets for propagation and distributed denial-of-service (DDoS) attacks.

Many technologies were targeted on a global basis, but none with the same volume as ThinkPHP. Other technologies tended to show targeting rates that were highly dependent on the industry being attacked. For example, vBulletin was highly targeted in education but Zeroshell Net Services was highly targeted in healthcare.



Regional analysis

Some trends were visible on a global basis, like increasing numbers of application-specific and web-application attacks. But certain details about hostile activity differed by the geographic areas in which they occurred. For instance, cryptominers dominated activity in EMEA and the Americas, but were relatively rare in Asia Pacific (APAC). Likewise, OpenSSL was the most targeted technology in the Americas but was not even on the top 10 list in APAC.

Analysing the differences in techniques and tools can provide insight into how hostile threat actors are targeting organizations in different geographic regions and countries.

The Americas

Like every other region, as well as globally, the top two attack types in the Americas were application-specific and web-application attacks. But the Americas showed the lowest total for those combined attack types, at 56%. This was below the global average of 67%. This gap was filled by DoS/DDoS and brute-force attacks, both of which were higher in the Americas than any other region.

Business and professional services was the most attacked industry in the Americas. The only other country in which the industry was highly attacked was Sweden (#3 at 11%).

Industry and percent of attacks in the Americas	Percent of attack types for industry
Business and professional services – 26%	Reconnaissance – 29% Application-specific – 19% Brute-force – 18%
Finance – 22%	Application-specific – 38% Web-application – 32% Reconnaissance – 17%
Hospitality, leisure and entertainment – 18%	Web-application – 76% Application-specific – 14% Brute-force – 7%

Figure 14: Percent of attacks and percent of attack types per industry in the Americas

Within the Americas, the US accounted for two of the highest rates of reconnaissance activity of any country analysed:

- Some 64% of all hostile activity targeting the technology industry was some form of reconnaissance.
- In the education industry, 58% of all hostile activity was reconnaissance.

Despite the high levels of reconnaissance in these two industries, overall reconnaissance in the Americas accounted for 23% of all hostile activity. This was only slightly above the global average of 20%.

Globally, both DoS/DDoS and brute-force attacks tended to appear relatively low on the list of common attack types. The Americas observed 8% of all attacks as DoS/DDoS attacks, while these attacks accounted for under 4% in APAC and 1% in EMEA. Attacks in specific industries were higher; for example, DoS/DDoS attacks accounted for 28% of all attacks against manufacturing organizations in the US.

It was also uncommon to see more than 1–2% of brute-force attacks against a specific industry. However, attackers targeting business and professional services (18%) and hospitality, leisure and entertainment (7%) made use of brute-force attacks during targeting.

The most common technologies attacked in the Americas also differed from global observations. In the Americas, OpenSSL was the most targeted technology. ThinkPHP, which was the most attacked application globally, emerged at fourth place as the target of 9% of all attacks. This was well below the global average of 30%.

Targeted technology in the Americas	Percent of attacks targeted
OpenSSL	14%
Adobe Digital	11%
Squid	10%
ThinkPHP	9%
WordPress	7%

Figure 15: Top targeted technology in the Americas

With 34% of all malware detections, XMRig was the most detected malware in the Americas and in the US, but comparably, EMEA observed significantly more XMRig. NetSupport Manager was the second most detected malware globally (6%) and in the US (13%). The US observed a higher rate of NetSupport Manager than any other country. While it was observed in other countries, it did not appear in any other list of top five malware. And while every country experienced a variety of malware, the US and Japan were the only countries analysed to experience more than one form of worm in their top 10 most commonly detected malware (Morto (13%) and Conficker (2%) for the US). The US also experienced a higher rate of Morto detections than any other country analysed.

Malware detections in the US	Percent of all malware	Malware family
XMRig	34%	Miner
NetSupport Manager	13%	RATs
Morto	13%	Worm
Cryptominer	10%	Miner
Torpig	4%	Botnet

Figure 16: Top malware detections by malware family in the US

Morto is a worm that targets Windows workstations and servers. When activated, it checks to see if Windows Remote Desktop Protocol (RDP) is enabled. It then attempts to log on as 'Administrator' with a preloaded password list. If it can open an RDP session, it copies itself to the targeted machine and repeats the process. This capability allows Morto to keep spreading once it's launched. Morto also enables remote control for the attacker, which gives the remote attacker local administrative control.

Europe, Middle East and Africa

Attacks in Europe, Middle East and Africa (EMEA) followed many of the same global trends, while showing some significant differences in technologies and malware observations. Targeted industries were quite narrow across the region, considering the differences in countries and their respective policies and initiatives. While the numbers varied somewhat in each country, healthcare, manufacturing and finance were the most attacked countries in EMEA, but some of the activity in those industries showed marked differences from other regions.

Industry and percent of attacks in EMEA	Percent of attack types for industry
Healthcare – 37%	Web-application – 62% Application-specific – 36% Network manipulation – 1%
Manufacturing – 31%	Application-specific – 50% Web-application – 27% Reconnaissance – 19%
Finance – 14%	Application-specific – 68% Web-application – 16% DoS/DDoS – 8%

Figure 17: Percent of attacks and percent of attack types per industry in EMEA

Healthcare was the most attacked industry in EMEA. The levels of attacks in all three of these industries were a result of the sheer amount of additional attack volume placed on these industries during the global pandemic. The combined attacks from web-application (62%) and application-specific (36%) attacks targeting healthcare in EMEA accounted for 98% of all hostile activity. This is well above the global average of 67%. It emphasizes just how much attention attackers focused on the web presence of these organizations, and how strongly they targeted their web-enabled applications.

As a region, EMEA experienced 79% of all attacks as combined application-specific (42%) and web-application (37%) attacks. At 91% of all such attacks, the UK had the highest rate of combined web attacks of any country analysed.

While technology has been among the top one or two most attacked industries in five of the past seven years, it did not appear in the top five industry list for any country analysed in EMEA.

Targeted technology in EMEA	Percent of attacks targeted
ThinkPHP	32%
Zeroshell Net Services	10%
PHPUnit	6%
Microsoft SQL Server	6%
Palo Alto Networks Devices	5%

Figure 18: Top targeted technology and percent of attacks in EMEA

In EMEA, targeting of ThinkPHP slightly exceeded the global average of 30%, and like other regions, targeted technologies dropped off sharply. Targeted technologies varied greatly by country in EMEA. Palo Alto devices were the most targeted in the UK&I; Zyxel devices in Germany; OpenSSL in France; and ThinkPHP in Sweden, Benelux and the Netherlands. But the technologies targeted were highly dependent on the industries being attacked. ThinkPHP and PHPUnit were highly targeted in finance and manufacturing organizations, which were the two most attacked industries in EMEA. Healthcare was highly targeted via Zeroshell Net Services.

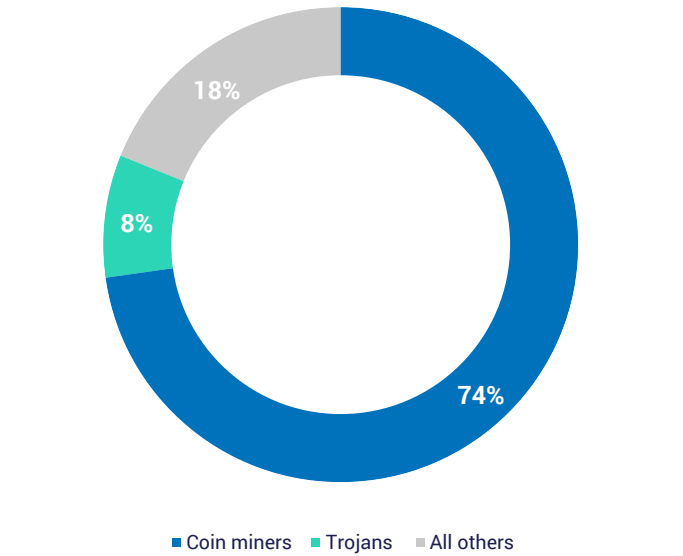


Figure 19: Breakdown of malware family detections in EMEA

Despite the differences between the countries, malware in EMEA was more consistent than in other regions. Overall, EMEA was dominated by miners, which accounted for 74% of all malware activity in the region. Miners were the most detected form of malware in the UK&I, Germany and Benelux.

Malware	UK & Ireland	Germany	Sweden	Norway	Benelux
XMRig	86%	65%	2%	<1%	89%
Coinmine	1%	2%	44%	37%	<1%
Trojans	Tofsee – 8%	Emotet – 15% Tofsee – 12% Trickbot – 2%	NetWiredRC – 17% GraceWire – 16%	GraceWire – 23% NetWiredRC – 17%	Trickbot – 2%

Figure 20: Percent of malware detections by country in EMEA

While most countries in EMEA experienced multiple miners, XMRig accounted for nearly 99% of all miner activity in EMEA and for over 87% of all malware detections. XMRig or Coinminer were the most common malware detected in every country analysed in EMEA.

Trojans were the second most common form of malware within EMEA. In the UK&I, six of the 10 most observed malware were some form of Trojan. In Sweden, four of the top five malware were a Trojan. Three of the top five malware in Germany were some form of Trojan. The most common Trojans observed in EMEA were Tofsee and Emotet. And, while miners dominated overall volume, each country experienced a greater variety of Trojans. Activity in each country was led by different Trojans, but Trickbot was in the top 10 most detected malware in over 80% of the countries analysed in EMEA.

Top 10 specific malware			
UK&I	Germany	Sweden	Benelux
XMRig	XMRig	Coinmine	XMRig
Tofsee	Emotet	NetWiredRC	Mirai
Conficker	Tofsee	GraceWire	Trickbot
Coinmine	Coinmine	njRAT	njRAT
Emotet	Trickbot	Gh0st	Coinmine
Bisonal	Regin	Conficker	Emotet
Trickbot	Torpig	Dorifel	Gh0st
Coinhive	EternalBlue	Viper	JexBoss
CryptInject	RIG	XMRig	Parite
NetWiredRC	Plead	WhatWeb	Regin

- Miners
- Trojans
- Botnets
- Worms
- Exploit Kits
- Ransomware
- Scrapers

Figure 21: Top 10 detected malware in the UK&I, Germany, Sweden and Benelux

While there were some global consistencies, there were also some regional differences in experienced malware. While the global average for botnets was 10%, barely 2% of malware activity in EMEA was associated with botnets. Despite the global average of ransomware rising to 6% of malware, organizations in EMEA experienced less than 1% of their malware as ransomware.

Asia Pacific

While many observations on activity within the Asia Pacific (APAC) region were consistent with details from global and other regional data, APAC experienced significant differences from some of the other geographic areas. Attacks against education dominated in several countries, and the industry joined finance and manufacturing as the most common targets in APAC. APAC had higher levels of botnet activity, and webshells made their impact felt throughout much of the region.

Industry and percent of attacks in APAC	Percent of attack types for industry
Finance – 24%	Web-application – 51% Application-specific – 22% Service-specific – 18%
Manufacturing – 22%	Application-specific – 59% Reconnaissance – 30% Web-application – 5%
Education – 18%	Web-application – 30% Application-specific – 26% Brute-force – 25%

Figure 22: Percent of attacks and percent of attack types per industry in APAC

Finance was the most attacked industry in APAC, led by activity in Australia and New Zealand. Attacks were consistent with the types of attacks observed globally, with web-application (51%) and application-specific (22%) attacks combining to account for 74% of all hostile activity. This was slightly higher than the global average of 67%. Service-specific (18%) attacks were the third most common in APAC. These attacks tend to be more advanced and less commoditized than many of the application-oriented attacks.

The second most common hostile activity targeting manufacturing was reconnaissance. This was the highest rate of reconnaissance in any of the industries analysed in the region. However, several other industries in Australia and New Zealand did show elevated levels of reconnaissance. While reconnaissance was the third most common form of hostile activity (20%) globally, most industries in APAC other than manufacturing experienced less than 6% of attacks as reconnaissance.

And while most attacks targeting education followed global expectations, brute-force attacks targeting education in APAC accounted for 25% of all hostile activity. This was the highest rate of brute-force attacks against any industry in any region or country analysed.

Targeted technology in APAC	Percent of attacks targeted
ThinkPHP	35%
Apache Struts	6%
D-Link devices	5%
vBulletin	5%
Linux	4%

Figure 23: Top targeted technologies in APAC

With 35% of all attacks, ThinkPHP was the most targeted application in APAC, exceeding the global average of 30%. Targeting of ThinkPHP was higher in Japan than many other APAC countries. ThinkPHP was widely used by attackers of finance, manufacturing, technology and education. These were the top four industries attacked in the region.

Targeting of other technologies was distributed widely throughout APAC, with only targeting of D-Link devices also appearing in the global list. All five of the most targeted technologies appeared heavily in the most targeted industries in the region.

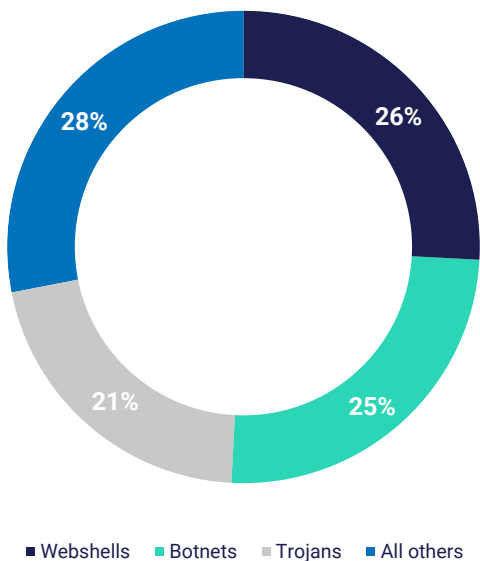


Figure 24: Breakdown of malware family detections in APAC

Malware varied greatly throughout APAC, but webshells, botnets and all forms of Trojans combined to account for 72% of all malware. The type of malware detected depended greatly on the country and industry being targeted.

Japan		Australia	
Mirai – 19%	Botnet	Mariposa – 36%	Botnet
Emotet – 17%	Trojan	China Chopper – 27%	Webshell
njRAT – 7%	Trojan	Winnti – 12%	Trojan
Conficker – 6%	Worm	Mirai – 6%	Botnet
Mariposa – 5%	Botnet	NetWiredRC – 5%	Trojan

Figure 25: Top malware detections in Japan and Australia

While Mirai was observed in nearly every country in APAC, it was the single most detected malware in Japan, especially targeting manufacturing and technology. Mariposa and China Chopper were the two most common malware in Australia, especially in education. Throughout APAC, botnets showed the highest volume of any malware family. Like EMEA, most countries in APAC tended to show activity from at least four different Trojans in their list of top 10 most observed specific malware. Throughout the region, Emotet and NetWiredRC were the most commonly detected Trojans.

Top 10 specific malware			
Japan	Australia and New Zealand	Singapore	
Mirai	Mariposa	XMR-Stak	Miners
Emotet	China Chopper	Virut	Botnets
njRAT	Winnti	Trickbot	Trojans
Conficker	Mirai	Zeus	Worms
Mariposa	NetWiredRC	Banload	Exploit Kits
DarkHotel	Emotet	NetWiredRC	Keyloggers
Bisonal	Morto	Conficker	Webshells
Ramnit	Gh0st	Coinmine	
Wapomi	Ganiw	Fiesta	
IoTroop	Bladabindi	Bottle	

Figure 26: Top ten detected malware in Japan; Australia and New Zealand; and Singapore

While XMRig was the most commonly detected malware globally, no country in APAC showed XMRig in their top 10 most common malware. In fact, Singapore was the only country analysed in APAC that experienced a significant amount of activity from any form of cryptominer (75% of activity in Singapore, while less than 1% in the rest of APAC).

As threats continue to evolve, it's critical for organizations to understand targeting patterns for their specific industry and how best to prepare.

7547 2374.71698113208

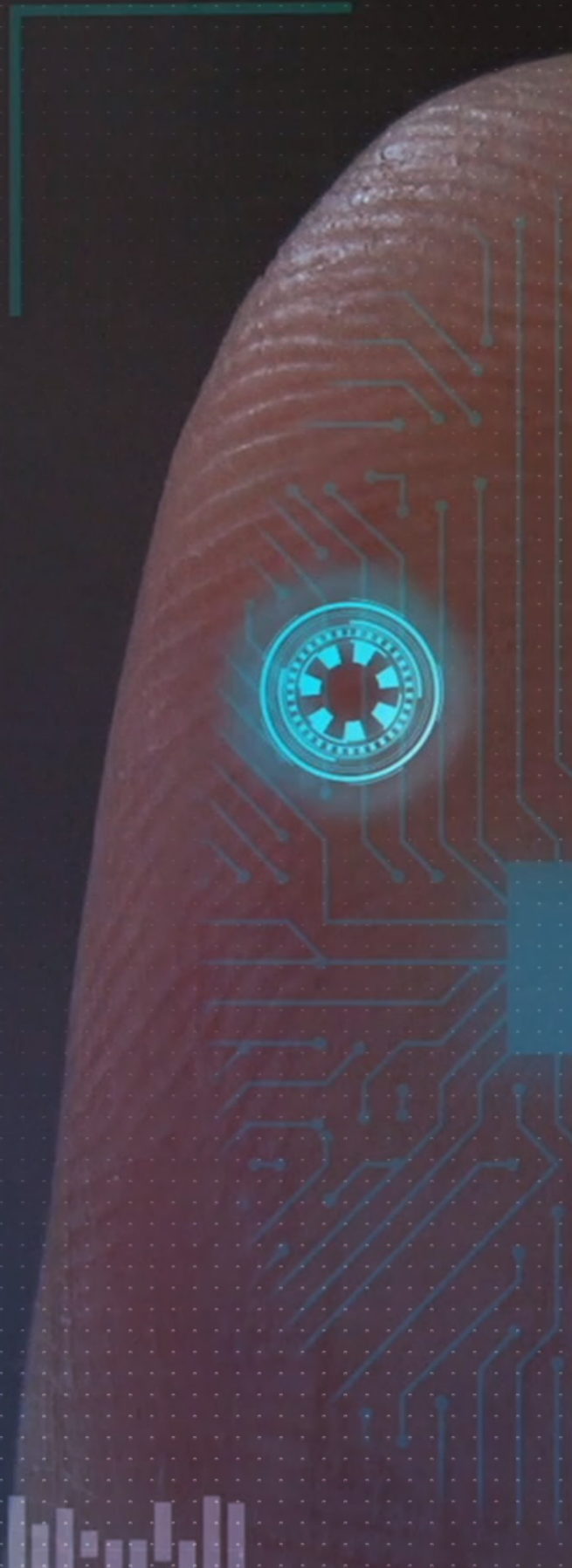
2445 953.200626959248

7143 424.428571428571

Focus on industries

In 2020, globally we observed less correlation between attack types and targeted industries. But in every region and country, we observed greater correlation between the malware used, the technologies being targeted and the industry of interest. Industries have a set of technologies of concern, on which they're focusing cybersecurity initiatives.

Protecting cloud services is the top cybersecurity focus area globally, cited by half of the respondents to our research. Network and application security, and securing IoT/operational technology were also stated as top focuses for organizations.



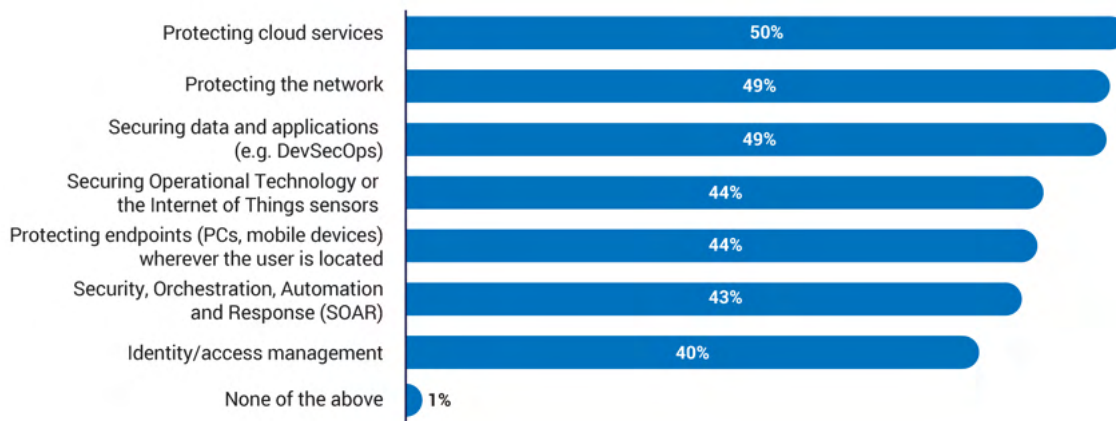


Fig 27: Cybersecurity technology focus in next 18 months

Meanwhile, attackers have their own priorities, and the technologies upon which they focus are almost predictable, with the top few technologies regularly accounting for more than half of attacks.

Much of the malware being used has become more commoditized, general purpose and multi-functional. But oddly enough, the malware being used to target specific industries has also tended to become more focused. Attackers have the malware they prefer to use, depending on the industry being targeted.

Finance

The finance industry is in a unique position compared to other industries. Attackers targeting the finance industry have three essential motivations: stealing data, modifying data integrity and committing direct financial theft. The motivations have not changed dramatically over the past year, but the available targets have. With bank lobbies closing due to COVID-19, some financial organizations saw less foot traffic. That traffic was redirected to mobile and online banking, which experienced an increase in use as customers relied more on digital services. Hostile threat actors also recognized and took advantage of this increased reliance on web-enabled apps.

Overall, attackers have demonstrated a willingness to continue targeting the finance industry, despite its security posture. Over the past nine years, we've found the finance industry to be the most targeted industry six times. Despite its heavy security apparatus, in 2020 finance was once again the single most attacked industry of the industries analysed. Attacks against finance represented 23% of all observed attacks. This was primarily related to about a 50% increase in attack volume and demonstrates that attackers still find value in the industry's data. While finance was the most attacked industry globally, the only analysed country in which finance was the most attacked

industry was Australia, where it was the target of 46% of all attacks. The industry is generally perceived as a target-rich environment containing both personal and financial data.

Targeting the finance industry

Due the large amounts of valuable data financial organizations maintain, they're a frequent target of threat actors. The value of this data is demonstrated by the consistent level of attacks against this industry, year after year. Financial organizations tend to have sizable client bases who access their account information through client portals. Attackers regularly target individuals for their log-on credentials, but also frequently target the exposed applications that service these external clients. The top attacks targeting the finance industry were application-specific and web-application attacks. Combined, these two attack types accounted for 73% of all attacks against the industry. In comparison, less than 3% of all hostile activity targeting the finance industry were DoS/DDoS attacks. This indicates that attackers are less interested in disrupting the operations of finance institutions than in compromising them.

Given the value and variety of information stored by finance organizations, strict regulations and requirements exist to protect consumer information and consumer and organizational financial details, and to prevent the likelihood of any fraudulent activities. While many of these regulations are decades old, new challenges exist. These include:

- new regulations that affect financial technology organizations
- risk from the adoption of cryptocurrencies
- implementation and support of new client portals
- central bank stress testing for climate change

According to our research, the finance industry had the lowest perception of threats.

Finance teams were less likely to perceive technical threats like ransomware, unpatched vulnerabilities or nation-state/organized criminal group attacks as an issue. However, finance had a higher perception of threats emanating from insider threats, supply chain issues, and failure to meet compliance obligations.

Our researchers found that ThinkPHP was the most attacked technology in the finance industry, comprising 36% of attacks. The second most attacked technology was PHPUnit, another PHP solution. The most commonly detected malware in the finance industry was Conficker, a worm which can spread through a known vulnerability in older Windows systems, network shares and removable drives.

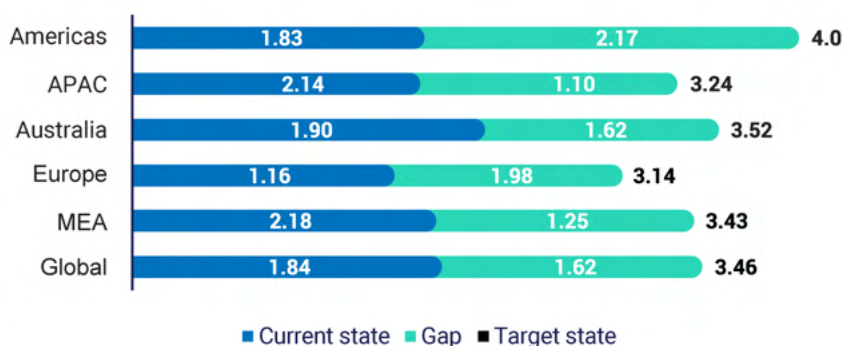


Figure 28: Finance - current and target maturity levels and the gap between them

As shown in Figure 28, finance's global baseline score in 2020 was 1.84, a slight dip from its benchmark score of 1.86 in 2019. Finance's global baseline was the second highest global average of the industries analysed, behind business and professional services. The MEA region leads globally with a 2.18 average maturity score, while organizations in Europe had the lowest maturity scores in the industry at 1.16. Finance organizations in Europe performed poorly in the Logical Security Architecture (1.03) and Risk Management (1.04) subcategories. Organizations can improve their scores by focusing resources on improving risk management and technical controls.

Top attack types	Top products targeted	Top malware variants
Application-specific attack – 42%	ThinkPHP – 36%	Conficker – 14%
Web-application attack – 31%	PHPUnit – 5%	Coinhive – 11%
Reconnaissance – 12%	OpenSSL – 5%	Brontok – 9%

Figure 29: Top targeting in the finance industry

Spotlight on: PHP technologies

We found the two most attacked technologies in the finance industry to be ThinkPHP (which comprised 36% of attacks) and PHPUnit (which comprised 5% of attacks). Altogether, 41% of attacks in the finance industry targeted PHP implementations. This was the highest attack rate of any industry analysed aside from manufacturing. The targeting of these technologies is likely aimed at the content management systems (CMSs) the finance industry uses in its web-facing sites and applications. PHPUnit is a widely used testing framework for PHP which also supports web-enabled devices, including content management suites like WordPress and Drupal. Likewise, ThinkPHP is a PHP framework used in NoneCMS.

This targeting is consistent with attackers overwhelmingly targeting the industry via application-specific and web-application attacks, which together accounted for 73% of all attacks against finance. The popularity of these attack types has seen year-over-year growth, rising from 67% of all attacks in 2018. By focusing on patching and securing PHP frameworks, the finance industry could potentially mitigate 41% of existing attack attempts.

Spotlight on: Worms

Worms are the single most detected malware variant affecting the finance industry, with Conficker and Brontok being the first and third most detected malware. These two malware types make up 23% of all detections in the finance industry. At 14% of all detections, Conficker was detected in finance more than any other industry analysed. Conficker spreads through a known vulnerability in Windows 2000, XP, Vista, Server 2003, Server 2008 and 7 Beta versions. Later versions of the worm spread via network shares with weak passwords and removable drives. Similarly, Brontok can spread by copying itself to USB drives, as well as through mass emailing copies of itself to contacts found in the address book on an affected system.

Both of these worms can disable certain Windows processes and security products, as well as download additional files and malicious code onto infected machines. Without the proper security precautions in place, worms can spread quickly throughout an organization. Organizations should ensure they have controls in place to prevent worm infections, such as:

- up-to-date patches and antivirus/antimalware services
- password policies that mandate the use of unique, complex passwords
- the implementation of multi-factor authentication whenever possible
- security awareness training to limit the chance of users' systems accidentally becoming infected via malicious attachments or links delivered by email

Governance, risk and compliance (GRC)

The finance industry is subject to GRC regulations which are intended to address how financial information is collected, managed and controlled. This includes directions regarding how organizations monitor transactions, perform disclosures, ensure the protection of data, handle risk, and prevent the illicit use and transfer of funds.

Important historic regulations put in place to protect financial transactions, processes and data include the US Sarbanes-Oxley Act of 2002, Japan's JSOX, the UK's Turnbull, MI 52-109 and Bill 198 in Canada. In early 2019, China's central bank released rules intended to prevent money laundering and terrorist financing through better 'know your customer' rules. China followed up on these rules with further regulations throughout 2020 tightening controls on how online finance platforms lend money. Similar regulations are being implemented globally as central banks and regulators worldwide introduce various measures such as:

- transaction thresholds
- on digital payments
- lending platforms

For example, California signed into law Assembly Bill 1864, which creates a new regulatory regime for financial services offered by fintech organizations. As many fintech organizations in the US are based in Silicon Valley, this law could have widespread effects.

Regarding anti-money laundering compliance, the US Financial Crimes Enforcement Network has proposed changes to the Bank Secrecy Act (BSA). The changes, which are under review as of the issuing of this Report, are intended to improve the effectiveness of anti-money laundering program requirements. Any changes to the BSA would impact how financial organizations create suspicious activity reports and currency transaction reports. This would have an impact on how the global financial industry handles reporting on detected suspicious financial activity.

The finance industry also faces increased risk from the growing adoption of cryptocurrency by financial institutions and pilot programs by central banks and fintech organizations. Any use of cryptocurrency requires strong security safeguards to ensure data integrity. Further risk facing the finance industry comes from the cumulative effects of climate change. The central banks of the UK, Australia and Japan have announced stress testing to prepare for climate change. Meanwhile, financial institutions face pressure from activists, regulators and clients to divest from financing projects linked to the fossil fuel industry.

Application security analysis

The finance industry continues to lead industries analysed in terms of its overall likelihood of exposure, though it has exposures lower than global averages across all the Open Web Application Security Project (OWASP) Top Ten vulnerability categories. The large difference in the likelihood of exposure between the industry's top five serious risk vulnerability classes and the top five vulnerabilities of all risk severity speaks to an approach of addressing application security through a robust prioritization process which includes vulnerability risk as a key factor.

Analysis of remediation rates in 2020 (37% overall versus 60% 'serious' risk) and time-to-fix (70 days overall and 57 days for 'serious' risk) bears out this idea of risk prioritization while revealing an opportunity for improvement. Unlike exposure likelihoods, these time-to-fix metrics are not as strong relative to other industries analysed. The overall picture for finance painted by the vulnerability data reveals that the industry leads others in application security practices and that it delivers strong results in overall vulnerability prevention. However, like all other industries analysed, finance struggles to find the right formula to quickly address exposures when they are detected.

Top 5 serious vulnerabilities	Likelihood of serious exposure
Insufficient transport layer protection	13%
Cross-site scripting	6%
Directory indexing	3%
Insufficient authorization	2%
URL redirector abuse	2%

Figure 30: Finance's likelihood of exposure to top serious vulnerabilities

Top 5 vulnerabilities	Likelihood of exposure
Insufficient transport layer protection	56%
Information leakage	36%
Improper input handling	30%
Frameable resources	21%
Fingerprinting	14%

Figure 31: Finance's likelihood of exposure to top five vulnerabilities

Recommendations

NTT has conducted consulting engagements and found the MITRE ATT&CK framework to be robust and provide excellent information to help organizations address cybersecurity threats and mitigate risk. As it is a powerful resource, NTT has chosen to align our suggestions for mitigation recommendations to this framework:

Mitigation	MITRE ATT&CK ID	Description
Vulnerability scanning	M1016	Routinely assess applications for vulnerabilities and institute a patching schedule to rapidly address critical vulnerabilities
Antivirus/antimalware	M1049	Use heuristic-based malware detection which has updated virus/malware definitions; create custom signatures as needed
Exploit protection	M1050	Leverage capabilities for detecting and then blocking any conditions which could cause or signal the occurrence of a software exploit; use web-application firewalls to limit application exposure to exploit traffic

Figure 32: Recommendations for the finance industry

Manufacturing

The manufacturing industry faced unique challenges over the last year. While manufacturing notoriously faces cyber-espionage attacks linked to the theft of intellectual property, the industry also experienced a surge in overall targeting, accounting for 22% of all detected attacks. This was an increase in volume of nearly three times compared to 2019. Of the industries analysed, manufacturing was the second most targeted in 2020. These cyber-challenges were further compounded by the impact of the COVID-19 pandemic. This caused demand for some items to plummet while demand for others, such as personal protective equipment, surged to levels that were difficult to sustain. This placed a burden on the global supply chains underpinning the manufacturing industry for high-demand products. In some cases, manufacturing organizations were already under strain due to an increase in tariffs and global trade disagreements.

The increase in the use of a remote workforce also raised the chances of cybersecurity incidents, as individual employees at home became the new entry point for attacks. Manufacturing also faced challenges from increased adoption of automated and embedded technologies. According to our research, 38% of respondents from the manufacturing industry were aware of threats to the Internet of Things (IoT) devices and operational technology. This was above the average of 30% for respondents from all industries.

As manufacturing spans a wide variety of subsectors, compliance requirements can vary widely. However, compliance tends to focus on workplace safety, the safety and reliability of the finished goods, and the organizations' overall environmental impact. As greater numbers of countries pledge to become carbon neutral within the next several decades, manufacturing organizations will face greater scrutiny. Not only do they have to worry about non-compliance penalties, they must also consider an increasingly pro-environment consumer sentiment.

We observed attacks targeting ThinkPHP and PHPUnit as accounting for 48% of all attacks against the manufacturing industry. This was the highest proportion of PHP attacks against any of the industries analysed. Overall malware activity against the industry was largely consistent with previous targeting. Virus and worm detection accounted for 36% of all detections. Manufacturing also saw a large percentage of malware detections stemming from the Mimikatz password stealer (15% of malware in manufacturing, but less than half of a percent in every other industry analysed). Overall, activity against manufacturing was the most consistent of the industries analysed when compared to previous years.

Targeting the manufacturing industry

Manufacturing organizations are a frequent target of threat actors due to the sensitive and proprietary information they hold. Over the past nine years, manufacturing has been one of the five most targeted industries seven times. Historically, targeting against the manufacturing industry has included significant reconnaissance activity. Such activity made up 24% of all hostile activity in 2020, in line with 22% of all activity in 2019. A high level of malware activity is also consistent in the industry, with virus/worm activity representing 36% of all detections in 2020, down marginally from 43% of all detections in 2019. Manufacturing detections also included penetration testing and data-exfiltration malware, indicating attackers are interested in finding vulnerabilities within manufacturing organizations that they can leverage for espionage and potential data theft. Overall, 69% of attacks against the manufacturing industry were application-specific (49%) or web-application (20%) attacks, in line with the global average of 67%. However, these two attack types made up 92% of attacks on manufacturing in Japan, 90% in Germany and 93% in the UK. These were all well above the global average.

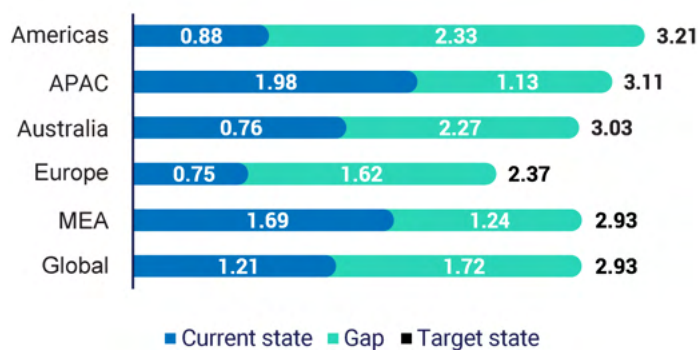


Figure 33: Manufacturing - current and target maturity levels and the gap between them

Figure 33 shows an average maturity level of 1.21 for the manufacturing industry, a slight drop from the 2019 baseline score of 1.32. Based on analysis of results, it appears this drop is likely due to the increased number of Cybersecurity Advisories we're completing for first-time manufacturing clients. Organizations in APAC lead with a 1.98 average maturity score and showed the highest regional score in Security Vision and Strategy. Manufacturing organizations in MEA also performed better than the global average, with a 1.69 average maturity score. Europe (0.75) and Australia (0.76) manufacturing maturity averages were significantly behind other regions. Both regions had low scores for Security Vision and Strategy (0.42 and 0.40 respectively).

Top attack types	Top products targeted	Top malware variants
Application-specific – 49%	ThinkPHP – 40%	Morto – 34%
Reconnaissance – 24%	PHPUnit – 8%	Mimikatz – 15%
Web-application – 20%	Palo Alto Networks – 6%	Parite – 12%

Figure 34: Top targeting in the manufacturing industry

Spotlight on: Potential espionage

As organizations attempted to manage their workforces and remain productive during COVID-19, they were often forced to enable remote access and more distributed operations to continue conducting business. As a result, many organizations were not prepared to fully secure their evolving environments, potentially remotely exposing servers and services (which were often unpatched and misconfigured). This is especially true in industries that have seen rapid evolutions in services such as manufacturing.

Our researchers found the Morto worm to be the top malware detected in the manufacturing industry, comprising 34% of all detections. Manufacturing was the only industry analysed to have Morto in their top ten most detected malware. Morto infections can stem from being dropped by other malware, downloaded from the internet, or through self-propagation via Remote Desktop Protocol (RDP). Morto variants search for RDP servers on a network, then try to log on as an administrator. Successful compromise provides the attacker with administrative control of the network, including the ability to exfiltrate data.

The second most detected malware variant in the manufacturing industry was Mimikatz (15% of all detections). Mimikatz is a password stealer that allows an attacker to obtain Windows account logins and passwords in cleartext. Given the high-value information manufacturing organizations possess, the industry should prioritize a defense-in-depth strategy to limit the potential impact of malware allowing for data exfiltration.

Spotlight on: PHP attacks

NTT researchers observed high levels of attacks against ThinkPHP and PHPUnit in the manufacturing industry. Attacks against ThinkPHP constituted 40% of all attacks against manufacturing, while attacks against PHPUnit made up 8% of total attacks against the industry. This was the highest rate of targeting for these technologies in any of the industries analysed. A large proportion of this targeting was likely due to reconnaissance activity within the manufacturing industry. Reconnaissance activity accounted for 24% of hostile activity against manufacturing, with port scanning accounting for

56% of activity. This scanning activity is likely due to both the Morto worm scanning for open RDP ports, as well as attackers scanning for PHP vulnerabilities.

We found Mirai and its variants accounted for 11% of all malware activity in the manufacturing industry. As Mirai is known to specifically target PHP vulnerabilities, the high level of PHP targeting in the industry is likely due to botnet activity. By prioritizing securing PHP implementations, the manufacturing industry can potentially mitigate as much as 48% of current malicious activity.

Governance, risk and compliance (GRC)

GRC is unique to each manufacturing subsector and can apply domestically, or internationally, covering a wide range of compliance issues. Overall, GRC encompasses technical, legal and corporate regulations with which manufacturers must comply to produce and market goods.

Overall, the manufacturing industry faces numerous regulations across subsectors, especially environmental regulations. These are likely to increase as countries announce plans to become carbon neutral in the following decades. Such pledges will increase regulatory compliance pressure on manufacturing organizations. They will have to find ways to offset their carbon footprint or face non-compliance violations, fines and potential substantial brand damage as activists increase pressure on organizations to 'go green'.

Additional, specific regulations govern the differing manufacturing subsectors, and strict regulations are in place for manufacturing medical devices and consumable products. As supply chains become more complex, especially due to reorganization in the wake of the COVID-19 pandemic, organizations must ensure every vendor and partner organization is compliant. Failing to properly vet new partners can open organizations up to substantial risk from both a cybersecurity and quality assurance perspective.

Overall, regulations are expected to grow across the manufacturing landscape as more organizations make the shift towards manufacturing 4.0, which leverages modern, smart technology such as machine-to-machine communication and an increased number of IoT devices.

Application security analysis

In most vulnerability classes, the manufacturing industry faces the highest likelihood of exposure. In particular, their likelihood of exposure to A1 – Injection (7%) is over three times the global average (2%). Of these injection exposures, 100% of them are SQL injections. In contrast, their remediation timeframe for both ‘all vulnerabilities’ and ‘serious vulnerabilities’ are among the lowest of the industries analysed (53 days and 50 days, respectively).

This divergence between exposure and remediation rates can be explained through an analysis of two factors. First, the mediation rate for serious risk vulnerabilities reported in 2020 was among the lowest measured (47%). This speaks to a remediation posture that reacts quickly to a small number of vulnerabilities while overall remediating a small number of them. Second, the low number of applications scanned compared to the industry size could represent a relatively small density of internet-facing applications within the industry, but more likely represents a low level of overall industry maturity regarding application security.

Top five serious vulnerabilities	Likelihood of serious exposure
Cross-site scripting	21%
Cross-site request forgery	10%
Insufficient authorization	8%
URL redirector abuse	8%
Injection	7%

Figure 35: Manufacturing's likelihood of exposure to top serious vulnerabilities

Top five vulnerabilities	Likelihood of exposure
Insufficient transport layer protection	69%
Information leakage	54%
Frameable resource	38%
Fingerprinting	36%
Predictable resource location	34%

Figure 36: Manufacturing's likelihood of exposure to the top five vulnerabilities

Recommendations

The following are our mitigation recommendations for the threats facing the manufacturing industry:

Mitigation	MITRE ATT&CK ID	Description
Exploit protection	M1050	Leverage web-application firewalls to limit application exposure to exploit traffic
Network intrusion prevention	M1031	Use network intrusion detection and prevention systems, which can identify malware activity and traffic for command-and-control infrastructure through network signatures
Filter network traffic	M1037	Filter ingress and egress traffic and perform protocol-based filtering using network appliances

Figure 37: Recommendations for the manufacturing industry

Healthcare

The healthcare industry faced increased challenges in 2020 from a cybersecurity, logistical and public health perspective. It jumped from being the sixth most attacked industry in 2019, with 7% of detected attacks, to becoming the third most attacked industry in 2020, with 17% of all detected attacks. This is the highest healthcare has ranked in the nine years we have produced this annual Report. Overall, attack volumes against healthcare more than doubled in the past year. This is likely associated with cyberthreats related to more telehealth visits, an increase in healthcare digital infrastructure, and greater pressure on the healthcare industry as it attempts to drive management of COVID-19 outbreaks and vaccines.

Web-application and application-specific attacks accounted for 97% of all hostile activity targeting the healthcare industry. This is the highest of any industry analysed and significantly above the global average of 67% of hostile activity detections. Trojan activity continues against healthcare, accounting for over 72% of identified malware. This is up from 58% in 2019.

Notably, attackers have also launched ransomware attacks against hospitals and healthcare organizations with the assumption that they can force organizations to pay. Such attacks can lead to equipment and critical medical records being unavailable. This can lead directly to cancelling of surgeries and other services which are not only the source of the organization's revenue, but can result in delay in treatment, potentially including life-saving care.

Healthcare regulations and compliance requirements are primarily concerned with the safekeeping of private patient information, financial information, and data on healthcare service providers. Healthcare breaches can incur hefty financial penalties, while also causing long-term brand damage. Securing such information became more difficult in 2020 as the pandemic forced healthcare organizations to increasingly offer online-based telehealth appointments and the infrastructure needed to support such care, which opened another potential vector for attacks.

We observed attacks targeting Zeroshell Net Services accounting for 45% of all attacks against identified targets within the healthcare industry. Zeroshell is a Linux-based distribution which supports administrative, web-enabled interfaces. We also found that 57% of all malware activity targeting healthcare was from activity related to NetSupport Manager. Use of this malware enables attackers to gain full control over the target machine.

Targeting the healthcare industry

Healthcare organizations maintain databases filled with high-value information such as electronic healthcare records (EHI), PII, financial information and data from suppliers, including data from a wide range of healthcare service providers. The healthcare industry must have cybersecurity infrastructure in place that is secure and resilient enough to manage and protect this sensitive, high-volume data. Cybercriminals target these systems seeking to monetize or ransom the sensitive data through various application-specific and web-application attacks. These two types of attacks accounted for 59% and 38% of all hostile activity targeting healthcare, respectively. The healthcare industry is also susceptible to malware attacks, with the remote access tool NetSupport Manager accounting for 57% of all malware activity in this industry. The use of this tool is likely due to attackers targeting distributed users to obtain the valuable information healthcare organizations hold. The level and severity of these attacks increases the need for a focus on security by building cybersecurity infrastructures that are secure by design.

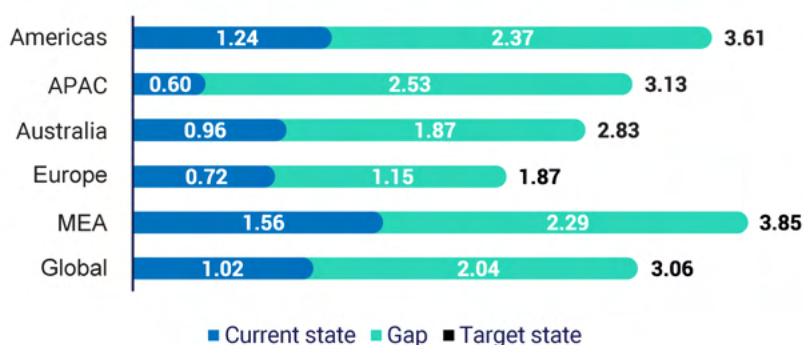


Figure 38: Healthcare – Cybersecurity Advisory scoring

As shown in Figure 38, the healthcare industry observed an average maturity level of 0.99, a slight decrease from 1.12 in 2019. Organizations within the APAC region showed the lowest maturity with average scores of 0.60. Organizations in APAC performed poorly in Risk Management (0.55) and Logical Security Architecture (0.58). Organizations in MEA led with a 1.56 average maturity score, with its most mature subcategories being Information Security Framework (2.03) and Risk Management (1.82). Organizations in the Americas scored best in the Risk Management subcategory, with an average score of 1.35.

Top attack types	Top products targeted	Top malware variants
Web-application – 59%	Zeroshell Net Services – 45%	NetSupport Manager – 57%
Application-specific attack – 38%	Cisco Data Center Network Manager – 7%	NetWalker – 11%
Known bad source – 1%	Apache Tomcat – 5%	Emotet – 9%

Figure 39: Top targeting in the healthcare industry

Spotlight on: Web-application and application-specific attacks

Web-application (59%) and application-specific (38%) attacks were the top two attack types against healthcare. Combined, web-application and application-specific attacks accounted for 97% of all hostile activity against healthcare. This is the highest concentration of these attack types in any of the industries analysed. The global average for application-specific and web-application attacks was 67% of attacks.

Attackers' focus on web-application and application-specific attacks is likely due to healthcare organizations scaling up their digital presence in the face of the pandemic. For example, the top three targeted products in the healthcare industry are Zeroshell Net Services, Cisco Data Center Network Manager and Apache Tomcat. If organizations prioritized patching vulnerabilities and fixing security misconfigurations in just these three products, it could potentially mitigate as much as 57% of current product targeting and would help decrease web-application and application-specific attacks.

Spotlight on: NetSupport Manager

We found NetSupport Manager to be the top malware detected in the healthcare industry, making up 57% of all malware detections. NetSupport Manager is a Windows-centric, cross-platform remote access tool which malicious actors have widely adopted for nefarious purposes. Attackers distribute NetSupport Manager via malicious email attachments, online advertising, social engineering, Microsoft tech support and related schemes. Once installed, it provides the remote attacker with full desktop functionality from outside the targeted organization.

Many healthcare organizations tend towards distributed operations, especially in a clinical setting, with a wide variety of workstations around a given facility. In times of COVID-19, healthcare organizations are making even more use of distributed working environments. This introduces risk, especially given that in a professional environment, employees are unlikely to be constantly vigilant about cyberattacks as that's not the nature of their jobs. If employees receive communication from a central authority (like an information systems department which is centralized, and not co-located with most staff), with assurances of improvements, it creates an ideal environment in which to operate NetSupport Manager.

Organizations should ensure they have up-to-date antivirus/antimalware on their systems, end-point protection and should prioritize user awareness training to help limit the likelihood of individuals accidentally installing NetSupport Manager. In addition, if organizations limit administrative rights, they can limit the ability of end users to install new software, such as NetSupport Manager.

Governance, risk and compliance (GRC)

GRC in the healthcare industry focuses on patient care, securing patient data and complying with healthcare regulations. Many healthcare organizations have made cybersecurity a top priority to bolster their defenses against breaches and the loss of personal healthcare information (PHI) and PII which can be sold and monetized by cybercriminals. These breaches can have a significant financial impact on affected entities. For example, throughout 2020, the US Health and Human Services Office for Civil Rights fined healthcare organizations millions in USD due to HIPAA violations.

C-suite healthcare concerns include regulatory changes and scrutiny; changes in management and succession challenges; and the ability to attract and retain top talent. Additional concerns include:

- privacy
- identity management and information security
- possible resistance to change in healthcare operations
- the ability of an organization's current operating procedures to meet stated performance expectations

Established organizations may also be unable to analyse large amounts of quantitative data and compete with healthcare start-ups which have deeper knowledge of data analytics and a larger digital footprint than most traditional healthcare organizations.

Cyberthreats and cybersecurity factor directly into an organization's culture if it doesn't place enough emphasis on employee cybersecurity training and education programs. Lack of training and education regarding cyberthreats within the organization could lead to difficulty in identifying, reporting and remediating breaches, thus increasing the healthcare organization's risk posture. These concerns and risks directly impact an organization's ability to retain clients and their loyalty.

Application security analysis

The healthcare industry saw the likelihood of exposure decrease across most of the OWASP Top Ten vulnerability classes. However, there was a notable exception with A6 – Security Misconfiguration, which remained steady at a 29% chance of exposure. This category includes multiple vulnerability classes and subclasses, such as Directory Indexing (6% chance of serious exposure). Organizations should view the overall decrease in likelihood of exposure with some caution as many applications scanned across the healthcare industry in 2020 were applications that they'd assessed in prior years. As such, the reduction in likelihood of exposure may represent a reduction in vulnerability introduction rates in existing applications, but it most likely represents the effects of remediation of vulnerabilities detected in prior years.

Overall, healthcare continues to struggle with remediation timeframes when compared to other industries. Vulnerability remediation in 2020 took an average of 80 days, and vulnerabilities rated as a 'serious risk' took an average of 93 days to remediate. This struggle to reduce remediation timeframes contributed to a relatively average performance in remediation rates. Organizations had fixed just over 39% of all vulnerabilities reported in 2020 and had resolved only 58% of serious vulnerabilities.

Top five serious vulnerabilities	Likelihood of serious exposure
Cross-site scripting	12%
Directory indexing	6%
URL redirect abuse	4%
Insufficient transport layer protection	4%
Insufficient authorization	2%

Figure 40: Healthcare's likelihood of exposure to top serious vulnerabilities

Top five vulnerabilities	Likelihood of exposure
Insufficient transport layer protection	64%
Information leakage	53%
Frameable sensitive resource	33%
Fingerprinting	22%
Improper input handling	17%

Figure 41: Healthcare's likelihood of exposure to the top five vulnerabilities

Organizations should view the overall decrease in likelihood of exposure with some caution as many applications scanned across the healthcare industry in 2020 were applications that they'd assessed in prior years.

Recommendations

The following are our mitigation recommendations for the threats facing the healthcare industry:

Mitigation	MITRE ATT&CK ID	Description
Network intrusion prevention	M1031	Use network intrusion/detection systems to prevent attackers from conducting scans for remote services
Encrypt sensitive information	M1041	Employ encryption for all sensitive information at rest in the cloud, all important data flows and on emails which contain sensitive information
Network segmentation	M1030	Employ network segmentation to isolate critical systems, functions and resources

Figure 42: Recommendations for the healthcare industry

Education

Education faced a year of increased challenges in 2020. Organizations were forced to grapple with school and university closures, a scramble to set up remote learning, potential attacks against universities for intellectual property and research, as well as increases in malicious activity aimed at exploiting school resources for personal profit. The migration to a virtual learning environment led to an increase in threat types. While some of these attacks, such as Zoombombing and DoS/DDoS attacks, were aimed at disrupting the learning process, others were more malicious, for example, phishing campaigns and ransomware.

Despite the variety of threats facing the education industry, attack volumes remained largely consistent with 2019. In 2020, education was the fifth most targeted industry, garnering 6% of all attacks. Attack types against education were markedly different from other organizations, with the industry suffering far below average counts for web-application and application-specific attacks. Instead, the industry faced significantly higher levels of brute-force activity and coinmining.

XMRig, a coin mining malware, was the single most detected malware in education, accounting for 62% of all malware detections. This high level of cryptocurrency malware detection was unique to the education industry.

We observed attacks targeting vBulletin accounting for 18% of all attacks against the education industry, while Linux attacks accounted for 15%. Like many other organizations, ThinkPHP was also widely targeted in education, accounting for 11% of attacks on targeted products.

Targeting the education industry

Education was the fifth most commonly targeted industry during 2020, garnering 6% of all attacks. The volume and percentage of attacks against education remained mostly consistent with the previous year. Web-application attacks accounted for 24% of attacks against education while application-specific attacks accounted for 22% of attacks. Combined, these attack types accounted for 46% of attacks against education, far below the global average of 67%. Only technology had a lower count for these attack types. At 16% of all attacks, education had the highest rate of brute-force attacks of any industry analysed (the global average for brute-force attacks was 3%). Targeting against the education industry was also unique, with vBulletin and Linux being the first and second most targeted technologies, respectively. While these technologies were both widely targeted globally, education was the only industry to have these products appear in their list of the five most targeted technologies.

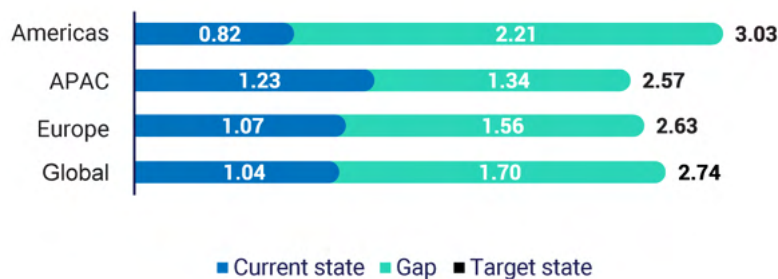


Figure 43: Education - current and target maturity levels and the gap between them

As shown in Figure 43, the education industry had an average maturity level of 1.04, a slight increase from 1.02 in 2019. Organizations globally scored highest in the Information Security Framework subcategory with an average score of 1.36 while having the lowest average score of 0.72 in the Security Vision and Strategy subcategory. Organizations within the APAC region showed the highest maturity with average scores of 1.23. Organizations in the Americas performed poorly (0.82), scoring lowest in the Security Vision and Strategy (0.60) subcategory. To improve in this area, organizations should focus on implementing managerial controls.

Top attack types	Top products targeted	Top malware variants
Web-application – 24%	vBulletin – 18%	XMRig – 62%
Application-specific – 22%	Linux – 15%	Cryptominer – 8%
Reconnaissance – 21%	ThinkPHP – 11%	Mariposa – 6%

Figure 44: Top targeting in the education industry

Spotlight on: Cryptocurrency miners

About 72% of all malware activity in education was some form of coin miner. Coin miners, also called cryptocurrency miners, are programs that generate Bitcoin, Monero, Ethereum or other cryptocurrencies. XMRig detections alone accounted for 62% of all analysed malware within education. XMRig is a coin miner that infects a user's computer to mine Monero. Cryptominer and XMR-Stak, other cryptocurrency miners that mine and process transactions for various forms of cryptocurrency, all contributed to malware detections in education.

Coin miners are popular among students who likely seek to exploit unprotected infrastructure to generate passive income. While coin miners are not inherently destructive, their presence can put a significant strain on system resources, potentially leading to machines overheating or performing poorly. The presence of coin miners can also alert threat actors to vulnerabilities in systems, leading to further, more malicious, exploitation. At the very least, if an attacker can install a coin miner in an environment, they likely have the potential to also install additional, more nefarious forms of malware.

The presence of coin miners can also alert threat actors to vulnerabilities in systems, leading to further, more malicious, exploitation.

Spotlight on: vBulletin attacks

vBulletin was the single most attacked product within education, accounting for 18% of all technology targeting. A proprietary internet forum software package, vBulletin suffered from two widely publicized vulnerabilities: CVE-2019-16759 and CVE-2020-17496. CVE-2019-16759 enabled remote command execution due to a lack of validation, while CVE-2020-17496 also allowed for remote command execution due to an incomplete fix for CVE-2019-16759. Exploitation of these vulnerabilities could allow an attacker to gain privileged access to and control over a vBulletin server, potentially leading to organizations being locked out of their own sites.

Organizations should ensure they have implemented patches and updates to fix these two vulnerabilities. If organizations in the education industry prioritized security just for vBulletin instances, they could potentially mitigate as much as 18% of the targeting currently affecting this industry.

Governance, risk and compliance (GRC)

Education GRC varies by region and country. In the US, education institutions and state and local school districts have the flexibility to adapt data privacy plans to fit their specific needs. No matter the country or region, education institutions must assess their unique risk of cyberthreats and create a data breach response policy, plan and procedure to mitigate and respond to cyberattacks. These initiatives should consider the variety of data types that the education industry holds, ranging from student health and education records to unpublished research and intellectual property.

Along with issues associated with running a business (like finances and responsible breach reporting) GRC issues in education tend to focus on three factors: student and faculty privacy (including personal information and grades); protection of educational resources like systems and applications; and privacy of potentially sensitive data associated with research projects. Educational institutions also tend to be sensitive to transparency about demographics. The various requirements create challenges when multiple requirements conflict, especially in public institutions. Effective GRC in education can be complex and requires active management.

Application security analysis

The education industry's likelihood of exposure across the OWASP Top Ten vulnerability categories is mixed. The industry has lower rates of exposure compared to the global averages in injection, sensitive data exposure and cross-site scripting vulnerabilities. However, the industry significantly underperforms in the areas of broken authentication and security misconfiguration vulnerabilities. A deeper analysis of the common causes of exposure of the underperforming versus overperforming classes reveals a potential relationship involving the use of purchased software rather than in-house development.

The education industry overperforms the global average in vulnerability classes typically associated with application code and underperforms in classes often associated with configuration and deployment of purchased software. This is further supported when we look at remediation metrics where education trails the other industries analysed, with only 41% of serious vulnerabilities reported in 2020 remediated at the time this Report was issued. Vulnerabilities related to software configuration are typically among the easiest to remediate when that software is developed and deployed in-house. However, when the software is purchased externally, receiving support and documentation for security best practices can be challenging.

Top five serious vulnerabilities	Likelihood of serious exposure
Directory indexing	16%
Insufficient transport layer protection	15%
Cross-site scripting	12%
URL redirector abuse	5%
Brute-force	4%

Figure 45: Education's likelihood of exposure to top serious vulnerabilities

Top five vulnerabilities	Likelihood of exposure
Insufficient transport layer protection	93%
Frameable resource	4%
Fingerprinting	42%
Information leakage	41%
Predictable resource location	40%

Figure 46: Education's likelihood of exposure to top five vulnerabilities

Recommendations

The following are our mitigation recommendations for the threats facing the education industry:

Mitigation	MITRE ATT&CK ID	Description
Encrypt sensitive information	M1041	Employ encryption for all sensitive information at rest in the cloud, all important data flows and on emails which contain sensitive information
Privileged account management	M1026	Manage all elements of privileged accounts, including their creation, modification, use and permissions; this includes SYSTEM and root accounts
Update software	M1051	Create a patch management process to perform regular software updates

Figure 47: Recommendations for the education industry

Technology

Technology enabled continued communication around the globe in 2020. Governments, justice systems, legal entities, business organizations and education institutions from preschool to college adapted to the new ‘get it done from home’ paradigm. This increased dependency on technological tools – software, hardware and the knowledge to make it all work. Businesses demanded more robust networking and the ability to support remote working with PCs and other devices. Consumer expectations also increased, with home-bound individuals demanding more robust bandwidth, better PCs, faster phones, sharper televisions and other entertainment technology. This heightened the demands on the technology industry and introduced greater expectations for product enhancements and supply. It increased the pressure on the technology industry to improve management of supply lines, development of new products and distribution of those products to end users. The result was an increase in technology organizations’ risk at each touchpoint along the supply chain.

Technology had the lowest rate of application-specific (23%) and web-application (15%) attacks of the industries analysed. The industry also recorded the highest rates of reconnaissance and DoS/DDoS activity. This is likely due to the increased demand placed on technology organizations and attackers taking advantage of the vectors they believed had the greatest potential to provide the desired result.

Cybercriminals used a wide variety of techniques in their attacks. They exploited vulnerabilities in online meeting software and mounted successful phishing campaigns to download malware and exfiltrate user credentials and personal information. They planted malicious software in systems, which awaited the command to do further damage to individuals or organizations. Depending upon the end goal of the crime, as well as the malware deployed, a threat actor can hold files for ransom or sell the stolen data on the dark web for monetary gain or even retribution.

Targeting the technology industry

Organizations in the technology industry are high-value targets for cybercriminals due to the sensitive data, intellectual property and trade secrets they hold on their systems. We found reconnaissance to be the most common activity directed against the technology industry, accounting for 43% of detections. Port scanning accounted for 60% of this activity. Technology was the only industry where reconnaissance was the most common hostile activity. The global average for reconnaissance activity was 20% of detections. Technology also saw the highest rate of DoS/DDoS attacks of the industries analysed, with 16% of all activity, down slightly from 25% of detections in 2019.

2020 saw GRC come to the forefront of global data regulations. This affected the technology industry, as many organizations incurred fines from the General Data Protection Regulation (GDPR) for data breaches. We also saw a trend towards implementing even more national data protection laws, with such laws going into force across the globe in countries including Brazil, Singapore, Thailand, Australia and Japan, to name a few.

According to our analysis, attacks targeting ThinkPHP accounted for 24% of all attacks against the technology industry. D-Link products were the second most popular target (20%). Overall, technology organizations stood out for having the lowest rates of application-specific and web-application attacks combined (38%), far below the global average of 67%. They also showed the highest rates of reconnaissance activity (43%) and DoS/DDoS activity (16%). However, averages varied drastically depending upon the region. In APAC, for example, application-specific and web-application attacks accounted for over 90% of attacks targeting the technology industry. The variance in these numbers suggests that the techniques attackers use may depend more on the targeted organization than attackers’ focus on specific, industry-wide techniques.

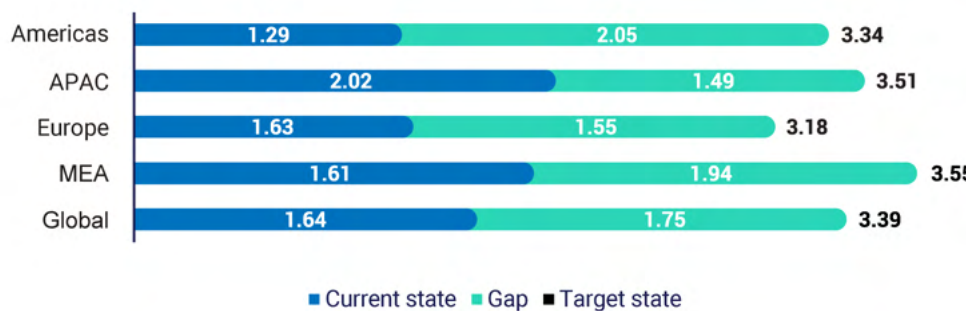


Figure 48: Technology - current and target maturity levels and the gap between them

Figure 48 shows the technology industry's average baseline maturity was 1.64 in 2020, consistent with their score in 2019. Organizations in APAC led with an average maturity score of 2.02, while those in the Americas had the lowest maturity scores in the industry. Technology's most mature subcategory in the Americas was a score of 1.49 for Security Vision and Strategy. Technology in the Americas performed poorly in the Logical Security Architecture (1.20) and Risk Management (1.09) subcategories. Focusing on risk management and improved technical controls must be a priority for organizations seeking to excel in these areas.

Top attack types	Top products targeted	Top malware variants
Reconnaissance activity – 43%	ThinkPHP - 24%	NetWalker – 71%
Application-specific – 23%	D-Link product - 20%	Conficker – 7%
Dos/DDoS – 16%	Apache Struts - 10%	Mirai – 4%

Figure 49: Top targeting in the technology industry

Spotlight on: NetWalker

NetWalker was the most common malware variant in the technology industry, accounting for 71% of all detected malware activity. NetWalker is a fileless ransomware which is written in PowerShell and executes directly in a targeted machine's memory. In 2020, it targeted Windows-based environments and operated using a ransomware-as-a-service model. Threat actors were highly active in leveraging this malware against COVID-19 virus research and vaccine manufacturing. Globally, NetWalker was the fifth most common malware we detected in 2020.

In January 2021, the US Department of Justice launched a coordinated global law enforcement action to disrupt NetWalker ransomware campaigns. While this successfully disrupted NetWalker campaigns, organizations should still take steps to mitigate against such attacks, for example, by restricting the use of PowerShell, employing up-to-date antivirus/antimalware and using application controls to prevent unauthorized code and application execution.

Spotlight on: DoS/DDoS attack activity

Of all the industries analysed for this Report, technology showed the highest rate of DoS/DDoS activity, at 16%. (In 2019, technology also showed the highest rate of DoS/DDoS attacks, at 25%.) Of these DoS/DDoS attacks, 88% were flood attacks. For all other industries analysed, 92% of DoS/DDoS attacks were application-based. At 9% of detected attacks, education was the only other industry analysed that experienced more than 4% of its detected attack types coming from DoS/DDoS activity. DoS/DDoS activity can result in a targeted system or service being unable to respond to legitimate requests or crashing, thus becoming totally unavailable.

Organizations can mitigate the impact of DoS and DDoS activity by employing services provided by Content Delivery Networks (CDNs) and DoS/DDoS mitigation service providers. These services will filter suspicious attack traffic upstream from services, with reduced or no impact on the target of the attack. Organizations can also dynamically filter attack traffic by blocking attack source addresses, closing targeted ports and blocking protocols being employed in the attack.

Governance, risk and compliance (GRC)

GRC came to the forefront of global data management regulations in 2020. The year marked the second year of existence of the GDPR, which took effect in the European Union (EU) on May 25, 2018. The GDPR brought about changes in managing the collection and use of an individual's information. In addition to data protection and risk mitigation, compliance with the GDPR can help to build trust between clients and organizations, thus enhancing the organization's reputation. These regulations apply to organizations who are based within the EU as well as those not based within the EU but who collect and use the personal data of persons living in the EU.

Many countries have also enacted rules and guidelines for data protection that attach fines for data breaches, as seen in the Facebook, Google and WhatsApp GDPR fines. Greece, Portugal and Slovenia have yet to enact their national data protection laws following the implementation of the GDPR. Brazil's General Data Protection Law (LGPD), California's California Consumer Privacy Act (CCPA), Singapore's Cybersecurity Bill, Thailand's Personal Data Protection Act, the Australian Privacy Act, and Japan's Personal Information Protection Commission (PPC) and Act on the Protection of Personal Information (APPI) all regulate how data is protected, managed and used within each country.

The global trend towards enhanced data protection continues to hold significance. Canada and Australia are considering new data protection regulations and India's legislature is set to vote on its Personal Data Protection Bill. The US states of Nevada, New York, Texas and Washington are also considering enacting data protection laws.

Application security analysis

The technology industry's likelihood of exposure across nearly all vulnerability classes is still among the highest of all the industries analysed and is significantly higher than global averages for all the OWASP Top Ten vulnerability categories. Organizations should pay specific attention to this industry's likelihood of exposure to any severity of cross-site scripting (24%), which is over double the global average (12%), and its exposure to SQL injection (3%), which is more than three times the global SQL injection average (1%).

These vulnerability classes have been 'headline' application security vulnerabilities for over two decades. The technology industry's struggle to achieve average performance in this area may represent an overall lack of attention to implementing robust application security processes, in a rush to deliver new software at an ever-increasing pace. A more rapid pace of software delivery could allow for decreased time-to-fix for detected exposures, but the data does not support this. The technology industry's performance in both time-to-fix (71 days overall; 59 days for serious vulnerabilities) and remediation rate (31% overall; 44% for serious vulnerabilities) is average at best.

Top five serious vulnerabilities	Likelihood of serious exposure
Cross-site scripting	22%
Insufficient authorization	6%
Insufficient transport layer protection	6%
URL redirector abuse	6%
Cross-site request forgery	5%

Figure 50: Technology's likelihood of exposure to top serious vulnerabilities

Top five vulnerabilities	Likelihood of exposure
Insufficient transport layer protection	60%
Information leakage	53%
Frameable resource	30%
Insufficient authorization	28%
Fingerprinting	24%

Figure 51: Technology's likelihood of exposure to top five vulnerabilities

Recommendations

The following are our mitigation recommendations for the threats facing the technology industry:


Mitigation	MITRE ATT&CK ID	Description
Execution prevention	M1038	Prevent code execution on a system via script blocking or application control
Antivirus/antimalware	M1049	Use heuristic-based malware detection which has updated virus definitions; create custom signatures for malware as needed
Filter network traffic	M1037	Use CDNs and DoS/DDoS mitigation providers to filter upstream traffic; dynamically filter attack traffic by blocking attack source addresses, closing targeted ports and blocking protocols being employed in the attack; enable SYN cookies to defend against SYN flood attacks

Figure 52: Recommendations for the technology industry

Managing malware threats

The speed with which malware can change has always posed a problem for cybersecurity. Malicious actors' ability to adapt and evolve their tactics, tools and procedures means that defenders must adapt and evolve rapidly, too. As a result, most organizations should rely on third-party cybersecurity providers to keep up with the evolving threats – they should depend on those entities whose business depends on keeping up, rather than trying to keep up themselves.

J. Michael Daniel, President & CEO
Cyber Threat Alliance

The background of the slide is an abstract, artistic composition. It features several concentric, slightly blurred circles in shades of brown, orange, and dark blue, creating a tunnel-like or lens-like effect. Scattered throughout the scene are numerous small, out-of-focus light spots in various colors, including yellow, orange, red, blue, and green, which resemble bokeh or distant stars. The overall lighting is soft and atmospheric, with a dark, moody palette.

Malware and threats – research and observations

As with previous years' Reports, the NTT 2021 Global Threat Intelligence Report covers a variety of different threats that organizations were challenged to manage during the last year. Notably, Trickbot, Emotet and APT41 played a large part in conversations related to threats across multiple industries.

Trickbot

Trickbot – also known as Trickster, TheTrick and TrickLoader – is a modular banking Trojan first identified in 2016. Based on similarities in operational tactics, web injects and code similarities, Trickbot may be a derivative of the Dyre malware. It's highly adaptable due to frequent updates via plugins which are loaded onto infected hosts. Trickbot is operated by the group Wizard Spider (also known as TA505). These operators are associated with the groups Grim Spider and Lunar Spider, which operate Ryuk ransomware and the IcedID Trojan respectively. Trickbot infections can function as a loader for these two malware families.

Plugin functionality includes infostealing, lateral movement and network abuse capabilities. These functionalities allow Trickbot to perform actions such as harvesting passwords from browsers, email clients and a variety of applications; modifying network traffic; performing Man-in-the-Browser attacks; brute-forcing RDP; and self-propagation. Trickbot has a module that leverages the EternalBlue exploit, allowing the malware to spread inside a local network via Server Message Block (SMB).

While Trickbot's targeting often appears indiscriminate, we observed Trickbot largely targeting the finance and healthcare industries during 2020. This targeting accounted for 6% and 3% of total malware variant detections, respectively. Although researchers observed Trickbot being distributed via malspam campaigns, it was primarily deployed as a secondary payload after an Emotet infection.

In October 2020, our Global Threat Intelligence Center (GTIC) collaborated with Microsoft's Digital Crimes Unit, ESET, Lumen's Black Lotus Labs and others to disrupt the Trickbot command-and-control (C2) infrastructure. NTT has been tracking Trickbot for several years through coordination between GTIC, NTT's Security Operations Centers and NTT Secure Platform Labs. With access to our global internet backbone traffic, and in coordination with applied threat intelligence, machine learning and advanced analytics, our analysts discovered Trickbot infrastructure communications. We shared this information, which led to the disruption and taking offline of much of Trickbot's C2 infrastructure on 12 October 2020.

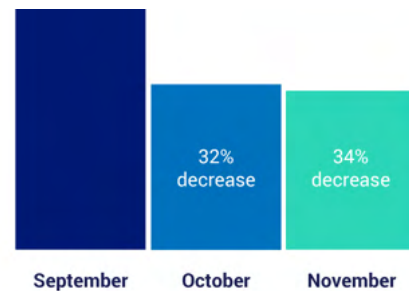


Figure 53: Trickbot activity levels before and after disruption

As illustrated in Figure 52, the disruption of Trickbot's infrastructure had a substantial effect on the malware's activity. Compared to a baseline level of activity in September, Trickbot's activity fell by 32% in October and by 34% in November. While the disruption significantly affected Trickbot, its operators have since released two new versions of the malware which contain updates to the obfuscation plugin and how the malware's C2 infrastructure operates. The new infrastructure now uses .bazar domains to help prevent takedowns. We continue to track Trickbot to proactively defend against this threat.

Emotet

Emotet – also known as Geodo and Heodo – is a modular banking Trojan first identified in 2014. While Emotet was originally aimed at stealing banking credentials, the malware evolved over time to include botnet functionality. Emotet was operated by the group Mummy Spider (also known as TA542 and Gold Crestwood). This group rose to prominence in the cybercriminal world as they rented access to the Emotet infrastructure to other cybercriminal groups in malware-as-a-service and infrastructure-as-a-service models. While access to Emotet itself was limited, Mummy Spider sold access to infected machines within the Emotet botnet.

Emotet was notorious as the first stage of infection for the Trickbot banking Trojan infection chain, which included Ryuk ransomware infections. Emotet also delivered other third-party payloads, such as the Qakbot Trojan and Gootkit. Emotet had various modules which included capabilities such as stealing credentials from web browsers and email clients. It also had a spam module to facilitate the distribution of the Emotet botnet, an email harvesting module and a spreader module which allowed for spread throughout currently logged-on network resources, as well as brute-force attack attempts on protected resources.

Emotet primarily spread through spam emails containing malicious links or attachments containing malicious macros. Researchers observed loaders in the wild distributing Emotet in November 2020. Due to its varied payloads, number of interested renters and wide distribution, Emotet has been one of the most prolific malware families over the past five years. It targets indiscriminately and has affected individuals, organizations and governments around the world.

According to our observations, in 2020, Emotet was in the top 10 most detected malware for four of the industries analysed – healthcare (9% of malware detections), finance (8%), manufacturing (4%) and technology (1%). Emotet was the most commonly detected Trojan globally in the finance, manufacturing and healthcare industries. Overall, Emotet was the fourth most detected malware globally, accounting for 5% of all malware detections. It accounted for 39% of all Trojan and banking Trojan detections.

On 27 January 2021, Europol announced a coordinated global law enforcement and judicial authority action against the Emotet botnet. Through collaborative international action, investigators took control of the Emotet botnet infrastructure by taking control of hundreds of servers located around the world. This action severed the connection between victims' machines and the malware operators. The disruption of the Emotet botnet will have a significant impact on the cybercrime ecosystem. However, attackers will likely attempt to find other distribution networks to replace Emotet's role.

Emotet activity by top 10 industries	Percentage of total Emotet detections
Telecommunications	29%
Healthcare	18%
Manufacturing	14%
Education	11%
Public	9%
Finance	5%
Transport and distribution	3%
Retail	3%
Insurance	2%
Government	1%

Figure 54: Percentage of Emotet detections in the top 10 affected industries

¹ <https://content.fireeye.com/apt-41/rpt-apt41>

Collaboration can impact cybercrime

An increasing professionalization of cybercriminal groups, as well as crime facilitating factors such as anonymization services and dark web marketplaces, pose significant challenges to law enforcement in countering these threats. The recent disruptions of Emotet and Trickbot, however, show how that they can be tackled effectively by working closely together. These successes also show that law enforcement is catching up by building a closely-knit, global network, dedicated to bringing cybercriminal perpetrators to justice.

At the same time, these operations may take a significant amount of time – time, during which organisations need to be able to protect themselves. A high level of cybersecurity and functioning information-sharing networks are critical to managing these threats effectively, as is a holistic approach which does not only focus on prevention, i.e., keeping the bad guys outside of the networks, but also on detection and incident response to ensure an organisation knows how to respond when criminals do manage to enter their networks.

Edvardas Šileris, Head of European Cybercrime Centre (EC3), Europol

APT41: A threat actor with global reach

In September 2020, the US Department of Justice indicted five Chinese hackers believed to be members of the threat actor group APT41. According to the indictment, the defendants committed cyberattacks against more than 100 organizations and individuals, including those in the US, Taiwan and Japan. Three of those indicted are believed to be employees of a security vendor in China. The FBI later released a Liaison Alert System (FLASH) report containing technical information on APT41, including a list of the group's TTPs. The indictment and FLASH report explicitly linked past attack campaigns and tactics, techniques and procedures (TTPs) to APT41. Based on this publicly available intelligence, we can summarize the characteristics and advanced attack techniques of APT41 with reference to other threat actors.

Observed APT41 activities date back to at least 2012. According to MITRE ATT&CK, APT41 is a group that carries out both state-sponsored espionage activity and financially motivated activity. Researchers first published a report¹ containing details about APT41. APT41 was initially believed to be a financially motivated group that focused especially on the video game industry. However, it later became known that APT41 also conducted cyber-espionage attacks like other state-sponsored groups. APT41's espionage attacks targeted organizations in the healthcare, high technology, education, media, travel and communications industries. Specifically, since 2017, APT41 has consistently targeted telecommunications organizations of various sizes worldwide in espionage campaigns.

APT41 is reported to have a close relationship with other threat actors, such as Winnti, BARIUM and Chimera. Although these groups are listed separately in the MITRE ATT&CK Groups, they partially overlap in terms of their TTPs. Some security vendors regard Winnti and BARIUM as aliases for APT41. These groups share a commonality of heavily targeting the gaming industry. A strong relationship between Chimera and Winnti has also been suggested. In particular, the FBI noted in the FLASH report that APT41 deployed a 'Skeleton Key' attack, which had been considered a distinctive Chimera technique.

The following section summarizes TTPs which were allegedly used in past APT41 and related actor attacks.

Initial Access [TA0001]

Supply Chain Compromise: Compromise Software Supply Chain [T1195.002] – APT41 has launched several supply-chain attacks that exploit software update downloads from compromised organizations. In July 2017, APT41 inserted malicious code into a software update package managed by South Korea's Netsarang Computer, signing the package with a legitimate Netsarang certificate. In June 2018, it compromised a utility software used to update ASUS computers, forcing devices with specific MAC addresses to install unauthorized updates².

Phishing: Spearphishing Attachment [T1566.001] – Between July and August 2016, APT41 sent spearphishing emails to Hong Kong news organizations known for pro-democracy articles. In addition to using breaking news as a lure, the lure themes were also selected to cause a significant psychological impact on individuals by using the fear of pandemics, as the region had experienced infectious diseases in the past. The decoy emails contained malicious shortcut (.lnk) files with hidden payloads, compiled HTML help (.chm) files and Microsoft Office documents with macros and exploits.

Exploit Public-Facing Application [T1190] – In early 2020, attackers exploited vulnerabilities in the Citrix Application Delivery Controller and Cisco routers (CVE-2019-19781, CVE-2019-1653, CVE-2019-1652), as well as a zero-day vulnerability in Zoho ManageEngine (CVE-2020-10189), through publicly opened services³.

Execution [TA0002]

Scheduled Task [T1053] – In May 2020, APT41 conducted a ransomware attack that targeted Taiwanese organizations. The attack altered a domain controller's Group Policy Object (GPO) which forced domain users to download and run ransomware on a task schedule. Between 2018 and 2019, Chimera used Cobalt Strike with 'schtasks' for lateral movement in a campaign targeting Taiwanese chipmakers.

Persistence [TA0003]

Create or Modify System Process: Windows Service [T1543.003] – In a November 2019 campaign targeting universities in Hong Kong⁴, the Winnti group created a service that mimicked legitimate service names used in Microsoft.NET optimization. In March 2020, Winnti created a service called 'Storage Sync Service' and registered the Cobalt Strike beacon loader 'storesyncsvc.dll' in the campaign which exploited the Zoho ManageEngine zero-day vulnerability.

Registry Run Keys/Startup Folder [T1547.0001] – APT41 reportedly used the malware 'POISONPLUG', which is a highly obfuscated modular backdoor with plug-in functionality. This malware has functions for registry or service persistence, self-deletion, plug-in execution and network connection transfer.

Defense Evasion [TA0005]

Deobfuscate/Decode Files or Information [T1140] – Obfuscated Files or Information [T1027] – APT41 uses a wide variety of packers to make detection by security products and analysis by researchers difficult. ESET reported the use of Winnti-specific custom packers with RC4. In early 2019, ESET also discovered that the payload of the Microsoft SQL Server backdoor 'skip-2.0' was encrypted with RC5⁵. In addition, several samples that FireEye tracked as 'DEADEYE' also used RC5 with a unique string to extract a key. In the campaign against universities in Hong Kong, the ShadowPad shellcode was XOR encoded and used false conditional jumps to prevent disassembly.

APT41 also used Meterpreter downloaders protected by VMProtect in the Zoho ManageEngine zero-day campaign. VMProtect has been used extensively in the past, especially with the PortReuse, ShadowPad, and skip-2.0 launchers of the Winnti group. Attackers also used ConfuserEx in the ransomware attack targeting Taiwanese organizations.

² <https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/>

³ <https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html>

⁴ <https://www.welivesecurity.com/2020/01/31/winnti-group-targeting-universities-hong-kong/>

⁵ <https://www.welivesecurity.com/2019/10/21/winnti-group-skip2-0-microsoft-sql-server-backdoor/>

Hijack Execution Flow: DLL Side-Loading [T1574.002] – In the campaign against universities in Hong Kong, the ShadowPad launcher was likely run by DLL sideloading the malicious file, which was installed as printing and scanning software.

Subvert Trust Controls: Code Signing [T1553.002] – In the supply chain attacks, APT41 used a legitimate digital certificate to sign the backdoor packages.

Automated Collection [T1119] – Other security firms reported that APT41 deployed a tool named ‘MESSAGETAP’ to monitor and save SMS traffic from specific phone numbers, IMSI numbers and keywords for subsequent theft⁶.

Credential Access [TA0006]

Modify Authentication Process: Domain Controller Authentication [T1556.001] – Chimera used ‘SkeletonKeyInjector’ malware which allowed attackers to log into domain controllers without using valid account credentials. The malware embedded Skeleton Keys in the memory of the lsass.exe process. This approach allowed legitimate users to log into the system with their original passwords since the embedded Skeleton Key is compared for verification when authentication fails due to incorrect credential input. This makes it difficult for the hijacked user to notice the Skeleton Key attack. Due to the nature of the domain controller’s role, the server is less likely to reboot. As the memory containing the Skeleton Key is not cleared, actors are more likely to be able to bypass authentication for a long time.

Command and Control [TA0011]

Dynamic Resolution: Domain Generation Algorithms [T1568.002] – The backdoors in NetSarang’s software package were designed to dynamically change the domain of the C2 server. This makes it difficult for defenders to block and analyse C2 domains.

Web Service: Dead Drop Resolver [T1102.001] – Attackers were observed in prior campaigns using legitimate websites such as GitHub, Pastebin and Microsoft TechNet for C2 servers to avoid detections. The encoded command string has also reportedly been stored on a legitimate web site to prevent C2 traffic from being detected.

Summary

The TTPs of APT41 characterize its advanced and diversified attack techniques. Overall, the group leverages multiple means of infiltrating its targets, such as via software supply chains, spearphishing emails and leveraging exploits that target vulnerabilities in public-facing services. Additionally, the group uses numerous software packing techniques to evade detection, some of which they leverage heavily. However, there’s no one technique the group relies upon. APT41 attempts to hide the existence of malware it deploys by using legitimate file and service names for obfuscation. The group also uses Domain Generation Algorithms and dead drop resolvers to prevent tracking and C2 detection. Additionally, APT41 takes advantage of compromised target environments to craft an effective attack strategy. This includes elements such as distributing software packages signed with stolen certificates or using Group Policy Objects to execute task schedules in a domain environment.

Overall, the group leverages multiple means of infiltrating its targets, such as via software supply chains, spearphishing emails and leveraging exploits that target vulnerabilities in public-facing services.

⁶ <https://www.fireeye.com/blog/threat-research/2019/10/messagetap-who-is-reading-your-text-messages.html>

Best practices

This section gave three examples of threats facing organizations – the Trickbot and Emotet Trojans, as well as campaigns from the threat actor group APT41. While each of these three represent unique threats to organizations and industries, several security best practices will help mitigate any hostile activities. Mitigating Emotet, Trickbot, APT41 and other sophisticated threats requires layered and proactive security controls. Organizations should employ the following mitigations:

Mitigation	MITRE ATT&CK ID	Description
Antivirus/ antimalware	M1049	Keep antivirus and antimalware up to date with the latest signatures and heuristics to detect infection
User training	M1017	Train users to be aware of potential behaviors which could lead to Trickbot infection; train users on social engineering techniques and how to spot phishing emails
Audit	M1047	Perform audits or scans to identify potential weaknesses throughout an organization, including in systems, permissions, non-secure software and non-secure configurations; perform system scans to look for unauthorized use of archival utilities
Vulnerability scanning	M1016	Perform regular scans to find and remediate software vulnerabilities which may be exploitable
Behavior prevention on endpoint	M1040	Establish measures to detect suspicious behavior and minimize damage through the introduction of User Entity and Behavior Analytics (UEBA) and Endpoint Detection and Response (EDR) products
Network intrusion prevention	M1031	Use intrusion detection signatures at network boundaries to block access to known C2s

Figure 55: Recommended mitigations against Trickbot, Emotet and APT41

USERNAME AND PASSWORD

Cyber-resiliency and agility

In last year's Report, we discussed the concepts of 'cyber-resiliency' and 'secure by design', as well as how to achieve both concepts.

- Cyber-resiliency refers to an organization's ability to continuously deliver products and services despite normal operations being impacted by cyber-related events.
- Secure by design refers to organizations being cybersecurity-aware at all levels of business.
- For organizations to master these concepts, security must be considered as a core business function and treated as such.

Based on the results of our research, 47% of organizations said that ensuring security is designed into their processes and technology is a key focus for the next 18 months.

SYST

UNAUTHORIZED ACCESS

Maintaining business continuity

Cyber-resilience is becoming increasingly important as attack surfaces grow and criminals continue finding new ways to carry out their malicious activities. For most, if not all, organisations, it is simply a matter of when rather than ‘if’ they are breached – recent high-profile cases have shown that every organisation needs to be fully prepared for when a cyberattack hits them. This is precisely why the emphasis needs to be on a holistic approach to cybersecurity, both within an organisation as well as within the sector and the supply chain. Ensuring that an organisation is cyber-resilient is critical in reducing the cost of the attack, keeping information safe and returning to business as usual as soon as possible with limited interruption.

Edvardas Šileris, Head of European Cybercrime Centre (EC3), Europol

Organizations seeking to become cyber-resilient and secure by design must ensure that they consider security best practices and build them into policies, procedures, infrastructure and applications. They must identify what data and capabilities are essential, what systems are involved in supporting this data and capabilities as well as how the organization and its clients will use the data and services.

With these policies in place and information in hand, an organization can start to define a comprehensive security program. This should include items such as components of network design, application development and deployment, development controls, policies, processes, and technologies. While this process can be difficult, organizations can leverage frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, to reduce complexity while building the components of a secure architecture.

Such secure architecture will become more important as threats to organizations continue to multiply and become more sophisticated. In our research, we asked organizations which threats they felt prepared/least prepared for, with the lowest levels of preparedness (76% of organizations) being for large-scale organized cybercrime.

Concerns about meeting compliance obligations, and addressing insider threats, cross-site scripting and threats to internet of things devices and operational technology were also identified in the top five areas for which organizations globally were least prepared.

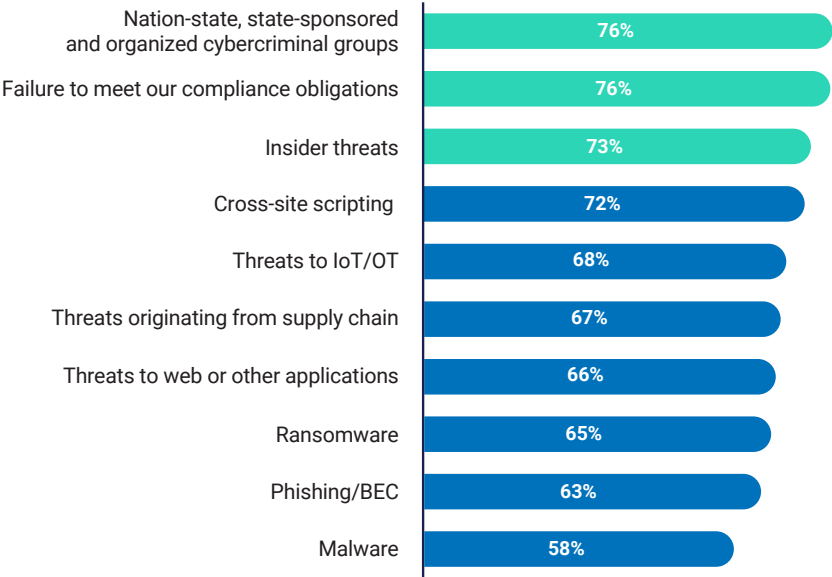



Figure 56: Threats that organizations are not prepared for

Organizations seeking to become cyber-resilient and secure by design must ensure that they consider security best practices and build them into policies, procedures, infrastructure and applications



Trust, the supply chain and how it affects business

Security, like almost all activities in which we engage socially, is fundamentally based on trust. Trust is not a new concept to the cybersecurity field, but the principle must be reinforced as it applies directly to business enablement and asset protection. We cannot rely on our instincts as a sole factor in trust. Events that have unfolded since the beginning of COVID-19 have reinforced the need for trust-based security.

Trust and security in business and client experience is no longer an option but a fundamental requirement. In this section of our Report, we discuss trust as it applies to cybersecurity, business relationships, technologies and broader business objectives.

After reading this Report, we recommend that you evaluate your own capabilities. Key considerations to ask:

- Do I have proper controls in place to manage trust relationships from a technology perspective?
- Have I included the topics of trust, resiliency and confidence in my implemented solutions?
- Has my organization implemented controls to manage, detect and respond to failures related to trust relationships?

Not trusting anyone or any system is a good starting place. Many organizations spend large amounts of money on internal identity access management controls to protect their assets. Why would you allow partners, vendors and technologies that have not been evaluated on trust to touch your data without authentication, authorization and access controls?

Now for the caveat...there's no such thing as 100% trust. This is where some of the concepts of risk management play a vital role. Ensuring that appropriate controls are implemented to manage risk can help your organization be more resilient when trust fails. This is a large part of why businesses use contracts. Contracts help to hold parties accountable and establish an initial understanding of the relationship and its expectations.

Business relationships

Relationships drive our ability to leverage our capabilities and collaborate with other organizations. This in turn supports the advancement of meeting tactical and strategic goals. There are many relationships businesses strive to maintain with trust and security in mind, such as:

- **Supply chain** – vendor management; software; hardware; goods and services
- **Facilities** – maintenance, service and custodial
- **Outsourced support** – developers and staff augmentation
- **Strategic business partnerships** – business-to-business and resellers

The skills of a trusted partner are invaluable to ensure optimal and secure deployment of services and solutions

89%

of cybersecurity professionals agree that a trusted technology partner is a key foundation for technology strategies.

Technologies

The technologies we implement help businesses meet their objectives. The notion that trust is something that must be evaluated, tested, earned and reevaluated becomes a larger challenge when dealing with software and hardware-based solutions.

In an 'there's an app for that' era, it becomes easy to implement solutions before proper vetting. The problem with software and hardware is that each 'solution' you bolt onto your organization creates more risk exposure. Simply put, the more you add the more you need to trust. Remember, you cannot trust anything 100%. Inherently, risk increases, especially in a world where 'version 1.0' of anything is usually riddled with critical vulnerabilities.

It's vital to focus on some of the key concepts supporting trust and technology. A good place to start is ensuring your organization designs and implements security controls supporting cyber-resilience and agility. Security controls must provide an adequate balance of security while being flexible enough to manage blended threats.

Business, competitive and threat intelligence are also key to an organization's success. But before we can collect, analyse, produce and share business and cyberthreat intelligence, it must be trusted and assigned confidence. There's far too much 'junk data' available on the internet to trust its value blindly. Organizations mustn't trust something because they believe it's 'intelligence'. Even well-curated intelligence should be reviewed until its value and accuracy has been properly vetted.

Trusted parties?

Trust has several different meanings in the cybersecurity context. In particular, personal and organizational trust differs from technical trust. Personal trust involves the relationships between people, and the level of trust between individuals drives how they interact with each other, how much risk they are willing with that person, and how much they will rely on that person. Organizational trust involves how an entity is perceived from the outside – does the organization typically live up to its commitments, do its products function as advertised, can it be relied upon to protect information. Technical trust is allowing computers to interact without authentication. Personal and organizational trust are necessary components for a functional ecosystem; technical trust is not. Therefore, since technical trust is easy to abuse, organizations should move away from technical trust and embrace zero-trust architectures, featuring segmentation and regular authentication.

J. Michael Daniel, President & CEO
Cyber Threat Alliance

Frameworks

In 2020, NIST unveiled SP 800-207 as its final version of the Zero Trust Architecture (ZTA) special publication. Given the current state of the COVID-19 pandemic and the proliferation of remote workers, bring your own device policies, and the deteriorating network edge, this publication provides a timely framework that public and private sectors can leverage to better manage risk in the enterprise. According to NIST, 'Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms which move defenses from static, network-based perimeters to focus on users, assets and resources.' Several guides are provided within the document which support different architectures.

A key component to the ZT approach is shifting the focus more towards protecting resources and assets as opposed to protecting networked segments. For ZT to be effective, organizations must have a strong understanding of their assets and the workflows supporting business operations. As many organizations don't have a strong grasp of these requirements, it may take time, money and dedicated resources with experience cataloging these areas to be successful.

With a ZTA, the focus is more on authentication and authorization of access to assets as opposed to trusting access from seemingly trusted network or physical locations. Organizations must ensure that the implementation of trust controls and policies supports the objectives of the entire organization.

Examples of NTT trust relationships

We're constantly maturing relationships with our trusted partners, vendors and intelligence providers. In 2020, we joined Charter of Trust⁷ as part of our global cybersecurity initiatives. We've entered into a joint agreement to ensure cybersecurity plays a key part in an open and fair digital future. NTT CISO, Shinichi Yokohama, stated 'We believe in contributing to resiliency build-up of the global cybersecurity and join the "shapers" community rather than waiting for the industry to be shaped.' This further extends the precedent that others involved in the agreement are bound by regulations. This fosters trust in cybersecurity.

We also maintain trusted relationships with well-known industry intelligence organizations, including the Cyber Threat Alliance, Europol and the National Cyber-Forensics & Training Alliance (NCFTA). These relationships have been mutually beneficial and not only support our intelligence goals, but also help us accelerate towards our business objectives while benefiting our clients directly.

Trust recommendations

Managing trust and implementing controls to maximize the enforcement of trust-based ideologies is vital. To achieve this, some foundational concepts must be well planned and executed:

- Identify and map risks to critical assets and enforce policy controls within the environment.
- Ensure your organization implements solutions that provide enhanced visibility across your entire enterprise, including logging and reporting.
- Embrace the applied intelligence approach and ensure proactive defense and adaptive response capabilities are well-architected and implemented.
- Measure your security capabilities and adjust your priorities based on insight from reporting, metrics and validation processes.

A Zero Trust model is not a new concept in cybersecurity, although recent events have reinforced how critical it is. Organizations globally need to navigate the increasing challenges they face in dealing with privacy, regulations and governance and compliance. This topic is addressed in our next section.

⁷ <https://csrc.nist.gov/publications/detail/sp/800-207/final>

⁸ <https://csrc.nist.gov/publications/detail/sp/800-207/final>

⁹ <https://hello.global.ntt/en-us/newsroom/ntt-joins-charter-of-trust>

How do we fulfill a 'Zero Trust' security approach for our clients?

Our solutions blend industry-leading security technologies to protect your network, cloud and mobile devices. Our threat intelligence is unsurpassed and will assist in preventing, detecting and responding to cyberthreats without hindering innovation.

We believe cybersecurity underpins what a business is trying to achieve. With cybersecurity at the core of our clients' strategies and embedded into digital programs, we help create a digital business that's secure by design.

NTT selects the appropriate security controls and technologies and also builds, implements and optimizes cross-technology architectures (across the network, data center, cloud, workplace and applications) which support the client's posture.

Lastly, we help to monitor, manage, support and optimize our clients' security posture through our Managed Security Services. This addresses potential skills gaps and helps organizations be more agile and responsive to the changing threat landscape via our threat intelligence capabilities, while delivering effective business outcomes.



Privacy, governance, risk and compliance

2020 was an interesting year for data privacy and protection as the world reacted to a global pandemic and it's one of the top business focuses for cybersecurity professionals in the next 18 months, according to our research. We observed fundamental changes in the way both the private and public sectors responded to COVID-19. This is especially true from a governance, risk and compliance (GRC) perspective, particularly with respect to both data privacy and protection.

#1
focus

GRC and data privacy are ranked as the top focus area for the next 18 months by cybersecurity professionals

95%

of organizations struggle to keep up with their compliance obligations

Source: NTT 2020 Hybrid Cloud Report

2020 – a year of privacy and protection in the ‘new normal’

Responding to the pandemic required a delicate balance of privacy and health interests, on a global scale. While regulators issued guidance calling for data protection by design, organizations needed to truly understand, assess and manage privacy risks to individuals associated with test, track and trace activities. Both private and public sectors had to make these decisions, often in the face of increasing pressure to respond, typically found in favour of privacy-eroding strategies to ‘flatten the curve’.

These strategies increased the ability of those in the private and public sectors to closely monitor the daily interactions, activities and symptoms of individuals through the introduction of dedicated contact tracing services and apps. In addition, all businesses, from the local grocer to large corporations faced new challenges not related to normal operations. These businesses were required to implement protocols to test and record the symptoms of patrons to their stores and their employees. This resulted in the unprecedented collection of health information. It also resulted in new rules regarding the management and reporting of this information. All of this from businesses which otherwise had few practices in place to ensure the proper handling and care of the data.

From the boardroom (and the classroom) to the living room

Lockdowns played a role in changing the relationship between employers and their employees by accelerating digitalization and remote working. Employers needed to consider the impact on employees and their families when work takes place in the living room. But working from home is more than a privacy issue. It has important implications for cybersecurity and business resilience as well. 2020 saw a rise in opportunistic cybercriminals using vulnerabilities introduced through increased digitalization and work-from-home arrangements, and we can expect more of the same in the coming year. Organizations are trying to adapt to the ‘new normal’ of mobility and working from home. In doing so, they need to ensure they’re looking out for their employees’ best interests, yet still using effective tools to protect their information assets and continuity of operations.

Employees aren’t the only individuals impacted by the evolving landscape. How organizations interact with clients has also changed. Organizations must be able to support clients as they move from ‘brick and mortar’ to the virtual store. They must leverage ‘behavioral excess’ online to create client profiles, predict client behavior and direct their promotional and advertising efforts. While client profiling may have benefits in delivering more personalized content and products to individuals, it also has its drawbacks. Organizations must ensure they understand the impact these activities may have on individuals and that appropriate measures are taken to act transparently and avoid any unforeseen bias.

The education industry felt the effects of COVID-19 as classes moved online. The move of employees and clients into the virtual workplace and store has changed the way we do business. Moving children online has significant consequences for data privacy and protection. Children are some of our most vulnerable members of society, and educators and organizations delivering online services to them need to ensure they apply extra diligence when offering services to children. These organizations can consider additional measures such as obtaining consent from parents for processing children’s data, educating parents and children about the dangers facing children online and implementing measures which can protect children and their families. Such measures include:

- making sure privacy notices are designed with children in mind and are clear and easy to understand
- putting in place additional safeguards to protect children against unscrupulous third parties and predators, inappropriate advertising and direct marketing as well as protecting children against inappropriate content and images

Data transfer protection and data localization

The second part of 2020 was dominated by the ongoing fallout following the Schrems II decision issued in July. This decision invalidated the EU-US Privacy Shield and placed additional obligations on organizations transferring personal data from the EU to third countries.

This is the second time the Court of Justice European Union has invalidated the agreed framework for the cross-border transfer of personal data between the EU and the US following the cancellation of the Safe Harbour regime in 2015. The outcomes of this decision illustrate ongoing concerns around the level of protection afforded to EU residents when their personal data is processed in the US and possibly subject to government surveillance and interception. But the decision extends far beyond EU-US transfers and will have a significant impact on any transfers outside of the EU.

The European Data Protection Supervisor (EDPS) and European Data Protection Board (EDPB)

issued further strategies and guidance following the Schrems II decision.

For multinationals and organizations that procure the services of international or foreign businesses, the decision is a game changer. It shifts the burden of interpreting and assessing the risks in third countries to organizations. This was a role previously performed by the European Commission through adequacy decisions. It also requires organizations have a comprehensive view of their data processing activities and locations, as well as those of their third parties who process personal data on their behalf.

The European Data Protection Supervisor (EDPS) and European Data Protection Board (EDPB) issued further strategies and guidance following the Schrems II decision. This guidance has received mixed reviews from the data protection community. The guidelines highlight some key trends for the future of cross-border transfers and will certainly keep privacy professionals busy implementing their recommendations.

Data localization strategies are rising on the agenda as new laws and regulations place increasing obligations, restrictions or limitations on the ability to transfer personal data to other countries. The recent strategy document shared by the EDPS highlights the preference for data localization within the EU. EDPB guidance illustrates the increasing burden placed on organizations to demonstrate sufficient safeguards when transferring personal data outside of the EU. However, the EU isn't alone. India's upcoming Personal Data Protection Bill places specific obligations on organizations to maintain local copies of personal information; Brazil's General Data Protection Law and South Africa's Protection of Personal Information Act (POPIA) demonstrate the increasing preference for legislatures to require that specific safeguards be in place for cross-border transfers of personal data.

Brexit continues to cause debate as to whether the UK will obtain an adequacy decision once it's exited the EU. Failure to obtain an adequacy decision will mean that the UK will be treated as a third country and organizations sharing personal data from the EU to the UK will need to perform an assessment of the regulatory regime and implement supplementary measures to support ongoing transfers.

The Schrems II decision, coupled with the increasing obligations under law to safeguard personal data when transferred across borders, highlights the ongoing push and pull between globalization and localization strategies. For the moment, localization may be winning.

Newly implemented regulations and others on the horizon

Looking back on 2020, the US Presidential election and the COVID-19 pandemic drew focus away from the data protection agenda. Neither regulators nor industry saw as much activity as anticipated in 2020. However, California led the charge for data protection rights in the US and introduced the California Consumer Privacy Act (CCPA) in January. They followed this with the California Consumer Rights Acts (CPRA), which brings in significant amendments to the CCPA and further entrenches privacy rights for Californian residents. The introduction of the CPRA will likely continue the drive for federal data protection legislation. However, additional state legislation may be implemented before comprehensive federal data protection legislation becomes a reality in the US.

Furthermore, the impact of the Schrems II decision has significant consequences for US organizations that process the personal data of EU residents, and we'll continue to see the ripple effects of this decision in 2021.

After the GDPR set the bar in 2019, many other countries have followed suit. In fact, several new privacy measures were enacted around the globe during 2020.

The New Zealand Privacy Act 2020 came into effect on 01 Dec 2020. It replaced the Privacy Act of 1993 and modernizes current privacy laws to keep pace with international standards.

While not as arduous as other international privacy laws, such as the GDPR, the new legislation introduces several significant changes. These include new regulatory powers for the New Zealand Privacy Commissioner, mandatory data breach notification if there's a risk of harm and new criminal penalties, including fines of up to NZD 10,000.

Notably, overseas organizations conducting business in New Zealand will be expressly required to comply with the new privacy laws as the Privacy Act 2020 has extraterritorial effect.

South Africa's (POPIA) was modeled heavily on the GDPR. It took effect on 01 July 2020 and applies to any organization processing personal information in South Africa. It allows organizations to process data deemed in a user's 'legitimate interest', potentially creating a loophole for possible abuse and enforcement difficulties. Enforcement begins on 01 July 2021.

The skills challenge



63% of organizations say that advancing digital transformation will increase needs for cybersecurity/threat intelligence skills in the coming two years



#1 cybersecurity/threat intelligence is the area where technology skills shortages are at their highest



Top challenges to managing in-house teams: lack of expertise and specialist security skills

Seeking to strike a balance between consumer trust and supporting personal data use for modernization, Singapore updated the terms of its Personal Data Protection Act (PDPA) in November 2020. The legislation allows organizations to collect, use or disclose personal data without an individual's consent. The organization must classify data management as 'legitimate interests' and ensure that the overall benefits outweigh any potential adverse effects. The legislation also increases the maximum fines an organization could pay for a data breach: up to 10% of its annual turnover or SGD 1 million, whichever is higher.

Organizations are feeling pressure as a result of these regulations. According to our research, 46% of respondents said they needed to hire additional skills in GRC, data protection and risk auditing because of compliance regulations. As mentioned above, over three-quarters (76%) of organizations felt unprepared to meet compliance obligations within the next 12 months. In 2021, we expect to see continued introduction of new data protection legislation globally and increased data protection enforcement by authorities.

Things to keep an eye on

The ongoing response to the Schrems II decision will continue to play out in 2021 as organizations rethink their strategies for cross-border transfers. However, while the compliance burden following Schrems II has certainly increased, there are opportunities for organizations that are able to build competitive solutions for what will likely become an increasingly localized EU market.

Organizations will be calling out for global harmonization of privacy laws. The number of competing laws and obligations will make it increasingly difficult for organizations to compete on a global scale and maximize opportunities through globalization strategies.

In the public sector, privacy will become a key area of contention in bids for privacy or transparency. We'll also see an increasing focus on the use of voter data in political campaigns, as well as the security surrounding electronic voting. The future will tell how important privacy is to enabling free and democratic societies.

Strategic guidance

Good data governance remains critical for managing risks associated with data privacy and protection. Understanding what data your organization has, who you share it with (i.e., third parties) and where it's located should be a top priority to help organizations manage their cybersecurity and data privacy risks.

Clear, open and transparent policies and notices for the distributed workforce including how employees are tracked and monitored when not in the workplace will be key to articulating the boundaries between business and private life.

Organizations will need to embed data protection by design practices (such as data protection impact assessments) throughout the business. This will be key to identifying cybersecurity and data protection risk up front and ensuring adequate technical and organizational measures are in place to protect individuals.

Organizations will need to train employees about information security, data privacy and protection risks. This will not just include policies, but what's expected of them in their roles in the protection of the organization's information assets and personal data. This will apply whether they're in the workplace, in a coffee shop or at home.

This sentiment is supported by our research, which indicates that overall, cybersecurity is the top technology priority for organizations over the next 12-18 months. It's also the number one factor impacting technology decision-making.



Regulatory compliance, COVID-19, ransomware and APTs have all been significant challenges for organizations to face during 2020. Any large, high-profile event, such as preparing for the Olympics, requires active management of a wide variety of such threats.

Clear, open and transparent policies and notices for the distributed workforce, including how employees are tracked and monitored when not in the workplace, will be key to articulating the boundaries between business and private life.



2020 Olympics threat landscape

The 2020 Olympic Games are scheduled to begin on 23 July 2021 in Tokyo, Japan. The Games were postponed due to heightened cases of COVID-19, globally.

The 2020 Olympics threat landscape includes cybersecurity and geopolitical threats stemming from current events, regional disputes over territories and longstanding historical animosities. Based on observations, current and past cyber-incidents, and considering Japan's role as the Olympics' host country, we expect that a high level of cyberactivity against targets in Japan is likely.

Historical tensions, geopolitically motivated attacks and hacktivist causes will likely help spur cyberattacks. Disruptive attacks, such as those which took place during the 2018 PyeongChang Olympics, could impact ticketing services, Wi-Fi, broadcast networks, POS systems or critical infrastructure.

DDoS attacks against Tokyo's critical infrastructure may impact the reliability of electricity, gas, water and public transportation. Disruption of critical infrastructure services would potentially cause health and safety issues, as well as cybersecurity problems.

Threat actors are expected to pursue financial gain by deploying ransomware to disrupt operations during the Games. A successful ransomware attack against Tokyo's Olympic Games' IT system could leave the Games and associated operations at risk.

Disinformation campaigns launched by nation-state threat actors pose a different risk. Nation-state disinformation and influence campaigns have been successful in sowing discord and creating chaos socially and politically. The Olympics is the type of high-profile event that could yield a negative or embarrassing impact from a successfully orchestrated and implemented disinformation campaign.

The World Anti-Doping Agency (WADA) recently levied anti-doping penalties against Russia. In January 2019, investigators received information that Russia manipulated laboratory results for their Olympic athletes. In December 2019, WADA banned Russia from competing in international sporting events for four years based on that investigation. Some of the penalties levied included not playing the Russian anthem during the 2020 (July 2021) Olympics; Russian athletes will have to compete under a neutral flag instead of the Russian flag. In retaliation, Russian threat actors launched attacks against WADA, breaching and exposing Olympic athletes' personal and medical information. It's likely that Russia will launch future attacks against anti-doping agencies and against the Olympic Games as this is the second time Russia has been banned from the Olympics.

Other potential targets

Olympic athletes, tourists visiting Tokyo and Olympic game attendees are high-value targets. But they're not alone as attackers are likely to target Japanese officials, visiting Government officials, Olympic partners, sponsors, supply chain entities and infrastructure providers. The international crowd and its accompanying personal, professional and financial information will be prime targets for cybercriminals. Many travelers use free Wi-Fi in transit and at their destinations. Most tourists don't practice good cyber-hygiene while using unprotected online systems. This lack of cybersecurity awareness may leave them vulnerable to cyberattacks and having their credentials and personal or financial information stolen.

Japan's cybersecurity posture and geopolitical threat landscape

The 2020 Olympics Organizing Committee has already seen phishing scams and other criminal activity preceding the 2020 Olympics. As host to the Olympics, Japan faces many cybersecurity challenges and is actively preparing to tackle them by implementing changes to secure cybersecurity systems in its business and government environments.

Cybercriminals and nation-state threat actors may leverage the 2020 Games as an opportunity to target Tokyo's infrastructure. Securing critical infrastructure and ensuring the resiliency of cybersecurity systems are critical to any country, or city. But it becomes even more important when relying on IT to deliver services securely and to support a global, high-profile event. Japan's dedication to securing its cyber-infrastructure will enhance its ability to detect, defend and respond to incidents during the Games.

Summary and recommendations

Cybersecurity plans for the Games must begin with instituting a comprehensive cybersecurity program. Focus on cyber-hygiene and train all employees in basic cybersecurity practices, and their roles in supporting effective security measures.

IT stakeholders must know which systems are running on their organization's network. They must patch these systems regularly, implement multi-factor authentication and segment networks. Following these steps will help secure systems against less-sophisticated threat actor attacks and provide additional obstacles for APTs and nation-state threat actors to overcome.

Regular communication and information sharing among corporate sponsors, government, industry and utilities, including electric, gas, water and internet service providers, will continue to be important in defending against threats. Open information sharing will allow for faster communication should a cyber-event be identified during the Games.

Incident response training exercises prior to and during the Games will keep all security stakeholders actively engaged and prepared to defend against cyberattacks. Designating one entity to coordinate, facilitate and disseminate cyberattack information will streamline the flow of attack data, aid in decision-making and reduce response times. Regular security briefings via public channels, the internet, social media platforms and the Olympics app, if one is available, will aid in countering any disinformation campaigns and arm the public with accurate knowledge with which to respond to emergencies.

Cybersecurity stakeholders must ensure regular examination of critical systems before, during and after the Games. IT providers and all involved in securing Tokyo's and Japan's cyber-infrastructure must monitor the security tools deployed, shut down any services unnecessarily exposed to the internet and ensure logging capabilities are centralized. Security teams must also identify a baseline for activity in their environments. Although the level of activity will change during the Games, establishing a baseline prior to the event will allow for quick identification and addressing of anomalies. Ongoing testing will also help identify security gaps and prompt a gap analysis.

Although these recommendations address threats to the 2020 Olympic Games, the concepts can be applied to security measures taken for events in which international organizations, Governments and business entities are involved, and in which heads of state, business executives and IT professionals are considered high-value targets.

Just as hosts of high-profile events need to address concerns regarding privacy and regulations, organizations globally need to navigate increasing challenges posed by how to deal with privacy, regulations and governance and compliance.

Regulatory compliance, COVID-19, ransomware and APTs have all been hurdles faced by organizations during 2020. In the next section, we'll summarize our overall conclusions regarding the threats, regulations, issues and mitigation strategies over the past year.

Conclusions

The consistent and reliable delivery of services is more complex than simply having the ability to recover from disruptions. Organizations must be able to predict and prevent them. Those organizations that invest in resiliency for all aspects of business operations, technology, people and controls will have the greatest success in managing risk.

Although we provide multiple recommendations throughout this Report, we believe the following principles can be valuable to help you move toward your information security and data protection goals:

Position cybersecurity as a key strategic component of the business

Organizations are trying to modernize their businesses. A key part of this is enabling effective digital transformation that better supports the current demands of the business. Given the scale of threats organizations are currently facing, they must include cybersecurity as a Board-level agenda item and treat it as a fundamental business requirement to support operations.

Prioritize people and process

Organizations need to embrace their most critical resources – their people. They can do this most effectively by implementing appropriate user education. The goal is not to make all employees security experts, but to make sure they understand the role they play in the organization's security posture. Train employees to do their jobs in a 'security aware' manner – not to be the weakest link, nor the strongest link, but one more key component. Those who are responsible for the technical components of the security profile must make sure their organizations provide employees with the technology and security training they need to do their jobs effectively.

Embrace security by design

Organizations simply cannot plug-in or add on the security required for them to operate in an effective manner. They must build security best practices into policies, procedures, infrastructures and applications. In what's functionally a systems design process, the organization should include consideration of security goals, strategies and tactics in the foundations of any project, product development or functional implementation.

Adopt existing cybersecurity frameworks and standards

Organizations should continue to emphasize leveraging standards, knowledgebases and frameworks defined by leaders in the cybersecurity community. MITRE ATT&CK and the NIST Cybersecurity Framework are examples of resources that contain valuable information from seasoned cybersecurity professionals and working groups. Leveraging these resources can provide your organization with a wealth of knowledge that can rapidly bolster your organization's security posture.

If we operate with a 'breach posture', we're functioning with less trust in the component parts of our organizations.

Prioritize continuous monitoring

Organizations need to be able to identify and react to attacks and breaches faster. Many breaches include compromises that have gone undetected for months, or even years. If we operate with a 'breach posture', we are functioning with less trust in the component parts of our organizations. Prioritize security to enable the organization to identify and manage breaches when they occur. The goal of security programs should be to focus detection and response activities on the breaches that have the greatest potential to affect the organization.

As threats continue to evolve, we're likely to observe the following activity throughout 2021:

- Attackers will target end users with phishing campaigns related to COVID-19 and the Olympics. Just as with any significant global event, malicious actors are waiting to leverage social media and current events to further their malicious campaigns.
- Ransomware and crypto-mining activities will continue to grow and be a key focus area for cybercriminals. Toolkits to support these capabilities proliferate and history illustrates it's a lucrative venture for attackers' financial gain.
- Organizations will continue to struggle with implementing effective security for a largely remote workforce. Although the tools are available to support remote work environments, organizations will need to leverage vendor expertise to implement them efficiently, together with secure by design solutions.
- Organizations will struggle to keep up with growing compliance mandates and will have to continue to adjust to the rapidly changing environment which COVID-19 has created over the last year and a half.

Lastly, organizations must remember the keys to an effective cybersecurity program are planning, execution, monitoring and accountability. Remaining vigilant and constantly updating your threat intelligence, detection; response and business continuity plans are vital to success.

The background is a dark blue grid of small, light blue dots. Two bright orange lines cross each other in the upper right quadrant. Faint, semi-transparent text from another page is visible in the background, including "Canada", "United States", and "United States".

NTT Global data analysis methodology

Our 2021 Global Threat Intelligence Report contains
global attack data gathered from four proprietary
NTT resources.

NTT Global Threat Intelligence Center (GTIC)

Our 2021 Global Threat Intelligence Report contains global attack data gathered from NTT and supported operating organizations from 01 January, 2020 to 31 December, 2020. The analysis is based on log, event, attack, incident and vulnerability data from clients as well as from our global honeypot network. Leveraging the indicator, campaign and adversary analysis from our Global Threat Intelligence Platform has played a significant role in tying activities to actors and campaigns.

We gather security log, alert, event and attack information which we enrich. We then analyse the contextualized data. This process enables real-time global threat intelligence and alerting. The size and diversity of our client base, which includes over 15,000 security engagements with clients spanning 57 countries in multiple industries, provides us with security information which is representative of the threats encountered by most organizations.

The data is derived from worldwide log events identifying attacks based on types or quantities of events. The use of validated attack events, as opposed to the raw volume of log data or network traffic, more accurately represents actual attack counts. Without proper categorization of attack events, the disproportionately large volume of network reconnaissance traffic, false positives, authorized security scanning and large floods of DDoS monitored by Security Operations Centers (SOCs), would obscure the actual incidence of attacks. The inclusion of data from our SOCs and research and development centers provides a highly accurate representation of the ever-evolving global threat landscape.

Cybersecurity Advisory data

The Cybersecurity Advisory data used in this Report includes sanitized current and target state maturity levels analysed globally and covering multiple industries. The data is used to benchmark clients against their industry peers on a regional and global level. In our benchmarking data we consolidate all global assessments used to measure clients' maturity of processes, metrics and tools. The focus areas for the evaluation include Security Vision and Strategy; Information Security Framework; Risk Management; Operations; and Applications, Devices, and Infrastructure.

NTT's WhiteHat Security

The application security data and analysis are provided by NTT's WhiteHat Security. This data is collected from our Dynamic Application Security Testing service and is sourced from testing running applications in production and pre-production environments. The statistical analysis focuses exclusively on assessment and remediation data for custom applications. Data is segmented along multiple dimensions including vulnerability risk levels, vulnerability classes and industries. Data analysis uses key indicators which include the likelihood of a given vulnerability class, remediation rates, time-to-fix and age of open vulnerabilities. Risk levels are based on the rating methodology of OWASP. Vulnerabilities are rated on five levels of risk – Critical, High, Medium, Low and Note. Critical and high-risk vulnerabilities are collectively referred to as 'serious' vulnerabilities. Vulnerability classes are based on the threat classification of the Web Application Security Consortium (WASC).

NTT's global research

For this year's Report, we commissioned Jigsaw Research to undertake 1350 online interviews of technology and business decision-makers in large organizations in 15 sectors and 21 countries, including 1046 IT and cybersecurity professionals.

Data analysis uses key indicators which include the likelihood of a given vulnerability class, remediation rates, time-to-fix and age of open vulnerabilities.

NTT resource information

The NTT Global Threat Intelligence Center (GTIC) protects, informs and educates our clients through the following activities:

- threat research
- vulnerability research
- intelligence fusion and analytics
- communication to NTT clients

The GTIC goes beyond the activities of a traditional pure research organization, by taking threat and vulnerability research and combining it with their detective technologies to produce applied threat intelligence. The GTIC's mission is to protect clients by providing advanced threat research and security intelligence to enable us to prevent, detect and respond to cyberthreats.

Leveraging intelligence capabilities and resources from around the world, our threat research is focused on gaining understanding of, and insight into the various threat actors, exploit tools and malware – and the techniques, tactics and procedures used by attackers.

Vulnerability research pre-emptively uncovers zero-day vulnerabilities that are likely to become the newest attack vector, while maintaining a deep understanding of published vulnerabilities. With this knowledge, our security monitoring services can more accurately identify malicious activity which is 'on-target' to our clients' infrastructure.

Intelligence fusion and analytics is where it all comes together. The GTIC continually monitors the global threat landscape for new and emerging threats using our global internet infrastructure, clouds, and data centers along with third-party intelligence feeds. It works to understand, analyse and enrich those threats using advanced analysis techniques and proprietary tools, and curates and publishes them using the NTT Global Threat Intelligence Platform (GTIP).

NTT-CERT, a division of NTT Secure Platform Laboratories, serves as a trusted point of contact for Computer Security Incident Response Team (CSIRT) specialists, and provides full-range CSIRT services within NTT. NTT-CERT generates original intelligence regarding cybersecurity threats, helping to enhance our organizations' capabilities in the security services and secure network services fields.

To learn more about NTT-CERT, please visit www.ntt-cert.org

Contributors

NTT is a proud member of the Cyber Threat Alliance and Europol. We thank them for their contributions and support.

Cyber Threat Alliance

The Cyber Threat Alliance (CTA) is a 501(c)(6) non-profit organization working to improve the cybersecurity of our global digital ecosystem by enabling near real-time, high-quality cyber threat information sharing among organizations in the cybersecurity field. CTA's mission is to improve the overall cybersecurity of the global digital ecosystem; enabling our members to share high-quality cyberthreat information at both human and machine speed; distribute critical defensive information and threat reports; and work in a trusted community.

Europol

Europol is the European Union's law enforcement agency. Its main goal is to achieve a safer Europe for the benefit of all EU citizens. Headquartered in The Hague, The Netherlands, it supports the 27 EU Member States in their fight against terrorism, cybercrime, and other serious and organized forms of crime.



Together we do great things