
NTT
INSIGHTS
DRIVEN BY DATA
2020
Global Threat
Intelligence Report
The nature of security:
Be resilient to thrive
Together we do great things
hello.global.ntt

The NTT Ltd. 2020 Global Threat Intelligence Report reminds us that the threat landscape is **continuously changing, especially during these tumultuous times.** In such a **dynamic environment,** and with absolute security as an impossible goal, businesses **must be ready for anything.**

To this end, our Report recommends that businesses strive to be both **secure by design** and **cyber-resilient.** It's through finding the right **application and balance** of these two concepts that they can **truly minimize business risk.**

Contents

Foreword

As the world unites and draws on all available resources to contain the global coronavirus (COVID-19) pandemic, unfortunately, there will be those who'll try to take advantage of the crisis for nefarious purposes.

As organizations continue to drive business practices through digital transformation, the challenges they face evolve as well. Cybercriminals are among this group. With large numbers of employees and students working from home, businesses are facing increasing risk of becoming victims of cybercrime. **Every organization should go the extra mile to protect their customers, partners and employees during these unprecedented and uncertain times.**

NTT Ltd. provides solutions for challenges impacting clients across many industries globally.

In our 2020 Global Threat Intelligence Report, we identify the unique challenges regions and industries face, and the operational, tactical and strategic considerations organizations should leverage to manage risk.

Our report identifies modern and emerging trends observed across many industries and regions. Armed with this knowledge, cybersecurity leaders will gain greater situational awareness allowing them to guide investments and support decisions to aid in improving their security posture.

Additionally, cybersecurity defenders should leverage this information to assess identified threats against their own risk profile and technology footprint to bolster targeted threat detection and response efforts.

Mark Thomas

Global Head of Threat Intelligence, NTT Ltd.

For the past 19 years, Mark has worked in the cybersecurity field establishing pragmatic, business-aligned risk minimization strategies and developing intelligence-led computer network defenses. His broad knowledge and in-depth expertise are a result of working extensively in consulting, technical, and managed security services with large enterprises across numerous industry including finance, government, utilities, retail, and education. Mark leads the NTT Ltd Global Threat Intelligence Center (GTIC) responsible for global threat research, communications and sharing alliances, and building intelligence-driven security services.

Follow Mark on LinkedIn

Executive Summary

Summary of key findings

Adversaries continue to innovate

Attack volumes increased across all industries between 2018 and 2019. Due to the overwhelming success of the use of tools such as web shells, exploit kits, and targeted ransomware, adversaries are still developing effective multifunction attack tools and capabilities. The most common techniques observed globally were remote code execution (15%) and injection (14%) attacks. In most cases, these attacks continue to be effective due to organizations poor practices related to network, operating system, and application configuration, testing, security controls and overall security hygiene. Adversaries are also leveraging artificial intelligence, machine learning, and investing in the automation of attacks. 21% of malware detected was in the form of a vulnerability scanner which also supports the premise that automation is key focus point of attackers.

Old vulnerabilities still a prime target

As with previous year's reports, attackers are still focusing on leveraging vulnerabilities which are several years old, have patches available, but are still not being addressed by organization's patch and configuration management programs. 258 new vulnerabilities were identified in Apache frameworks and software, such as Struts and Tomcat, over the last two years. Additionally, Apache software was the third most targeted in 2019, accounting for over 15% of all attacks observed.

IoT weaponization: IoT devices continue to be compromised

The re-emergence of Mirai and variants has helped widen the spread of IoT attacks. Botnets such as Mirai, IoTroop, and Echobot have advanced their propagation capabilities by investing in automation. IoTroop remains a persistent threat, accounting for 87% of botnet activity detected in Japan.

Technology leads top attacked industries

Technology was the most attacked industry in 2019, accounting for 25% of all attacks observed. Significant increases in application-specific and DoS/DDoS attacks, along with weaponization of IoT attacks against technology contributed to technology becoming the most attacked industry. Technology was previously the second most attacked industry in 2017 and 2018 and had the highest occurrence of ransomware activity at 9%, while no other industry showed higher detections of ransomware than 4%. Government activity driven by geo-political activity accounted for 16% of activity this year, compared to 9% in 2019. The technology industry also had the lowest performance of application security, with an average of 12 serious vulnerabilities per web application.

Content management systems heavily targeted

Malicious actors leverage compromised web servers to steal valuable data and use these powerful resources to conduct additional cyber-attacks. Some of the most dominant activity during the past year was related to attacks against popular content management systems (CMS), malware activity, and web-application attacks. Popular CMS platforms such as Joomla!, Drupal, and noneCMS account for the majority of CMS market share. They also represent being the target of approximately 20% of all observed attacks globally. Additionally, nearly 55% of all attacks were application-specific (33%) and web-application (22%) attacks.

2019 a year of enforcement: GRC continues to become more complex

More data privacy professionals are influencing the digital agenda. At the current rate of increasing governance, risk, and compliance (GRC) initiatives globally, being complacent with compliance will likely continue to create challenges for organizations. The regulatory landscape is continuing to make dynamic shifts and globalization of third-party vendors and suppliers compounds complexity. Several acts and laws are influencing how organizations handle data and privacy, including the California Consumer Privacy Act, Brazilian General Data Protection Law, India's Personal Data Protection Bill, and Singapore Personal Data Protection Act.

Although we provide multiple recommendations throughout the report, we believe the following principles can be valuable to consider as you move towards your information security and data protection goals.

Summary of recommendations

Mature your organization's approach to be secure by design

Cyber-resiliency and implementing solutions which are secure by design is a vital component in conducting business in a digital world. Understanding your organization's goals, identifying acceptable risk, and building cyber-resilient capabilities are essential to navigating the threat landscape. As a start, NTT Ltd. strongly recommends evaluating your organization's current state and identifying your desired future state. We devoted an entire section of this year's report to discussing what cyber-resiliency is, how to achieve it, and how to measure its effectiveness and value.

Pursue intelligence-driven cybersecurity

Organizations following traditional cybersecurity practices have been forced to rethink their approach. The complexity of the threat landscape, coupled with ever-changing standards, regulations, and privacy legislation, continue to raise the bar for what a complete security program must address. Traditional practices are, and will remain, inadequate against modern threats, and organizations must acknowledge absolute security is simply not possible. Cybersecurity and business leadership must change the way they think and apply security, and must transform from a reactive mindset, to a more effective, proactive, intelligence-driven approach.

Monitor the threat environment

Organizations which keep a close watch on the current threat environment will have a significant advantage in addressing threats. Leveraging intelligent cybersecurity to guide decisions, support business agility, and maintain an acceptable risk level for the organization is essential to success. If your organization is not leveraging organic threat intelligence capabilities, or actively collaborating in threat intelligence communities, it will be at a disadvantage while attempting to manage risk.

Focus on standardization of controls

Cybersecurity defenders should focus on leveraging standards, knowledgebases, and frameworks defined by global leaders in the security space. MITRE ATT&CK and NIST Cybersecurity Framework are a few examples of knowledgebases and frameworks which are becoming increasingly popular with cybersecurity practitioners abroad. Security frameworks containing standard recommendations exist to help organizations mitigate risks and provide excellent information to help organizations assess organizational risk.

[1] *https://hello.global.ntt/insights/risk-value-report*

If your organization is not **leveraging organic threat intelligence capabilities**, or actively collaborating in threat intelligence communities, it will be at a disadvantage while attempting **to manage risk**.

The impact of COVID-19 on global business

A species thought to be over 310–320 million years old, reptiles possess a hardy exterior. Found on every continent, they have a talent for adapting to even the harshest environments.

From the first amphibian emerging from the water, to the giant Tyrannosaurus Rex stalking the earth in the Mesozoic era, and the household pet lizard, reptiles could singularly define evolutionary success.

The impact of COVID-19 on global business

The COVID-19 pandemic is affecting every aspect of society and disrupting lives, as well as standard business operations. COVID-19 is impacting the globe like no event has since World War II.

Many businesses have been crippled by the outbreak; some have shut down, and others will likely be unable to recover. Some are thriving due to the increased demand COVID-19 has placed on their particular business – but even those organizations are changing the way they operate at a very basic level. Organizations are engaging working from home options and supporting physical isolation to help protect their staff. In this environment, organizations need to learn how to continue to operate while managing the well-being of their people, along with the changing demands of the market.

Somewhat understandably, managing unexpected change often means 'security' takes a back seat while businesses focus on 'getting things done'. That means it becomes even more important for security managers and groups to focus on the aspects of security which are designed to enable businesses – to 'get things done, in a secure manner' – to enable safe and secure operations in a way which may not otherwise be possible.

As a recap of events leading up to the production of the GTIR, the following timeline summarizes the escalation of both the COVID-19 virus and hostile cyberactivity for the first quarter of 2020. In general, attacks related to COVID-19 rose as infections increased around the world.

31 Dec 2019 - Chinese authorities inform WHO's China office of pneumonia cases in Wuhan City, Hubei province.

Jan

Early to mid-January - first observations of COVID-19 related phishing emails observed; NTT J-CERT observes campaigns leveraging EMOTET.

7 Jan 2020 - China identifies new coronavirus as cause of the outbreak.

Suspected nation state actors conduct attacks against multiple industries, attempting to exploit vulnerabilities in Citrix applications as Wuhan sees its first wave of infections.

9 Jan 2020 - China reports first death linked to the new coronavirus, 2019-nCoV.

Phishing campaigns continue to increase, becoming more targeted.

20 Jan 2020 - The CDC confirmed that a US patient tested positive for COVID-19.

Domain registrations using COVID-19 themed domain names peak at close to 2000/day. The initial spike coincided with a large spike in reported COVID-19 cases in mid-February, possibly indicating that attackers have begun to realize the utility of COVID-19 as a cyberattack vector. Ongoing.

30 Jan 2020 — WHO Director-General declares the 2019-nCoV outbreak a public health emergency of international concern.

Feb

Phishing campaigns continue to increase, becoming more targeted.

11 Feb 2020 - WHO assigns the novel coronavirus its official name: COVID-19.

The Johns Hopkins University COVID-19 map is leveraged to distribute malware. Johns Hopkins University issued an advisory in mid-March to address.

Threat actors employ ransomware under the guise of security software. The new CoronaVirus ransomware is being distributed via the WiseCleaner website. This same campaign attempts to deploy Kpot, a password-stealing Trojan, as well.

Mar

11 Mar 2020 - WHO Director-General Tedros Adhanom Ghebreyesus declares the global COVID-19 outbreak a pandemic.

Information stealers like Trickbot are being leveraged in phishing and campaigns, in attempts to steal sensitive data.

13 Mar 2020 - Cyber-attack against a healthcare facility in the Czech Republic, significantly affecting operations and patient care, prompting a new look at laws and regulations protecting healthcare facilities.

Attackers leverage Oski information-stealing malware to hijack a router's DNS settings. In this attack, internet browsers display alerts for a fake COVID-19 information app appearing to be from the WHO.

Zeus Sphinx Trojan remerges after 3 years, with several instances beginning in Dec 2019, continually intensifying through April 2020.

Apr

Cyber criminals target remote communications applications like Zoom, as remote work and online education become more prevalent.

2 Apr 2020 - Passed 1 million infected.

COVID-19's impact on organizational operations

COVID-19 is impacting people and organizations around the world. It directly impacts the health of many and affects others who are not infected. It also impacts organizations as they strive to support their people through this global crisis, while trying to manage some sense of ongoing business and normalcy of social interaction.

All business and security impacts from COVID-19 come from the effect the virus has on people. COVID-19 does not target systems, applications, or other technologies, it affects the people who design, build, manufacture, ship, sell, use, and support them. As such, business processes are disrupted during the COVID-19 pandemic, as organizations struggle to maintain as much business capacity as they can during the crisis. Social distancing and physical isolation techniques are being used in attempts to help control the spread of the virus and to protect the people being isolated.

The business effects of COVID-19 vary greatly, depending on the specifics of the industry. As discussed in the Cyber-resiliency section of this report, organizations can maximize their preparedness to continue delivering goods and services by focusing on resilience and security as a core business requirement. But even businesses who had very mature security programs have been affected by the scale of this virus. Some businesses are suffering because of travel restrictions, isolation requirements, and other reactions to the virus, while others are thriving because their business fulfills a demand. But regardless of the exact business, many of the security implications of the virus are similar.

Working from home

Businesses around the world have implemented 'work from home' policies. This can be anything from an employee taking regular business calls at home to an organization building a virtual workplace with modern collaboration tools, file sharing, and teleconferencing suites. In any remote working environment, the organization still needs employees to be able to:

If COVID-19 has changed the profile of 'remote' workers – like increasing the number or composition of their remote workforce – is has the potential to cause significant disruption in the work environment. It is now 'business unusual' instead of 'business as usual'. The organization is forced to build and maintain an infrastructure which supports the changed computing, collaboration and communication needs of the business in order to enable employees. Change increases organizational and business risk. Rapid, reactionary change introduces the highest amount of business risk. One of those business risks includes the organization's capability to adapt security policies and procedures to that change – the ability of the organization to continue to protect organizational and customer information.

Increased cyberthreat

COVID-19 has brought its own 'cyber' threats along with the actual virus. Phishing attacks leveraging the coronavirus started in mid-January 2020. Cyberattack type and volume escalate daily, with attacks including:

1. Websites posing as 'official' information sources, but host exploit kits and/or malware – created at an incredible rate, sometimes exceeding 2000 new sites per day.
2. Campaigns which distribute Emotet, Trickbot, Lokibot, Kpot, CoronaVirus (a ransomware variant), Zeus Sphinx, and other malware variants.
3. Attacks which spoof DNS, or hijack router DNS settings via weak or default admin passwords.
4. The use of an open redirect which pushes Raccoon info-stealing malware to the affected system and prompts the user to download a 'COVID-19 Inform App allegedly from the World Health Organization.
5. Exploit attempts against a previously known remote code execution vulnerability in Citrix Application Delivery Controller (ADC) and Citrix Gateway devices (CVE-2019-19781).
6. A variety of cyberattacks on healthcare and support organizations responsible for helping people through this health emergency.

NTT Ltd. attack data from 2019 indicates that about 55% of all attacks were a combination of web-application and application-specific attacks. About 20% of all attacks targeted CMS suites, and more than 28% targeted technologies which support websites, like ColdFusion and Apache Struts. For organizations relying more on their web presence, like customer portals and supported web applications, this is increasing reliance on the very systems which attackers have already been targeting at high levels.

Industry-specific impacts

NTT Ltd. analysts evaluated the affects COVID-19 and related cyberattacks have had on the industries discussed in this report. Many of the impacts and attacks are similar in nature, but there are some notable differences depending on the specific industry.

Healthcare: The COVID-19 pandemic has spawned an uptick in a variety of cyberattacks against healthcare organizations. Ransomware attacks, phishing exploits, fake domains, disinformation campaigns, and supply chain disruptions are threats currently facing the healthcare industry. In addition to contracting COVID-19 and coronavirus-related cyberattacks, supply chain disruption could be the next most significant healthcare threat, should manufacture and delivery of ventilators, medical supplies, and medicine be disrupted for long periods of time, or become unavailable. As COVID-19 patient care continues to overwhelm the healthcare system, doctors are moving from in-office visits to virtual visits to protect frontline medical professionals and staff from infection, and to mitigate the spread of COVID-19. Telehealth comes with inherent cybersecurity and patient privacy risks, such as protection of Personal Identifying Information (PII), and protection of medical information, including diagnoses, types of medicines prescribed, medical tests, and lab results, all of which can be accessed in the medical provider's patient portal and potentially exploited. Increased reliance on e-portals places greater use on the exact internet systems which threat actors are attacking – the web-presences and customer portals of targeted organizations.

Finance: The COVID-19 pandemic has directly affected global financial markets and the banking industry. Fluctuations in stock prices, financial losses, and minimal market recovery have impacted the ability to purchase food, household items, and other necessities dramatically changing spending habits for millions of people. People are furloughed, laid off, or simply not getting hours, and are unable to make mortgage or auto loan payments. In-person banking has dropped off dramatically, but the use of e-banking has increased. Credit card use is up as online shopping replaces in-person purchases, increasing the amount of credit card information available in the market. Commercial banking is facing challenges as many organizations are unable to pay bills, including leases, as well as mortgages and other loan payments. In fact, many organizations are looking for capital to support cash flow and keep businesses open.

Financial and banking institutions, as well as their customers, are being hit with a barrage of cyberattacks with phishing attempts at the top of the list. One such example is Zeus Sphinx which uses malicious documents (maldocs) with email subject lines touting coronavirus relief payments for those staying home to stem the spread of COVID-19. Once opened, the email recipient is directed to click on a link to complete the attached form which infects the computer with malware when downloaded.

Technology: As people are having to socially distance themselves, they are turning more and more to technology to remain in contact and conduct more day-to-day activities. Unfortunately, the technology industry itself faces supply chain and vendor resource challenges as their assembly lines and distribution channels fall victim to COVID-19 outbreaks and isolation requirements. The technology industry, while impacted similarly to most other industries, has seen an increase in business opportunities during this crisis, primarily due to the significant increase in remote work, remote education, and remote healthcare. But these added requirements also are likely pushing the thresholds of delivery and customer service capacities. The downside to this is that it is taking its toll on Internet bandwidth across the globe. Another downside is that many applications are being urgently implemented but not properly secured, as more people are working and schooling from home, and attackers are taking advantage by, for example, exploiting virtual meeting applications. And, to add insult to injury, cyber criminals, in true form, are attempting attacks on already overloaded emergency systems, to include law enforcement, fire departments and emergency dispatch systems, exploiting the urgency factor with things like ransomware and denial of service, further hampering the ability of emergence personnel to assist those in need. Cybercriminals and other threat actors will always try to capitalize on a crisis in any way they can; technologies – especially those which remain unsecured – will prove viable targets.

If COVID-19 has changed the profile of 'remote' workers – like increasing the number or composition of their remote workforce – it has the **potential to cause significant disruption in the work environment**. It is now 'business unusual' instead of 'business as usual'.

Manufacturing: Supply chain issues are plaguing the manufacturing industry due to COVID-19, as factories scale back, cease operations, or have to close altogether to keep workers safe. And manufacturers are truly under the gun to continue to provide materials and goods to other essential services across the globe. This requires identifying essential personnel and critical infrastructure and keeping both safe – from physical and cybersecurity standpoints.

This increased demand from manufacturers requires a greater security for their organizations, personnel, operations and products – and are only as great as the weakest link in the supply chain, for which there are increasing unknowns during this pandemic. Like many industries, manufacturers are having to adjust operations to accommodate a more digitized and remote workforce. Again, if network and system security are poorly implemented, the entire supply chain is affected.

The silver lining, though, for some organizations in the manufacturing industry, are the pleas from government officials to convert operations to create much needed items, like personal protective equipment – for instance in the case of General Motors (GM) and FORD, to convert operations to manufacture ventilators essential to treating patients stricken with COVID-19 – assisting with the economic side of this crisis from a business perspective.

Retail: In most cases brick and mortar retail has fallen dramatically, with many retailers closing doors to face-to-face sales. Retailers are working to replace some of that revenue with online sales, but this requires the capability to support online ordering, order fulfillment, and payment processing, as well as having the ability to ship or deliver goods. While this might not impact some retailers, it could be a significant shift in retail operations, even an impractical shift for others.

Retailers are also faced with supply dynamics – a potentially unpredictable supply chain and distribution channels. Demand for some products has dropped considerably, while retailers are faced with a marketplace with tendencies to panic shop. As retailers place greater stress on their online capabilities, this has the potential to create instability in their internet sites – relying on applications and tools which have consistently been highly targeted by attackers for years. New or updated applications are likely to be targeted by attackers looking to take advantage of exposed vulnerabilities. At the same time, online retailers are getting new account holders, or old account holders are reactivating inactive accounts. As users make more use of online sites, they become more susceptible to phishing attacks – especially when directed at inexperienced online shoppers.

With more people shopping online to comply with stay-at-home orders in many areas of the world, retailers are having to up their online game, including maintaining security on public-facing websites, ensuring customer data (name, address, credit card information) security. Domain registrations of fake websites and phishing emails continue to surge – consumers need to make sure they're not clicking on links in emails, especially from retailers which promise extraordinary discounts, but manually go to the website. In addition, customers should purchase only from known retailers.

Recommendations

There are many recommendations for organizations trying to adapt to requirements businesses are faced with, while managing the impact of COVID-19. Most of those recommendations fall into five higher level categories which organizations should consider:

1. **Focus on the people.** To the extent possible, organizations should focus on making sure their staff are safe and put in a position where they can thrive. COVID-19 is a global health emergency the likes of which no one alive has ever seen. It is the source of great concern and anxiety around the world. Some people can function in chaos, and others are paralyzed, spending hours daily reading COVID-19 updates and news. COVID-19 has the capacity to affect all aspects of operations, including the ongoing ability of the business to meet both security and business goals. Organizations should work to understand what their people are going through, and actively work to support them through this time of chaos. This may mean patience. This may mean more flexible work hours. It may mean understanding that people cannot function at maximum capacity when at least some of their mind is occupied by the potential impact of the virus. It may mean making counselling services available, or even mandatory, if the situation calls for it.

2. **Prioritize carefully.** COVID-19 has placed all of us in a dynamic environment which forces organizations to work differently. Rapid change has the potential to derail planned initiatives and careful actions, but it does not need to. Organizations must continue considering the impact of new and changing initiatives to evaluate their impact on the well-being of their staff, on the ability of the organization to move forwards on its business goals, and the effectiveness (and practicality) of security controls. It will be necessary for organizations to weigh the risk/value of initiatives more carefully, especially when it comes to the secure management of data.

3. **Don't forget about security.** Organizations are in a position where they must be able to quickly adjust to changes in the world, and should be in a position to protect their people and their operations. Part of business operations is getting the job done, but the other part must be about getting the job done in a secure manner which protects organizational assets. Businesses have different priorities, models, regulatory requirements, and expectations. Organizations who have access to highly sensitive information like patient healthcare information or customer financial records, are expected to maintain proper compliance and protect that information as appropriate. In reality, when organizations are implementing new or updating features, it may be more efficient for the organization to consider security first, not thinking 'how can I do this?' but asking 'how can I do this securely?'.

4. **Re-educate all employees on policies, procedures, and acceptable practices.** Most organizations have changed operations in some way, from changing vendors, processes, or marketplaces, to adopting a more virtual workplace. As organizations change, they must effectively communicate new business rules and processes to help ensure operations can continue, while managing impacts to the business. This includes updated security policies and procedures, including how to report incidents and request security guidance. Organizations should continue to educate employees on evolving COVID-19 relevant cyberattacks and phishing attacks. Organizations should consider directing all employees to official sites where they are able to get accurate, high-integrity information about the virus. Organizations may wish to consider establishing their own internal communication mechanism or clearing house for official COVID-19 news to help reduce employees' exposure to hostile sites and disinformation.

5. **Continue to emphasize good security hygiene.** COVID-19 has thrown the world into chaos. Threat actors are continuing to take advantage of that chaos by escalating cyberattacks. A significant number of those attacks attempt to take advantage of lapses in our security preparedness. With the rise in hostile cyberactivity, it is more important than ever that organizations prioritize the timely application of patches and updates, especially in the environments upon which organizations are relying. If you are making more use of flexible meeting/communication enablement applications, make sure you are running the latest versions, and monitor for updated versions. Continue to patch and update the systems you rely on, since threat actors are targeting organizations at an ever-increasing rate. Beyond that, organizations should continue to prioritize good backups, and place even greater emphasis on end-point control, including appropriate antivirus software.

Final thoughts on COVID-19 and cybersecurity

From a security point of view, COVID-19 is an exercise of an organization's business continuity plan – managing the effect of mass disruption in a changing environment. COVID-19 affects organizations because it targets the most valuable part of those organizations – the people. The COVID-19 pandemic has brought about fundamental changes to businesses and their operational environment. Organizations must support their staff in this potentially chaotic environment, not just in a work capacity, but in their health and mental well-being.

Regardless of the business impact, it is still incumbent on the organization to continue to meet appropriate regulatory obligations, maintaining customer/patient security from both physical and data perspectives. To do this effectively, organizations and staff must communicate clearly and often. Organizations should ensure they share changing business and security requirements, policies, and procedures. In turn, staff must clearly communicate roadblocks to effective collaboration and workflow. And, both sides have to listen. Working together, organizations can enable staff to maintain a healthy, safe, productive, and secure work environment.

Key findings

Chameleons lack necessary internal defenses. They don't possess a poisonous bite and the majority move at an incredibly slow pace.

However, they've evolved some exceptional camouflage capabilities that protect them from predators. They can also change colour to send social signals or dynamically respond to their changing environment.

Key findings

NTT Ltd. analysed data from our managed security services, incident response engagements, application testing, and threat research teams. The analysis revealed information about attack trends, targeted technologies, tools, and techniques used by attackers. This information can help organizations manage threats and mitigate risks.

Global analysis

While commodity ransomware attack volumes have dropped, the success rate of targeted ransomware attacks is still high. The popularity of illicit coinmining has also dropped along with the value of digital currency.

Organizations have begun making advances in securing their environments, managing ransomware and coinmining activity, and are investing more in effective and repeatable incident response capabilities.

Industry	2019 Baseline	2018 Baseline
Technology ↓	1.64	1.66
Finance ↑	1.86	1.71
Business and Professional Services ↑	1.54	1.31
Education ↓	1.02	1.21
Manufacturing ↓	1.32	1.45
Healthcare ↑	1.12	1.03

Figure 1: Benchmark score by industry

Figure 1 shows comparisons between 2018 and 2019's benchmark scoring using the Cybersecurity Advisory service described more fully in the Cyber-resilience section of this report. Overall baseline scores have not progressed appreciably in the past year, but individual industries do show some small variations.

Small decreases in baseline scores are likely a result of poor prioritization which may indicate misallocated resources and potentially interferes with security's ability to deliver for the business. Small increases in the baseline tend to be related to improvements in visibility and strategy.

Figure 2 illustrates the gap between the current vs. the desired state of several industries. The difference between current and target state is one driven by aspiration, not necessarily where they need to be. Many business drivers, including cost, compliance, and resources, are all factors which may result in achieving less than the desired goals. In order to close the gap, each of these industries must ensure a constant focus is placed on maturity of processes, tools, and executive support.

Maturity level gap

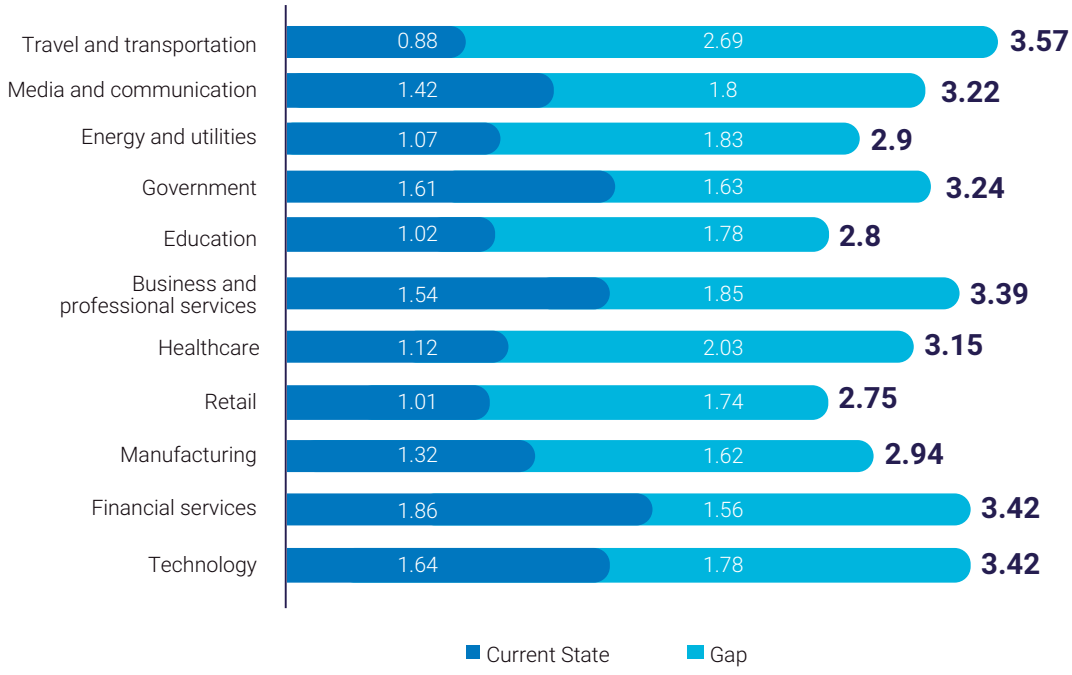

Figure 2: Maturity level gap

Botnets are comprised of multiple infected internet-connected devices used to carry out coordinated actions, such as sending spam or conducting distributed denial-of-service attacks. **Mirai, Echobot, and IoTroop are examples of botnets.**

Botnets such as Mirai and Echobot have advanced in automation, improving their propagation capabilities. Primarily aided by attacks leveraging default or hardcoded credentials, Mirai and variants targeted network backbone devices from several different vendors. Mirai and IoTroop are known for spreading through Internet of Things (IoT) attacks, then propagating through scanning and subsequent infection from identified hosts.

15% of all attacks observed. Additionally, attacks against Apache solutions were in the top seven vulnerabilities targeted in each industry, and the top five in each country analysed.

Based on NTT Ltd.'s observations Mirai and IoTroop lead in malware detections with more vulnerability scanning activity from these variants than any other family of malware. Attacks against Netis/Netcore, Linksys, and D-Link routers, as well as ThinkPHP, were commonly detected across most geographies and industries. Many of these attacks are directly related to activity from botnets like Mirai and IoTroop, including the high levels of vulnerability scanning activity detected globally.

Globally, organizations continue to experience high levels of malicious scanning focused on identifying Shellshock (CVE-2014-6271) vulnerabilities. Continued attacks against vulnerabilities such as HeartBleed (CVE-2014-0160) help make OpenSSL the second most targeted software technology with 19% of hostile activity globally. 17 vulnerabilities in OpenSSL identified in the last two years contributed to a constant focus of attacks against vulnerable implementations. As shown in Figure 3, OpenSSL was often the first or second most targeted technology. OpenSSL was also the most targeted technology in both the manufacturing and technology industries.

Apache products like Struts, Tomcat, and others, experienced 258 new vulnerabilities defined in the past two years. Apache software implementations were the third most targeted during 2019, accounting for over 15% of all attacks observed. Additionally, attacks against Apache solutions were in the top seven vulnerabilities targeted in each industry, and the top five in each country analysed.

Attacks targeting CMS platforms were also significant in this year's analysis. WordPress, Joomla!, Drupal, and noneCMS account for about 70% of CMS market share. They are also the target of approximately 20% of all attacks globally with the most targeted being a SQL Injection vulnerability (CVE-2019-9184) in Joomla!. Additionally, every region included two to four CMSs in their top 15 targeted technologies, and most countries included either Joomla! or WordPress in their top five.

Attacks targeting SSL by region		
Grouping	**Targeted technology rank**	**% of attacks**
Global	#2	19%
Americas	#2	10%
United Kingdom	#2	20%
Hong Kong	#1	67%
Australia	#2	21%

Figure 3: Global attacks against OpenSSL

Global key findings

- Technology was the most attacked industry in 2019 accounting for 25% of all attacks. Significant increases in application-specific and DoS/DDoS attacks, along with weaponization of IoT attacks contributed to technology becoming the most attacked industry. Technology was previously the second most attacked industry in 2017 and 2018.
- Nearly 55% of all attacks were application-specific attacks (33%) and web-application attacks (22%).
- Attacks targeting CMS suites accounted for 20% of all attacks.

31% of all attacks targeting the technology industry.

Global highlights

Technology was the most attacked industry accounting for 25% of all observed activity. As shown in Figure 4, application-specific attacks made up 31% of all attacks targeting the technology industry. Of all attacks targeting technology, over 15% of them targeted vulnerabilities allowing remote code execution (RCE).

Industry percent of global attacks	Percent of attacks for industry	Percent of exploit techniques for industry
Technology – 25%	Application Specific – 31% DoS/DDoS – 25% Network Manipulation – 13%	Remote Code Execution – 15% Buffer Overflow – 13% DNS Attack – 13%
Government – 16%	Application Specific – 44% Web Application – 15% Reconnaissance – 14%	Remote Code Execution – 32% Injection – 10% Port Scanning – 7%
Finance – 15%	Application Specific – 35% Web Application – 31% Reconnaissance – 14%	Injection – 16% Buffer Overflow – 10% DNS Attack – 9%
Business and Professional Services – 12%	Application Specific – 47% Reconnaissance – 18% DoS/DDoS – 15%	Remote Code Execution – 25% Flood Attack – 13% Port Scanning – 8%
Education – 9%	Web Application – 54% Application Specific – 20% Dos/DDoS – 9%	Injection – 52% Remote Code Execution – 8% Desktop App Exploit – 3%

Figure 4: Top global attack targets and types

Application-specific attacks target vulnerabilities in applications, including broken authentication and session management, insecure direct object references, lack of encryption for data at rest and in transit, escalation of privileges, and Trojanized or unpatched third-party components.

The top five targeted industries have been heavily targeted in previous years. Attacks against the web presence of organizations in these industries are common, as attackers attempted to either compromise public-facing applications, or compromise the underlying systems supporting web services. Organizations view vendor, supplier, or customer portals and external access as required services, and attackers are taking advantage of this, regardless of the industry. Application-specific attacks or web-application attacks were the most common attack type in all five of the top attacked industries, as well as in most industries analysed.

Industry	2019 Rank	2019 %	2018 Rank	2018 %
Technology ↑	1	25%	2	17%
Government ↑	2	16%	5	9%
Finance ↓	3	15%	1	17%
Business and Professional Services ↓	4	12%	3	12%
Education ↓	5	9%	4	11%

Figure 5: Industry comparisons

Figure 5 shows a comparison between the five most attacked industries in 2018 and 2019. Overall, the top five industries remained the same, though their order did change. Attack volumes increased across every industry from 2018 to 2019. Most changes in the order of the top five were mostly due to the increase in application-specific attacks and web-application attacks, or the relative decrease in DoS/DDoS attacks or service-specific attacks, which often tend to be more technical attacks.

The biggest changes in the top five attacked industries were in technology and government. Technology experienced nearly a 70% jump in overall attack volume. This was led by significant jumps in both application-specific attacks and DDoS attacks. Like most industries, application-specific attacks focused on technologies supporting the industry's web presence, most notably CMS systems and web technologies such as Microsoft's IIS, Joomla! and ColdFusion. DDoS attacks focused on OpenSSL, as well as a wide variety of available internet services and systems. The types of malware detected, most notably rats (jsp and gh0st) and web shells (China Chopper) suggest attackers are infiltrating technology organizations for persistent access. This is supported by high volumes of the zmeu and muieblackcat scanners, which are used to identify other vulnerable hosts from inside a compromised network.

Weaponization of IoT attacks against technology also contributed to the technology becoming the most attacked industry. While no single botnet dominated activity, analysts identified significant volumes of both mirai and IoTroop activity.

Targeting government organizations

Along with increases in the targeting of technology, attacks focused on government targets nearly doubled in 2019. Most notably, this included significant jumps in both reconnaissance activity and in application-specific attacks. Application-specific attacks tended to focus on the same technologies as most industries – CMS suites, along with supporting tools and applications. This has been helped by an increase in internet-delivered services designed to help citizens obtain regional or local assistance. Unfortunately, those same internet-enabled applications have provided additional opportunities to attackers.

Along with application attacks, regional and local governments have experienced significant impacts from denial of service and ransomware attacks. These attacks can be difficult to hide from customers, and smaller government offices often do not have the resources available to deal with significant outages. The automation and commoditization of these attacks appeared to have a direct effect on government organizations.

Automation affected more than just government organizations. As shown in Figure 6, the five most common attack types accounted for 88% of all attacks globally. Application-specific attacks comprised 33%, and web-application attacks made up 22% of all attacks. Attackers are maximizing the use of application-specific and web-application attacks, some of which are implemented into exploitation tools, or are automated.

The most common techniques attempted worldwide were RCE in 15%, and injection in 14%, of attacks. RCE attacks allow an attacker to execute their code on a targeted system with the privileges of a user on that system. Injection attacks can allow an attacker to submit unvalidated input to a vulnerable application and are often designed to extract data or execute code. Injection attacks are listed as the number one web-application security risk in the OWASP Top 10[2].

The Open Web Application Security Project (OWASP) **Top 10 is an awareness document for developers and web-application security** which defines consensus good practice for web applications.

Global attack types

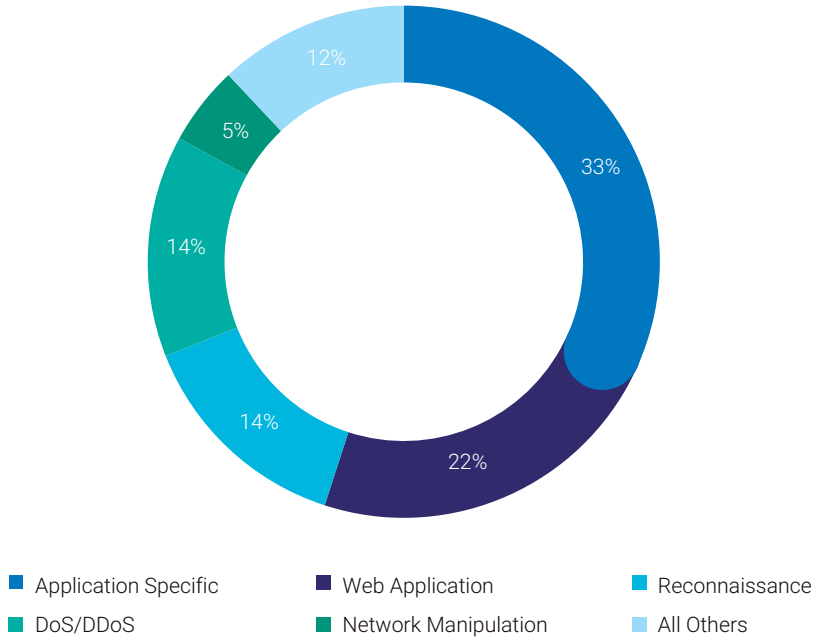

Figure 6: Global attack types

Malware has continued to become more complex and more effective. Multifunction malware is more common than ever, and attackers continue to deliver malware through phishing attacks, social engineering, malspam campaigns, and exploit kits. As seen in Figure 7, vulnerability scanners are the single most commonly detected malware component observed globally.

Malware family	Vulnerability scanner – 21%	Remote access trojan – 16%	Botnet – 11%	Trojan – 11%	Webshell – 10%
Malware variant	muieblackcat zmeu	jsp gh0st doublepulsar	IoTroop mirai virut	pmabot Ramnit zeroaccess	China Chopper Cknife C99

Figure 7: Global common malware variants and families

2 owasp.org/www-project-top-ten/

Americas analysis

The re-emergence of Mirai and derivatives has helped spread IoT attacks in a market which craves IoT but has not evolved to secure it effectively. News organizations report breach after breach, making breaches resemble the new norm. Attackers have directed attacks towards small and medium-sized businesses, and effectively spread ransomware into state and local governments.

The Americas were dominated by reconnaissance activity, likely for the same reason it affected global attacks; the automation of scanning in common malware like Mirai, Echobot, IoTroop, and derivatives.

Reconnaissance activity was followed by application-specific and web-application attacks. Overall, attacks were not unlike those in other regions, but the United States was one of only two countries (the other being South Africa) where the top type of malware detected was not some form of vulnerability scanner.

Americas key findings

- Joomla! was targeted more than any other application, accounting for 45% of all attacks.
- The most common type of malware in the Americas was the webshell family. China Chopper accounted for 54% of all webshell activity and was the second most detected malware.
- The single most detected malware in the Americas was WannaCry ransomware.
- The most attacked industry in the countries analysed was business and professional services (41%) followed by manufacturing (20%), technology (17%), and finance (15%).

45% Joomla! was targeted more than any other application, accounting for 45% of all attacks.

Americas highlights

While there was some variance by country, the most attacked industries in the Americas were business and professional services, manufacturing, and technology. As shown in Figure 8, attack types in business and professional services and manufacturing showed the expected application-specific and web-application attacks, as well as reconnaissance activity. Technology in the Americas was the only industry which identified network-manipulation as the most common type of attack. Network-manipulation attacks are often more advanced attacks which require greater skills or use more advanced tools. Attack volumes against technology and several other industries were high enough to make network-manipulation attacks the fourth most frequent attack type.

DoS/DDoS attacks were the fifth most common attack type, falling right at the global average of 14% of attacks, but nearly half of those DoS/DDoS attacks were directed at business and professional services organizations.

Top targeted industries	Top attack types
Business and Professional Services – 41%	Application Specific – 36% Reconnaissance – 32% Web Application – 16%
Manufacturing – 20%	Application Specific – 25% Reconnaissance – 20% Web Application – 13%
Technology – 17%	Network Manipulation – 48% Brute Forcing – 17% Reconnaissance – 16%
Finance – 15%	Reconnaissance – 29% Network Manipulation – 19% Web Application – 19%
Telecommunications – 6%	Reconnaissance – 92% Application Specific – 2% Web Application – 2%

Figure 8: Americas - industry details

Network-manipulation attacks target network protocols. These types of attacks typically include spoofing IP addresses and hijacking. **They are often used to bypass network-based security controls like intrusion-detection systems and firewalls.**

Attacked technology	Common technology vulnerabilities	Reported
Joomla!	CVE-2015-8562 – Joomla! RCE Vulnerability CVE-2019-9184 – J2Store Plugin for Joomla! SQL Injection Vulnerability	13 Dec 2015 26 Feb 2019
Apache	CVE-2017-9805 – Apache Struts RCE Vulnerability CVE-2018-9791 – Apache Struts RCE Vulnerability	15 Sep 2017 10 Jul 2017
OpenSSL	CVE-2016-6309 – OpenSSL Use After Free Vulnerability	26 Sep 2016

Figure 9: Americas targeted technology

Joomla!, Apache products, and OpenSSL were the three most targeted technologies. Figure 9 presents the vulnerabilities frequently detected for each technology shown. All these vulnerabilities are among the top 15 observed. Figure 9 also shows that only one of these five vulnerabilities is less than 2 ½ years old, and they all have patches available. Three of the vulnerabilities support RCE which allows an attacker remote interaction with the targeted device, and a fourth allows an attacker to execute SQL commands.

Webshell was the most popular malware family in the Americas, with China Chopper being the top detected web shell. Nearly every other region analysed showed vulnerability scanners were the most common type of malware identified.

The most detected malware was the WannaCry ransomware; China Chopper was second. Germany (18% of malware as ransomware) and the United Kingdom (12%), were the only countries which showed a higher percentage of ransomware than the United States (10%).

While other regions detected more IoTroop, Virut was more common in the Americas, which may account for increased levels of DoS/DDoS attacks in some industries.

Most common malware in the Americas	Malware type
WannaCry	Ransomware
China Chopper	Webshell
jsp	Remote Access Trojan
Ramnit	Trojan
Virut	Botnet
zmeu	Vulnerability Scanner
muieblackcat	Vulnerability Scanner

Figure 10: Americas most common malware

While not the most commonly detected malware family, vulnerability scanners were still the third most common. Zmeu and muieblackcat were the most common vulnerability scanners implemented by malware within the Americas.

Technology, manufacturing, government, and education were the top industries targeted in the Asia-Pacific (APAC) region, as detailed in the following APAC analysis.

Vulnerability scanners are programs which search computers, networks, and applications for specific vulnerabilities. Muieblackcat scans servers for PHP vulnerabilities while Zmeu scans for servers which are open to attacks through phpMyAdmin.

Asia Pacific analysis

The APAC region showed significant activity related to the technology and manufacturing industries – the design, development, and manufacturing of technical components and products. Tension in the region can impact operations and have an effect on the priority and attention provided for cybersecurity.

Attacks in APAC were considerably different than in other regions. While the second most attacked technology in Japan was Joomla!, Hong Kong did not show any CMS suites in their most commonly attacked technologies. Although OpenSSL was the second most attacked technology in Australia, it was the 14th most attacked in Japan.

APAC key findings

- DoS/DDoS attacks were more common than in other regions, regularly appearing in the top five common attack types (Australia #3, Singapore #4, and Japan #5).
- Web-application and application-specific attacks dominated the region. They were the two most common attack types in Japan and Australia, and application-specific attacks were the most common attack types in Singapore and Hong Kong.
- Attacks in Japan included three CMS platforms in the eight most targeted technologies. Joomla! was the most highly targeted CMS in every country analysed.
- IoTroop made up 87% of all botnet detections in Japan. Botnet activity, accounting for 32%, was the most common form of malware activity detected in Japan.

APAC highlights

As depicted in Figure 11, technology was regularly among the most attacked industry in many countries. Attacks against government, finance, and education also appeared with some regularity. As with the case of Benelux and Norway, Japan's reliance on the transport and distribution industry helped generate attacker interest. In most cases, the top three or four attacked industries were targeted in 80-85% of all attacks, meaning activity within other industries dropped off quite quickly.

87%

IoTroop made up 87% of all botnet detections in Japan. Botnet activity, accounting for 32%, was the most common form of malware activity detected in Japan.

Country	Top targeted industries	Top attack types
Japan	Technology – 29% Manufacturing – 25% Transport and Distribution – 13%	Web Application – 36% Application Specific – 23% Brute Forcing – 22%
Australia	Technology – 35% Government – 26% Finance – 13%	Application Specific – 40% Web Application – 20% DoS/DDoS – 19%
Singapore	Government – 38% Education – 29% Finance – 15%	Application Specific – 32% Brute Forcing – 21% Reconnaissance – 19%
Hong Kong	Manufacturing – 46% Technology – 25% Business and Professional Services – 23%	Application Specific – 46% Service Specific – 18% Reconnaissance – 17%

Figure 11: APAC select country details

Application-specific attacks dominated activities within APAC, followed by web-application attacks. Combined, these two types of attacks made up nearly 60% of all hostile activity across the countries analysed.

Attackers used DoS/DDoS attacks against identified targets in APAC at a rate higher than the global average, and about three times of the DoS/DDoS rate in EMEA. The reconnaissance rate in countries analysed in APAC was less than half the rate of reconnaissance activity globally. While Hong Kong and Singapore showed high amounts of reconnaissance, Japan and Australia were dominated by web-application, application-specific, brute-force, and DoS/DDoS attacks. Hong Kong had the highest share of application-specific attacks of any country analysed in the region.

Common technology attacked in APAC	Japan	Australia	Singapore	Hong Kong
Apache	1	3	1	12
Joomla!	2	8	15	
Netis/ Netcore	3	1		
Microsoft IIS	4	6	4	17
WordPress	5		11	
Oracle	6	13		
Drupal	8	12		
OpenSSL	14	2	6	1
jBoss	15	17		
Novell		4		

Figure 12: Commonly attacked tech in APAC

Reviewing these details reveals some technologies which were more commonly targeted. Apache products (i.e., Struts and Tomcat) **and Netis/ Netcore routers were common targets in multiple countries.**

Figure 12 includes a summary of commonly attacked technologies and their rank within each country. While some types of technology were heavily attacked in one country, another country may have showed a different result. For instance, OpenSSL was the most commonly attacked technology in Hong Kong, second in Australia, and 14th in Japan.

Reviewing these details reveals some technologies which were more commonly targeted. Apache products (i.e., Struts and Tomcat) and Netis/Netcore routers were common targets in multiple countries. The most commonly targeted vulnerability in Japan was Struts (CVE-2017-5638) and the most targeted vulnerability in Australia was OpenSSL (CVE-2017-3731). Both vulnerabilities have had patches available for over two years.

Conficker and IoTroop were the most commonly detected malware in APAC. Conficker was the most common malware in Australia, IoTroop in Japan, and pmabot in Singapore. While each country was affected by a different malware as their most common, much of the malware activity was observed in multiple countries within the region. Conficker, first detected in 2008, was the only malware observed with significant volumes in every country. Figure 13 shows which malware was observed in high volumes in which APAC countries.

Most common malware in APAC	Malware type	Japan	Australia	Singapore	Hong Kong
Conficker	Worm	X	X	X	X
IoTroop	Botnet	X			X
zmeu	Vulnerability Scanner	X	X		
muieblackcat	Vulnerability Scanner	X	X		
gh0st	Remote Access Trojan	X	X	X	
jsp	Remote Access Trojan	X	X	X	
China Chopper	Webshell	X	X		
pmabot	Trojan		X	X	

Figure 13: Most common malware APAC

Spotlight on: Emotet malware in Japan

The NTT-CERT performed research and analysis on the Emotet banking Trojan which was originally discovered in 2014. Since then, it has undergone surges in popularity as the malware evolved and detections adapted. Emotet is modular and includes worm-like capabilities, and it has also undergone a series of stealth modifications.

In Japan, infections of Emotet malware have grown since September 2019, along with the global increase in Emotet activity in that timeframe. As part of this latest surge, approximately 3,200 organizations have been damaged by the malware between September 2019 and February 2020. This includes the infection of about 2,000 organizations since January 2020[3]. This increased infection rate is supported by alerts of suspicious email which appear to be related to Emotet.

Email supporting Emotet has often been disguised as an invoice, a receipt or a download link to a coupon related to online shopping. Subject lines such as 'Payment Remittance Advice' or 'Overdue invoice' are common for Emotet emails. Attackers have also used a current topic of interest, such as a bonus payment or a special Christmas sale. Since 28 January 2020, Emotet email has been detected with a subject line including[4] 'COVID-19'.

If a system is infected with Emotet, the malware can exfiltrate SMTP server credentials, authentication information of email, web browsers, and network accounts, and more. Moreover, Emotet takes information from harvested email and systems to spread the infection by using spambots to send additional malicious emails. Emotet can use this technique to spread itself around the organization, as well as to external recipients.

Emotet email which is disguised as a reply to a sent email can indicate a compromised system, as it typically uses harvested information to build the email. Since the attack email appears to be an actual reply from someone the recipient knows, people who receive it are at increased risk of being successfully tricked. Analysts have regularly observed Emotet 'reply' emails in Japan since March 2019.

NTT Ltd. analysts observed Emotet emails in September 2019 and NTT-CERT issued a security alert regarding this malware[5]. The following attack email impersonated a reply to an email thread.

[3] *https://blogs.jpcert.or.jp/en/2019/12/emotetfaq.html*

[4] *https://www.ipa.go.jp/security/announce/20191202.html#L12 (in Japanese)*

[5] *http://www.nsc.ecl.ipxp/article/143883 (in Japanese)*

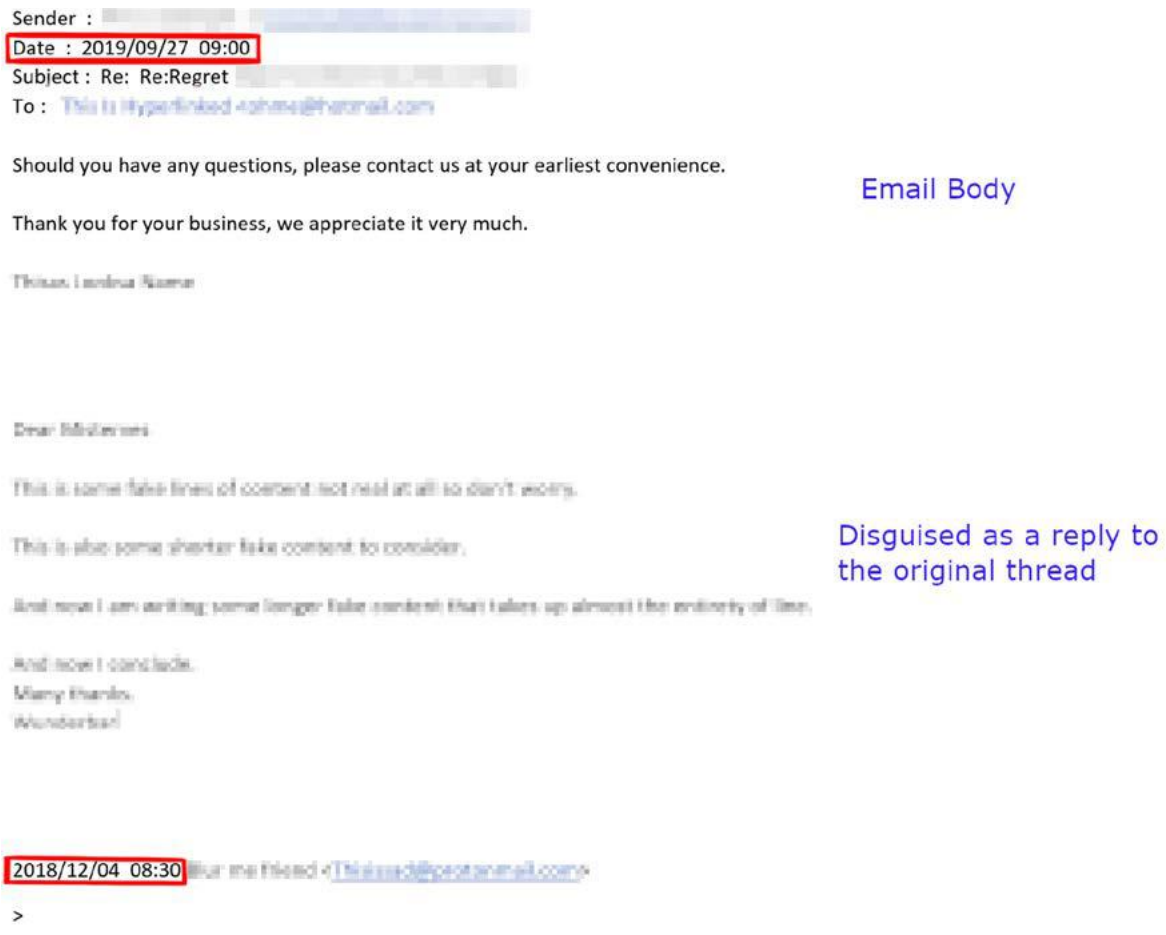

Figure 14: Observed sample Emotet email

In this most recent cycle of Emotet, attackers may attach a malicious Word document, include a URL to a malicious Word document, or a PDF file which contains the URL for downloading the malicious Word document, often from a compromised WordPress site. Fortunately, if the targeted system is configured to automatically disable macros by default, Emotet will not activate and the end system will not be infected, unless that user explicitly clicks the 'Enable Content' button displayed upon opening the attached or linked Word document. If the victim clicks the 'Enable Content' button on the disguised email, Emotet will be installed and activated.

Emotet commonly installs additional malware during an infection. In Japan, some Emotet-infected systems have downloaded banking malware such as Ursnif and Trickbot. In some other countries, Emotet has downloaded ransomware such as Ryuk[6]. The variety of techniques and follow-on infections combine to help make Emotet a persistent malware with the potential to have significant impact on organizations into the future.

While Emotet was found in every region, Trojan horses were the most common forms of malware in EMEA.

[6] *https://www.jpcert.or.jp/at/2019/at190044.html (in Japanese)*

Europe, Middle East, and Africa analysis

Events in Europe, Middle East, and Africa (EMEA) were affected by the requirements to meet Global Data Protection Regulation (GDPR) compliance. As is the case with any significant compliance activity, GDPR initiatives helped reinforce maturing security programs, and in some cases, they distracted organizations from advancing their efforts.

Hostile activity in EMEA resembled those of other regions with notably high levels of web-application attacks, application-specific attacks, and a variety of reconnaissance activity. Denial of Service (DoS) and brute-force attacks spiked in some industries and countries, but overall resembled those observed globally. Attackers attempted exploits against Cisco devices with greater regularity than other regions.

40% Reconnaissance activity was the most common form of activity in EMEA, often accounting for more than 40% of observations.

EMEA key findings

- Reconnaissance activity was the most common form of activity in EMEA, often accounting for more than 40% of observations. Reconnaissance was pronounced in Sweden (67%), the United Kingdom (50%), Benelux (50%), and Germany (47%).
- Exploit attempts against CVE-2018-15454, a vulnerability in Cisco ASA, were common across EMEA, dominating targeted vulnerabilities in several countries. It was the most targeted vulnerability in Benelux (50%) and South Africa (35%), and second most targeted vulnerability in Sweden (22%).
- CMSs were common attack vectors in EMEA, with several countries including multiple CMSs in their list of technologies most commonly attacked.

EMEA highlights

While targeted industries varied by country, the most commonly attacked industries in EMEA were finance, business and professional services, technology, manufacturing, and retail. Some countries experienced attacks which were strongly related to industries prevalent within their borders, like transportation and distribution in Norway and Benelux, which helps reinforce the fact attackers tend to migrate towards targets which interest them the most – just because you are not in a 'top five' industry, it does not mean attackers are not targeting your organization.

Country	Top targeted industries	Top attack types
United Kingdom and Ireland	Manufacturing – 29% Technology – 19% Business and Professional Services – 17%	Reconnaissance – 50% Web Application – 22% Brute Forcing – 12%
Sweden	Pharmaceuticals – 62% Finance – 22% Telecommunications – 12%	Reconnaissance – 67% Application Specific – 12% Brute Forcing – 11%
Germany	Technology – 51% Manufacturing – 21% Finance – 11%	Reconnaissance – 47% Service Specific – 13% Application Specific – 13%
Norway	Business and Professional Services – 45% Retail – 19% Transport and Distribution – 15%	Application Specific – 36% Web Application – 29% DoS/DDoS – 16%
Benelux	Technology – 33% Transport and Distribution – 31% Manufacturing – 22%	Reconnaissance – 50% Application Specific – 18% Web Application – 15%
South Africa	Insurance – 50% Finance – 44% Retail – 3%	Web Application – 66% Application Specific – 27% DoS/DDoS – 4%

Figure 15: EMEA select country details

As can be seen in Figure 15, reconnaissance accounted for over 40% of hostile activity in many EMEA countries, including Germany (47%), Benelux (50%), the United Kingdom & Ireland (50%), and Sweden (67%). Levels of web-application and application-specific attacks were close to levels of reconnaissance, and both were in the top four attacks in every country analysed.

As with other regions, web-application and application-specific attacks were common throughout industries and countries within EMEA. Additionally, a vulnerability in Cisco ASA Session Initiation Protocol inspection engine (CVE-2018-15454) was highly targeted in several countries.

Several countries included multiple CMS suites in their list of commonly attacked technologies. In Sweden, attackers targeted a noneCMS input validation vulnerability (CVE-2018-20062) more than any other vulnerability. As depicted in Figure 16, Joomla! and WordPress were the CMS suites most commonly attacked, with the majority of the CMSs appearing in the top ten attacked technologies in the specified countries.

Country	CMS commonly attacked
Norway	WordPress
Germany	Joomla!, WordPress, Magento, Drupal
United Kingdom and Ireland	WordPress
Benelux	WordPress, Joomla!, noneCMS, Drupal
Sweden	Joomla!, WordPress, Drupal, noneCMS
South Africa	Joomla!, Drupal

Figure 16: Commonly attacked CMS suites by country

Similar to the global analysis, vulnerability scanners, testing tools, and malware appeared in the top five most common malware and attacker tools in EMEA. As shown in Figure 17, the Trojan Horse pmabot was the most commonly detected malware in the analysed countries in EMEA, followed closely by the IoTroop botnet. South Africa was the only country other than the United States which did not show vulnerability scanners as the most commonly detected malware variant. At 18% of all malware, Germany showed the highest rate of ransomware detection among any country analysed.

Most common malware in EMEA	Malware type
Pmabot	Trojan Horse
IoTroop	Botnet
Sqlmap	Vulnerability Scanner
Nmap	Vulnerability Scanner
muieblackcat	Vulnerability Scanner

Figure 17: Most common malware in EMEA

As with other regions, web-application and application-specific attacks were **common throughout industries** and countries within EMEA.

In this most recent cycle of Emotet, attackers may attach a malicious Word document, include a URL to a malicious Word document, or a PDF file which contains the URL for downloading the **malicious Word document, often from a compromised WordPress site.**

Cyber-resiliency

With a range of bright colours — yellows, oranges, reds, greens, blues — poison dart frogs have developed elaborate designs to warn potential predators to 'stay away'.

This species is at risk of extinction, and without these evolutionary investments, the frog would be unable to defend itself from attacks.

What is cyber-resiliency?

Cyber-resiliency is the ability of an organization to continuously deliver products and services despite cyber-related events impacting normal operations. This belief embraces the concept which businesses must prepare for, prevent, respond, and successfully recover to secure state without disruption or degradation to normal delivery expectations.

Security must be considered as a core business function, designed to protect resources and implemented to mitigate risk. Organizations must implement infrastructure, applications, and operations which are secure by design — so including security is a key and conscious decision in the approach to designing business solutions end-to-end. Implemented properly, cyber-resilience brings together information security, business continuity, and organizational resilience, ensuring a secure by design approach. Security best practices must be considered and built into policies, procedures, infrastructure, and applications, as well as provide appropriate visibility into, and control over these components, regardless of normal or adverse activity.

How does an organization approach cyber-resiliency?

A good place to start is understanding what it is the organization is trying to protect. An organization's ability to identify key intellectual property, critical assets, data, and core delivery functions are fundamental to its capability to design an appropriate infrastructure and overarching security program. Although there are several risk assessment methodologies organizations may consider, the foundational concept is to address the following questions:

1. What data and capabilities are the most important for the business?
2. What are the systems involved with supporting the data and capabilities?
3. How will the organization and its customers use the data and services provided?

What do we mean by 'secure by design'?

Cybersecurity can no longer be an afterthought. We have all seen the impact that a successful cybersecurity attack can have on a business: the damage to brand reputation, trust, and profitability can take years to repair.

'Secure by design' means being cybersecurity conscious at all levels of the business. This involves:

- Security as a key tenant of an organization's overall business strategy.
- A security strategy that is aligned to what the business wants to achieve, as well as the businesses' risk-tolerance.
- An intelligence-driven cybersecurity posture that enables businesses to be agile in the face of a changing threat landscape and technology ecosystem.
- Building-in security (rather than bolting on) to digital programs, be it:
  - A secure and intelligent infrastructure (network, data center, clouds).
  - A secure and intelligent workplace (employees, buildings, customer experiences).
  - Secure and intelligent business transformation and innovation initiatives (such as IoT or OT, blockchain, DevSecOps).

Security must be considered as a core business function, **designed to protect resources and implemented to mitigate risk.**

With the information, an organization can begin to define a comprehensive security program which includes the policies, development controls, processes, technologies, and training as well as components of network design, application development, and deployment.

This is not a simple process; however, organizations can reduce complexity by implementing a framework to support definition and management of an active security program. The National Institute of Standards and Technology (NIST) Cybersecurity Framework[7] can be a great resource for organizations to leverage while building the components of a secure infrastructure.

As described by NIST[8], 'The Framework is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.'

The framework defines accepted and effective business practices which have been refined over the several decades of information security practice management. The framework's security and privacy controls are outcome-based, rather than end-goals in themselves, and integrate risk management with cybersecurity for the design of the security and privacy controls of an organization. While the framework was originally intended for use in protection of critical infrastructure, it can be applied to any organization wishing to strengthen its cyber-resiliency. The framework builds upon the following core focus areas:

[7] *https://www.nist.gov/cyberframework*

[8] *https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics#framework*

Area	Description
Identify	Build an understanding of the data, infrastructure, people, and applications the organization needs to protect.
Protect	Implement the elements of security which assist in providing a secure cyber environment for our business.
Detect	Establish the organization's capability to detect cyber events.
Respond	Determine the organization's response should an event occur.
Recovery	Plan for how the organization can minimize the time it takes to recover from a cyber event.

Figure 18: Overview of the NIST Cybersecurity Framework core focus areas.

When exercised properly, every initiative within your organization includes analysis and planning at each core function listed above. The importance of the framework's characteristics is in the alignment of its functions with your business strategy. Profiles are used to identify the implementation, standards, and practices for each given implementation scenario. The profiles help you understand either where your business is today, where you want it to be in the future, and to establish both, so you are aware of the gaps which are in danger of preventing you from reaching your desired level of implementation of operational and security controls.

Ultimately, the security controls designed to support a resilient organization are generally recognized good practices. The organization needs to ensure the implemented technologies and controls support not only the objectives of an application or operational element, but of the entire organization.

How does an organization know if they have reached an effective degree of cyber-resiliency?

Cyber-resilience can be difficult to achieve but stakeholders in the enterprise are required to be focused on reaching that goal. Senior leadership must be vigilant in supporting security initiatives and the resources needed to achieve and maintain a cyber-resilient state. Leadership should consider that effective cyber-resiliency is not simply deploying individual technologies to address specific threats, but rather is being able to identify vital assets and how current security measures relate to them. Reducing downtime and recovery will significantly reduce financial losses, meet legal and regulatory requirements, and protect the organization's brand and reputation.

Part of building cyber-resilience must include development of Key Performance Indicators (KPIs) to measure performance against expectations or desired results. Red and blue team exercises can also be a great way of assessing how an adversary would target your organization, and how well your people, processes, and technologies perform in maintaining your security posture. These indicators and assessments should be used to drive improvements in mean-time-to-detect, mean-time-to-respond, and restore. Lessons learned should serve as a continuous feedback loop in capturing and applying incremental improvements to the cybersecurity program. This approach will demonstrate the return on security investment and how it supports and aligns with the business mission.

NIST framework

Organizations can evaluate their efforts by comparing current capabilities against the defined tiers built into the NIST framework. The tiers help identify how your organization views cybersecurity risk and evaluate the processes implemented to manage the risk. Each tier is evaluated in part by degrees of Risk Management Process, Integrated Risk Management Program, and External Participation. High level descriptions of the four tiers are described below:

Tier	Description
Tier 1: Partial	The organization's risk management capability is not formalized. Limited understanding of cybersecurity risk across the organization. Does not understand external impact and dependencies. None or limited collaboration and use of intelligence to manage risk and unaware of supply chain risks.
Tier 2: Risk informed	The organization's risk management practices are approved but there may limited direction for the program shared across the organization. Understands external impact and dependencies. Collaborates and uses intelligence to manage risk and is aware of supply chain risks. Has general guidance in place but capabilities may not be to a degree of repeatability which is consistent.
Tier 3: Repeatable	The organization's risk management practices are approved and shared as official policy. An organization-wide program exists which continually addresses cybersecurity risks. Understands external impact and dependencies and actively collaborates by sharing and receiving intelligence and uses intelligence to manage risk. Aware of supply chain risks. Can manage risks in a consistent manner.
Tier 4: Adaptive	The organization leverages experience from past events and can adapt to cyberthreats quickly. Cyber risks are understood and evaluated in similar context to financial risks. Collaborates in real-time by sharing and receiving intelligence, uses intelligence to manage risk, and is aware of supply chain risks. Can manage risks in a consistent and repeatable manner with a high degree of success.

Figure 19: The tiers built into the NIST Cybersecurity Framework

Benchmarking cyber-resilience

The NTT Cybersecurity Advisory[9] assessment focuses on business outcomes with a modular framework. The framework spans the entire lifecycle of security, developing a strategy aligned to your organization's business needs, optimizing existing security controls, and designing comprehensive next-generation enterprise security architecture, policies, and framework.

This view of an organization's capabilities is a key part in identifying gaps in its ability to become cyber-resilient.

The comprehensive evaluation and transformational planning capability assesses maturity across an organization in several areas including:

Security vision and strategy	Executive level support, documentation and communication of the security strategy and architecture that is aligned to the business needs
Information security framework	Compliance, policies and standards, security domain modelling, data classification, and roles & responsibilities
Risk management	Risk assurance, asset management, threat identification & management, and vulnerability identification & management
Operations	Operations management including asset management, change control, incident management, vulnerability remediation, as well as governance, risk, and compliance measurement and reporting
Applications	Application security including source code analysis, application sand boxing, application container security, cloud access security brokers, and web application firewalls
Devices	Digital workplace security including architecture, mobile device management, identity & access management, and privileged access management
Infrastructure	Digital infrastructure security covering virtual & physical networking & workloads, threat management, security information & event management, infrastructure protection, and deception technologies

Figure 20: Areas assessed in the comprehensive evaluation

The process evaluates capabilities and evaluates current vs. future maturity levels based on an organization's processes, metrics, and tools. These maturity levels are identified as Non-Existent, Initial, Repeatable, Defined, Managed, and Optimized.

[9] *https://hello.global.ntt/en-us/products-and-services/consulting-services/security-consulting-services*

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 21: Maturity levels defined in the Cybersecurity Advisory

The following chart depicts the level of engagement observed by organizations across industries.

Cybersecurity Advisory engagements by industry

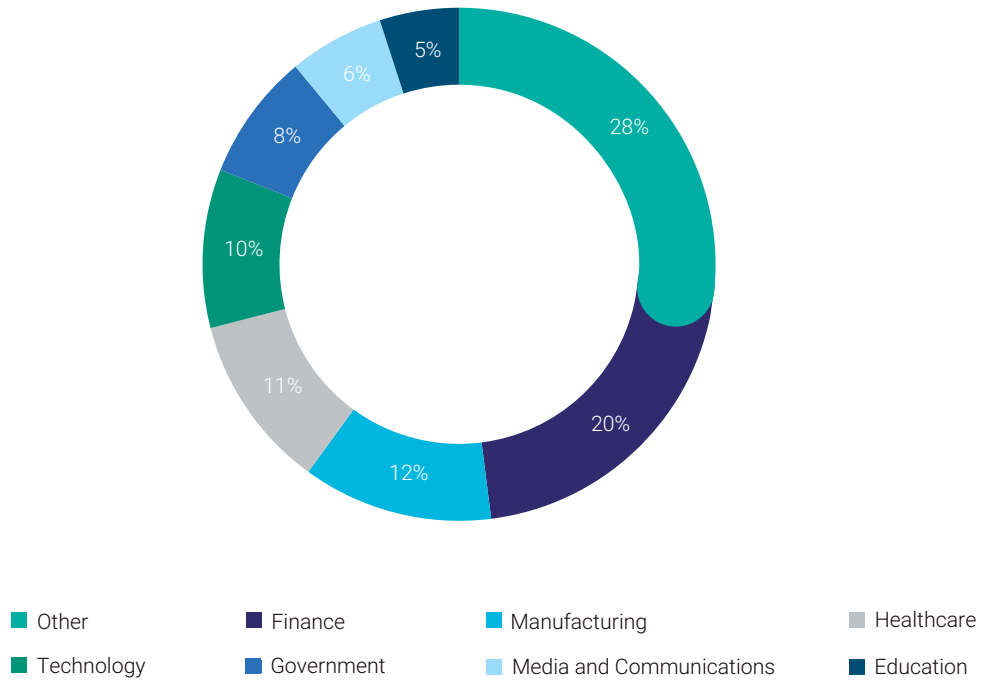

Figure 22: Cybersecurity Advisory engagement by industry

Throughout the report we will highlight some of the key findings based on the benchmark data and will include those details within the industry analysis sections.

Cyber-resilience recommendations

Integrating cybersecurity processes from the outset can strengthen digital transformation projects. Organizations must understand cyber threat actors have the advantage of time, robust tools, and the element of surprise. In assuming a breach, organizations will need to prepare, manage, respond, and recover to their desired state, and do so rapidly. To achieve this, some foundational concepts must be well planned and executed:

- **Develop** a cybersecurity strategy and ensure proper leadership support.
- **Use** a common language of risk while aligning security with business objectives.
- **Establish** the optimal security mindset and ensure all employees are aware they have a role in the success of the organization's security program.
- **Identify** and map risks to critical assets.
- **Design**, build, and deploy solutions which are difficult to attack and are 'secure by design'.
- **Secure** the foundation and do not undervalue the foundations of security. Get the basics right first and build additional capabilities upon the strong foundation.
- **Implement** appropriate security monitoring to reduce adversary dwell time.
- **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.

An organization must strive to reduce the complexity of operational models to the extent possible. An organization's cyber-resilience plan is secure by design when cybersecurity solutions and processes are embedded into the fabric of the business to secure digital assets and minimize risk. It must be integrated from the outset and embedded as a core value across the organization – represented as a baseline requirement, directly affecting processes, technology, policies, and people. Unfortunately, an organization might not really know it has achieved cyber-resilience until it has survived that inevitable cyberattack, but the organization must do its best – using all resources to maximize its resiliency, including cybersecurity experts – to embed cyber-resilience and embrace secure by design ideologies.

The following industry specific reports show analyses of threats uniquely facing each industry and will implicitly show how a cybersecurity program which is resilient and secure by design can help better position organizations to protect their data.

> An organization's cyber-resilience plan is secure by design when cybersecurity solutions and processes are **embedded into the fabric of the business to secure digital assets and minimize risk.**

Integrating cybersecurity processes from the outset can **strengthen digital transformation** projects.

Focus on industries

Fish have evolved to swim in ‘schools’ to better protect themselves from predators, improve foraging and swim more efficiently.

Schooling requires coordinated body positions and synchronized movement. It is an intricate, meticulous, and highly-skilled motion, that enables the fish to stay safe from predators – proving there is safety in numbers.

Focus on industries

Globally, attacks, techniques, and tools used by attackers followed some recognizable themes. Application-specific and web-application attacks were, globally, the two most common attack types.

The most common malware family observed, globally, was that of vulnerability scanners. Geographies varied somewhat from global observations – on attack types and in observed malware. NTT Ltd. observed even more differences when that analysis included observations of activities within specific industries.

Focus on industries

This section of the report includes more detailed analysis of attacks, tools, techniques, and malware used in the following five industries:

- Technology
- Retail
- Finance
- Healthcare
- Manufacturing

Each industry section contains important observations, findings of particular interest, and relevant GRC details. Each industry also includes a summary of analysis related to NTT Ltd.'s Cyber Security Assessment maturity model, and a summary of analysis from WhiteHat Security's application testing services.

WhiteHat Security results are based on the results from WhiteHat Sentinel Dynamic tests of millions of applications running in both production and pre-production environments. Scan results show as the likelihood that applications running in the industry environment will have an exploitable vulnerability. Additionally, if the successful exploitation could lead to attacker control or remote code execution, the identified vulnerability is identified as 'critical'.

Each industry also includes a targeted set of recommendations based on the MITRE ATT&CK framework appropriate for the types of detections identified for that industry.[10]

71% Of the top 20 targeted CVEs, attacks on OpenSSL accounted for 71% and attacks on Joomla! accounted for 28%. All other targeted vulnerabilities accounted for about 1% of hostile activity.

Technology Industry

Technology is one of the fastest moving industries, where small advances in research and development can easily lead to huge jumps in competitive advantage. As such, technology organizations spend significant amounts of economic and mental capital on the development of new tools, systems, services, and technical solutions. These organizations are often the most attractive target for investment in any economy because of the potential return on that investment.

Targeting the technology industry

Organizations in the technology industry often maintain large amounts of sensitive data. They tend to function in a collaborative environment and are often pathways to other industries as they provide business enablement capabilities. Attackers wishing to gain a competitive advantage, or shrink a competitive disadvantage, often target these organizations to steal insider information such as technical secrets. Historically, this targeting includes establishing long-term access in the infrastructure of technology organizations, the identification of account details (systems, usernames, and passwords) and the subsequent exfiltration of sensitive internal data. Significant increases in application-specific and DoS/DDoS attacks, along with weaponization of IoT attacks against technology contributed to technology becoming the most attacked industry in 2019.

Recent regulations such as the EU's GDPR have been at least partially designed to help control the amount of sensitive, private information technology companies retain about their customers, and give control of that information back to those consumers.

NTT Ltd. researchers identified that OpenSSL and Joomla! accounted for 99% of vulnerabilities targeted in the technology industry. Of the top 20 targeted CVEs, attacks on OpenSSL accounted for 71% and attacks on Joomla! accounted for 28%. All other targeted vulnerabilities accounted for about 1% of hostile activity.

[10] *https://attack.mitre.org/*

Technology – Cybersecurity advisory scoring

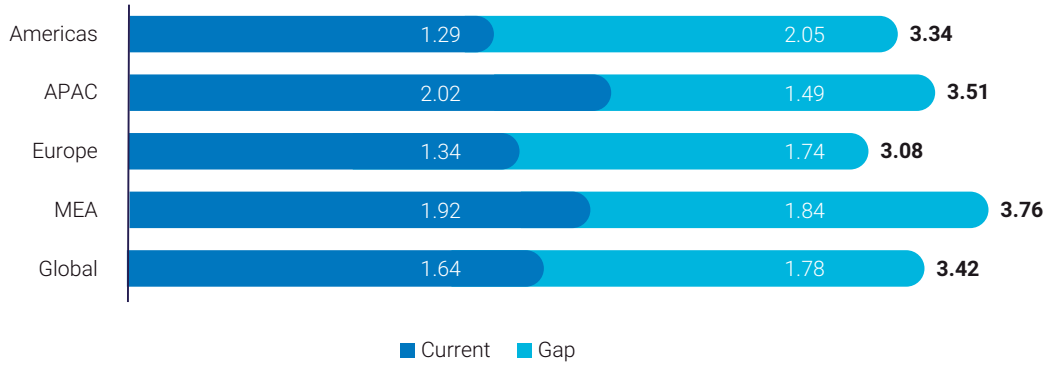

Figure 23: Technology - Cybersecurity Advisory scoring

As shown in Figure 23, the technology industry's average baseline maturity within the Cybersecurity Advisory scoring remained consistent with a score of 1.66 in 2019 to the most recent score of 1.64 in 2020. Organizations within APAC lead with an average maturity score of 2.02. MEA showed the next highest maturity score with an average of 1.92. In the Americas, technology's most mature subcategory was a score of 1.49 in Security Vision and Strategy, the Americas performed poorly in Information Security and Risk Management. Focusing on compliance, data classification, and risk management must be a priority for organizations to excel in these areas.

Activity against technology was marked by three main attack types:

1. Consistent denial of service attacks against OpenSSL and other internet services;
2. Application-specific attacks against Joomla! and other web technologies; and
3. IoT attacks lead by mirai and IoTroop.

Top attack types	Top vulnerabilities targeted by CVE number	Top products targeted	Top malware categories
Application Specific – 31% Dos/DDoS – 25% Network Manipulation – 14%	CVE-2017-3731 (OpenSSL) – 71% CVE-2015-8562 (Joomla!) – 28%	OpenSSL – 71% Joomla! – 28%	Trojan/Dropper – 63% Virus/Worm – 17% Ransomware/Fakeware/ Dialers – 9%

Figure 24: Top targeting in the technology industry.

Spotlight on: Two vulnerabilities

The technology industry faced an extremely focused targeting of vulnerabilities. The OpenSSL vulnerability CVE-2017-3731 and the Joomla! CMS vulnerability CVE-2015-8562 accounted for 99% of targeting. Successful exploitation of the OpenSSL vulnerability, which was disclosed in May 2017 and given a CVSS score of 7.5, allows an attacker to crash a server or client by causing it to perform an out-of-bounds read. Successful exploitation of the Joomla! vulnerability, which was disclosed in December 2015 and given a CVSS version 2 score of 7.5, allows an attacker to execute arbitrary PHP code via the HTTP User-Agent header in Joomla! versions 1.5.x, 2.x, and 3.x before 3.4.6 through a PHP object injection attack.

Due to the high attacker focus on these two vulnerabilities, organizations in the technology industry must ensure they have mitigations in place to prevent exploitation. For these vulnerabilities, this includes proper patch management. For any targeting of CMS suites, organizations should pay particular attention to the proper configuration of the CMS services, including the use of strong passwords and removal of default passwords.

Spotlight on: Malware in technology

The technology industry had the highest rate of detected ransomware of any industry. NTT Ltd. researchers found 9% of all threat detections were ransomware; no other industry showed detections for this malware category above 4%. WannaCry ransomware was the most commonly detected variant, accounting for 88% of all ransomware detections. WannaCry spreads through the EternalBlue exploits found in unpatched versions of Windows Server Message Block (CVE-2017-0144), which was patched in March 2017 (with Microsoft Security Bulletin MS17-010).

Additionally, NTT Ltd. found 23% of detected malware belonged to the RAT malware family. Of these detections, 51% were the jsp RAT variant and 30% were the gh0st RAT variant. The presence of these RATs suggests threat actors are seeking to gain access to organizations in the technology industry to maintain persistence and exfiltrate sensitive information over prolonged periods of time, just as they have done historically.

Governance, risk and compliance

The GDPR of 2018, the California Consumer Privacy Act of 2019, Singapore's signing of its Cybersecurity Bill into law in February 2018, Thailand's Personal Data Protection Act of 2019, and the 2018 updates to the Australian Privacy Act were five relatively recent additions to compliance and regulatory requirements. Additionally, on 23 January 2019, Japan's Personal Information Protection Commission (PPC) determined the GDPR has equivalent data protection standards as its Act on the Protection of Personal Information (APPI). The EU likewise determined equivalency between the APPI and GDPR, allowing for the transfer of personal information between Japan and the EU.

It appears likely additional privacy laws will be enacted (such as a federal privacy act in the United States and India's Personal Data Protection Bill), if not in 2020, soon after, designed to add additional requirements for organizations to protect the security of data and privacy of customers. If an application also processes payments, then PCI will also be a concern.

> WannaCry is a wormable ransomware variant which first emerged in May 2017. **Although patches are available, WannaCry infections continue and researchers** have found variants of the ransomware circulating.

One act currently going through the United States Senate is the Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act – designed to force large tech companies to make the user data they maintain portable and services interoperable with other platforms. The goal is to enable end users to help manage their own privacy and account settings.

Although no regulations have been passed at this time, there have been movements to regulate some technology companies with antitrust legislation to limit their ability to offer horizontal services in the same market. Self-regulation seems more likely in the short-term, as companies like YouTube announced a stricter anti-harassment policy, and Facebook announced it would invest USD 130 million to help determine how to filter objectionable content.

Application security analysis

The technology industry has the lowest performance of all industries in this focus, with an average of over 12 serious vulnerabilities per site. This industry also has the most varied set of applications from a diverse set of organizations, including short-handed startups as well as tech giants.

Companies in this industry usually aren't lacking in engineering talent. If their security teams can work together with engineering teams to jointly develop processes to build security into the culture, they will likely see a drastic reduction in the number of vulnerabilities which make it through the process into production.

Figure 25 shows highly rated vulnerabilities, along with the probability they will impact the organization. The 'Likelihood of Any Exposure' is the likelihood that vulnerability exists in the organization in a form which could lead to some level of compromise or exposure. The 'Likelihood of Serious Exposure' is the chance that the existence of that particular vulnerability will lead to a serious exposure such as a compromise or breach, which includes outcomes such as the compromise of sensitive data, the execution of remote code, or the takeover of the supporting platform.

Top serious vulnerabilities	Likelihood of serious exposure	Likelihood of any exposure
Cross Site Scripting	23%	25%
Insufficient Transport Layer Protection	13%	92%
URL Redirector Abuse	9%	10%
Cross Site Request Forgery	8%	8%
Information Leakage	6%	66%

Figure 25:Technology's likelihood of exposure to top serious vulnerabilities

Application exposure

When considering the vulnerabilities in their exposed systems, the technology industry unfortunately is amongst the worst performing. This is most likely due to the pressure to keep up - case of quantity vs secure quantity. Many of these companies are staffed with developers who are under pressure to field products or implement rapidly, and unfortunately have not had proper training in secure coding and application development techniques.

A commitment to DevSecOps can help these teams tremendously. A commitment to agile-like development styles and continuous integrations and automations are a must-have for companies in this industry. Fitting application-security into this model will help these teams continue to iterate quickly, while improving the organization's ability to seamlessly introduce security into their processes, making security a fundamental building block for the organization.

The number of URL Redirect Abuse, cross site scripting, and cross site request forgery findings all share similar components of issues. Applications using JavaScript must be tested heavily for spaces in the application which a user can edit/modify/replace. Basic application security training can help developers learn to spot these issues before their code hits production, improving the speed with which applications can be developed, implemented, and successfully tested.

Don't forget stored information. These sites will likely contain a profile aspect, where the user can add their own content, from photos (file upload) to a description of themselves, and other items. This is a hotbed for adding malicious injections.

Recommendations

Security frameworks containing standard recommendations exist to help organizations mitigate risks. NTT Ltd. has conducted consulting engagements and, in the course of providing guidance to our clients, found the MITRE ATT&CK framework to be robust and provides excellent information to help organizations address cybersecurity threats. As it is a strong resource, NTT Ltd. has chosen to align our suggestions for mitigation recommendations:

Mitigation	MITRE ATT&CK ID	Description
Update Software	M1051	Conducting regular scans looking for vulnerabilities in externally facing systems, establishing procedures to patch systems rapidly if a critical vulnerability is discovered or disclosed, and instituting a patch schedule for non-critical vulnerabilities.
Antivirus/ Antimalware	M1049	Employing malware detection platforms using heuristic detection. Ensuring virus definitions are up to date. Employing network/host intrusion prevention systems, detonation chambers, and antivirus software to stop infected documents from executing malicious payloads.
Filter Network Traffic	M1037	Filtering network traffic to identify non-standard protocols and to stop the use of unnecessary protocols across the network boundary.

Figure 26: Recommendations for the technology industry

Just like the technology industry, finance faced challenges in application-specific attacks. In the following section, we discuss the impact attacks on their web presence had on the finance industry.

Finance industry

The finance industry has a unique risk profile due to the value of its data, the frequency of attacks against the industry, and the security controls the industry has in place. Attackers tend to view the industry as a target rich environment containing personal and financial data which can be sold in the criminal underground or exploited directly for fraud. Attackers particularly target banking and financial service organizations with focus on credit card companies. Due to the finance industry's heavy security apparatus, attackers have sought most often to conduct quick and stealthy attacks.

Targeting the finance industry

Financial organizations maintain large amounts of valuable data. To support controlled access to this information, financial applications tend to be large and complex, and some of these applications are exposed to the public in web-facing applications designed to support customer portals. In fact, these web applications are the primary form of access for most financial customers. Attackers are highly motivated to take advantage of these customer portals. Application-specific attacks and web-application attacks made up a higher percentage of attacks against finance than any other industry. The value attackers place on this data is demonstrated in the consistent targeting of financial organizations, year after year. Attacker also highly target financial organizations with information stealers, keyboard loggers, and Trojans which help grant them extended access within the target environment, and identify usable account credentials.

72% NTT Ltd. researchers identified Apache, Microsoft, and GNU products as accounting for 72% of vulnerabilities targeted in the finance industry.

NTT Ltd. researchers found 83% of all malware detections were for Trojan/droppers. The finance industry is highly regulated with requirements around protecting consumer information, consumer and organizational financial details, and protecting the integrity of financial markets, including protections against fraudulent activities and money laundering. While some of the applicable legislation is decades old, organizations are still responsible for compliance.

NTT Ltd. researchers identified Apache, Microsoft, and GNU products as accounting for 72% of vulnerabilities targeted in the finance industry. Of the top 20 targeted CVEs, attacks targeting Apache products accounted for 31%, with attacks on Apache Struts accounting for 20%; attacks related to Microsoft products accounted for 29%, with Microsoft Windows Server 2003 R2 being the top target accounting for 9%; and attacks targeting GNU products accounted for 12%, with attacks on GNU BASH accounting for 11%.

Finance – Cybersecurity Advisory scoring

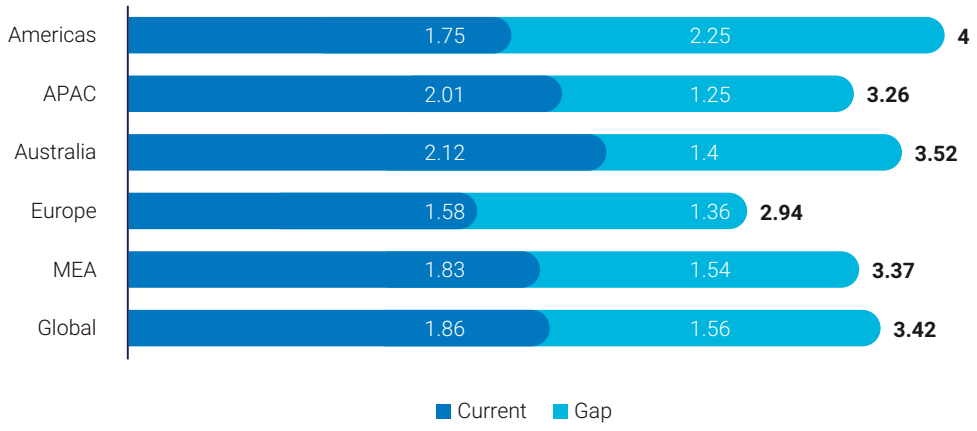

Figure 27: Finance - Cybersecurity Advisory scoring

As shown in Figure 27, finance continues to be among the highest scoring industries across all evaluated assessment areas in Cybersecurity Advisory scoring. However, like other industries, it has a long way to go to reach a consistent Managed or Optimized maturity. Initial benchmark scores showed the finance industry maintained the highest maturity with an average score of 1.86, up slightly from the 2019 maturity benchmark of 1.71. The APAC region leads globally with a 2.01 average maturity score, ahead of MEA at 1.83 and the Americas at 1.75. In Middle East & Africa, the maturity score dropped from 2.21 in the 2019 report, to 1.83 for 2020. Maturity scores in finance in APAC increased from 1.88 in 2019 to 2.01 in 2020. Australia had the highest maturity for finance of any country tested, with a maturity score of 2.12.

Activity against finance was marked by two main attack types:

1. Application-specific and web-application attacks targeting Joomla!, IIS and Apache products.
2. Consistent use of pmabot, China Chopper, and gh0st (accounting for over 30% of all malware detections) used to maintain persistent control over finance infrastructure.

Top attack types	Top vulnerabilities targeted by CVE number	Top products targeted	Top malware categories
Application Specific – 37% Web-Application Attack – 30% Reconnaissance – 12%	CVE-2017-9805 (Apache Struts) – 13% CVE-2009-3075 (Mozilla Firefox, Thunderbird, SeaMonkey) – 11% CVE-2014-6271 (GNU BASH) – 11%	Apache – 31% Microsoft – 29% GNU – 12%	Trojan/Dropper – 83% Spyware/Keylogger – 5% Virus/Worm – 2%

Figure 28: Top targeting in the finance industry

Spotlight On: Older vulnerabilities

NTT Ltd. researchers observed the top ten most targeted vulnerabilities in the finance industry were all originally defined in 2017 or earlier. These vulnerabilities accounted for 72% of all observed targeting. This suggests attackers are attempting to exploit older vulnerabilities which organizations may not prioritize in their patching schedule compared to more recent vulnerabilities.

Attackers are focusing on vulnerabilities present in Apache, Microsoft, and GNU products. Products in the Apache suite, like Struts (notably CVE-2017-9805), were targeted in 31% of all attacks against finance. Organizations which can verify their patch management programs are including these highly targeted vulnerabilities to make substantive improvements in their security programs and decrease their available attack surface.

Spotlight On: Web-enabled applications

NTT Ltd. researchers identified 37% of all hostile activity targeting finance were application-specific attacks and 30% were web-application attacks. This indicates 67% of attacks affecting finance targeted web-enabled applications or the systems and tools supporting them. Injection attacks and cross-site scripting dominated these attacks, regularly targeting Apache Struts, ColdFusion, Joomla!, and other CMS suites. Attacks against CMS suites commonly included attempts to infect systems with China Chopper, Cknife, and other web shells.

These attacks often allow RCE to enable the extraction of sensitive data. Since web-enabled applications are important to business operations, organizations must design specific security controls to help mitigate threats to them. Along with controls to harden and secure fielded hardware and maintain operating systems and application patches, this includes secure coding techniques. Organizations can also help protect web-enabled applications with the practical use of web-application firewalls.

Governance, risk and compliance

Financial GRC addresses the way financial institutions collect, manage, and control financial information in its control. It dictates how an organization monitors financial transactions, how it manages performance and control data, operations, and disclosures.

The US Sarbanes-Oxley Act of 2002, Japan's JSOX, the UK's Turnbull; MI 52-109, and Bill 198 in Canada are a few of the financial regulations put in place to protect financial transactions, processes, and data. In 2019, Australia's CPS 234 came into effect to ensure organizations regulated by the Australian Prudential Regulation Authority (APRA) are adequately protected from cyberattacks and other security incidents which may impact information asset and data's confidentiality, integrity, and availability. China's central bank also released rules which took effect on January 1, 2019 to prevent money laundering and terrorist financing through better 'know your customer' rules and by reporting large and suspicious transactions in a timely manner.

The US Department of the Treasury's Office of Foreign Assets Control (OFAC) instituted the following anti-money laundering and combating financing of terrorism (AML/CFT) laws: The Bank Secrecy Act 1970; Money Laundering Control Act 1986; Anti-drug Abuse Act 1988; Annunzio-Wylie Anti-money Laundering Act 1992; Money Laundering Suppression Act 1994; Money Laundering and Financial Crimes Strategy Act 1998; USA PATRIOT Act 2001; Suppression of the Financing of Terrorism Convention Implementation Act 2002; and Intelligence Reform and Terrorism Prevention Act 2004.

The global finance industry operates under a wide variety of data privacy regulations which uniquely positioned the industry for GDPR compliance. The risks of non-compliance with financial GRC includes fraud, misappropriation, material errors, regulatory penalties, loss of consumer confidence, and fines or sanctions.

Financial institutions must understand the processes and regulations for GRC, understand the possible repercussions from interacting with personal financial data, and must obtain consumer consent before transferring or processing that data. The shift in financial GRC mandates financial institutions and all who process financial data must incorporate data protection into their data protection design.

Application security analysis

Finance is outperforming all other industries by a large margin. A large portion of their success can likely be attributed to the fact that their industry was one of the first to embrace application-security as a key part of their business model. We are seeing firms in the finance industry continue to invest in their security teams, and the results are apparent.

Finance continues to lead in secure app design, as well as running very progressive security operations. Their internal process (and expanded security budgets) has allowed them to outshine other industries in their security results.

Top serious vulnerabilities	Likelihood of serious exposure	Likelihood of any exposure
Cross Site Scripting	7%	7%
Insufficient Transport Layer Protection	5%	85%
URL Redirector Abuse	3%	3%
Insufficient Authorization	2%	9%
Brute Forcing	1%	6%

Figure 29: Finance's likelihood of exposure to top serious vulnerabilities

Application exposure

The finance industry saw an average of just under five serious vulnerabilities per site, which significantly out-performs all other industries in this focus.

A large portion of their insufficient transport layer protection vulnerabilities are likely related to the fact that many of their assets are run by third parties, making it a challenge to inventory and keep their servers up to date.

Recommendations

Security frameworks containing standard recommendations exist to help organizations mitigate risks. NTT Ltd. has conducted consulting engagements and, in the course of providing guidance to our clients, found the MITRE ATT&CK framework to be robust and provides excellent information to help organizations address cybersecurity threats. As it is a strong resource, NTT Ltd. has chosen to align our suggestions for mitigation recommendations:

Researchers first detected Conficker in 2008. The worm is fast spreading, has infected millions of devices, and established botnet infrastructure. **Its presence often indicates lax patching or the lack of a robust security suite.**

Mitigation	MITRE ATT&CK ID	Description
Vulnerability scanning	M1016	Regularly scanning external facing applications for vulnerabilities and instituting a patching schedule, as well as being ready to rapidly patch critical vulnerabilities. Employing network segmentation so externally facing servers are segmented from internal networks.
Exploit protection	M1050	Employing web-application firewalls to stop exploit traffic from reaching a potentially vulnerable application.
Application development	M1013	Provide guidance and training for developers to avoid introducing security weaknesses which an adversary may be able to take advantage of.

Figure 30: Recommendations for the finance industry

While finance faced a variety of challenges, including consistent levels of attacks and regulatory pressures the manufacturing industry faced data breaches for financial gain as well as intellectual property theft, disruptive attacks, global supply chain risks, and risks from unpatched vulnerabilities.

Manufacturing industry

The manufacturing industry has notoriously faced cyber espionage attacks linked to the theft of intellectual property and disruptive attacks launched by suspected state-backed actors. However, the industry also faces various other challenges, including financially motivated data breaches, global supply chain risks, and risks from unpatched vulnerabilities, which is reflected in the targeting of this industry. For example, NTT Ltd. researchers found the single most observed malware variant was the Conficker worm, which suggests organizations have out of date patches, users are employing weak passwords, or there is a lack of a robust security suite for identifying and preventing infection.

Compliance requirements within manufacturing can vary widely depending on the exact nature of the organization, but tend to focus on workplace safety and environmental impact. The manufacturing industry is beginning to be held to greater scrutiny because of the prospect of long-term damage to the environment and global warming. Judgements can be harsh, and non-compliance penalties substantial.

NTT Ltd. researchers identified GNU, Microsoft, and Apache products as accounting for 88% of vulnerabilities targeted in manufacturing. Of the top 20 targeted CVEs, attacks targeting GNU products accounted for 64%, with attacks on GNU BASH via the 2014 GNU Shellshock vulnerabilities accounting for 60%; attacks related to Microsoft products accounted for 19%, with Microsoft Windows Server 2003 R2 being the top target accounting for 9%; and attacks targeting Apache products accounted for 5%, with attacks on Apache Struts accounting for 3%. Overall, activity against manufacturing was the most consistent when compared to activity from previous years.

> Overall, activity against manufacturing was the most **consistent when compared to activity** from previous years.

Targeting the manufacturing industry

Manufacturing organizations often maintain valuable data about processes, supply chains, and distribution, as well as potentially sensitive design or specification information, much of which is sensitive intellectual property. Modern manufacturing is also highly automated, and highly dependent on technology for support, including the widespread use of connected systems and IoT/OT devices. Manufacturing infrastructure is often built on platforms which supported efficient operations, but were not necessarily designed to be secure. High volumes of reconnaissance helps let attackers determine where to focus web-application and application-specific attacks for maximum effectiveness. Additionally, attackers take advantage of the complex environments to attacks manufacturing's networking infrastructure; the underlying servers and network devices. Attackers support these attacks by making extensive use of viruses and worms which help identify vulnerable infrastructure.

Manufacturing – Cybersecurity Advisory scoring

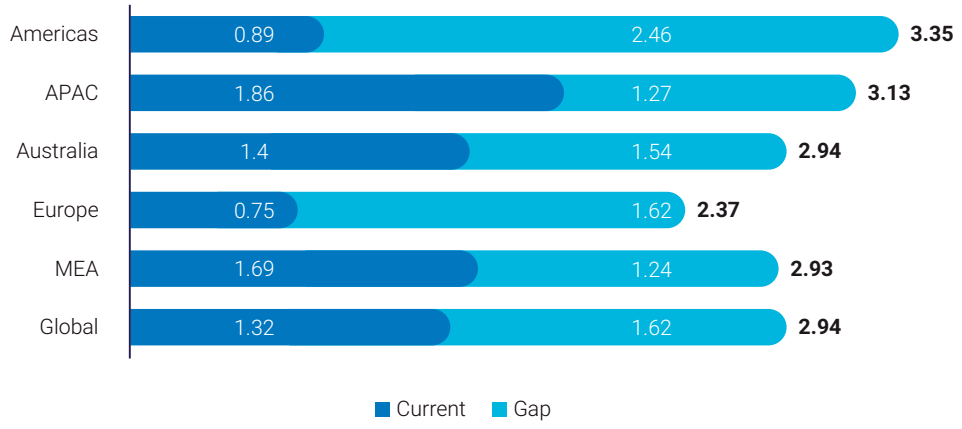

Figure 31: Manufacturing - Cybersecurity Advisory scoring

As shown in Figure 31, the manufacturing industry observed an average maturity level of 1.32 in Cybersecurity Advisory scoring. MEA beat the global average, with a maturity score of 1.69, and performed strongest in Security Vision and Strategy, and Information Security Framework assessment areas. Organizations in APAC lead with a 1.86 average maturity score and showed the highest regional score in Risk Management. Australia's manufacturing maturity was benchmarked at 1.4. well ahead of the Americas (0.89) and Europe (0.75) region averages. The Americas showed the lowest maturity of all major regions with a score of 0.89. The Americas region was significantly behind other regions in every maturity subcategory measured in manufacturing.

Activity against manufacturing was marked by three main attack types:

1. Reconnaissance and targeting of Shellshock.
2. Application-specific attacks against WordPress (and other CMS suites), Apache Struts and other web technologies.
3. Persistent use of Conficker, as well as the Ramnit Trojan, and China Chopper to compromise and maintain persistence.

Top attack types	Top vulnerabilities targeted by CVE number	Top products targeted	Top malware categories
Reconnaissance – 22% Application Specific – 22% Web-Application Attack – 20%	CVE-2014-6278 (GNU BASH) – 60% CVE-2017-7269 (Microsoft Windows Server 2003 R2) – 9% CVE-2018-1003 (Microsoft JET Database Engine) – 4%	GNU – 64% Microsoft – 19% Apache – 5	Virus/Worm – 43% Trojan/Dropper – 26% Spyware/Keylogger – 7%

Figure 32: Top targeting in the manufacturing industry

Spotlight on: Shellshock

The GNU vulnerability CVE-2014-6278 – known as Shellshock – accounted for 60% of all targeted CVEs in the manufacturing industry. First announced in September 2014, NVD gave the vulnerability a CVSS version 2.0 score of 10. While many of these detections are more properly classified as reconnaissance, successful exploitation of this vulnerability, which affects GNU BASH through 4.3 bash43-026, could allow a remote attacker to execute their own commands on remote systems. Through a successful exploitation of Shellshock, attackers can compromise a server and steal data, launch DDoS attacks, or compromise other connected machines.

By instituting a security process which includes regularly scanning external facing applications for vulnerabilities and instituting a patch management process, organizations can reduce their potential attack surface from these types of vulnerabilities.

Spotlight on: Malware

NTT Ltd. researchers found 69% of all malware detected within the manufacturing industry were either virus/worms (43%) or Trojan/droppers (26%). Of this malware, researchers discovered the Conficker worm was the single most commonly detected variant, comprising 11% of all detections. The worm's presence suggests the use of weak passwords, outdated security precautions, and outdated or unpatched systems, which leaves organizations vulnerable to infection via other malware variants.

Ramnit was the most detected Trojan in this industry, making up 60% of all Trojan detections. Ramnit affects Windows users, propagates aggressively through a variety of techniques, and has been discovered in the Google Play store. It can exfiltrate data from infected devices, including FTP passwords, cookies, and credentials. This can lead to serious reputational or financial loss.

Modern malware requires a multi-prong approach. While consistent anti-malware software is required, organizations should also implement an active patch management program to reduce infection vectors, network segregation to help interfere with propagation, and an active response program which includes offline backups to help with recovery.

Ramnit is a RAT which has been identified circulating in the wild for approximately a decade. Originally a worm, **Ramnit has continued to evolve over the years to include the theft of login credentials.**

Governance, risk and compliance

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

The emergence of global standards to address the unique landscape of global manufacturing has brought the risk of non-compliance to the forefront of the industry. Manufacturers spend an estimated USD 192 billion annually to remain compliant with GRC regulations. Violations can result in fines, products removed from markets, and in the case of catastrophic accidents caused by non-compliance, manufacturers can face lawsuits with a steep financial cost, as well as substantial brand damage.

There are many regulations governing the manufacturing subsectors, particularly manufacturing medical devices. In addition to medical device manufacturing, we expect to see a growing number of laws and regulations related to industrial IoT, which also influences this industry.

Implementing GRC across each organization's unique landscape can help manufacturers deliver safe products worldwide. Ensuring manufacturing suppliers throughout the supply chain remain compliant helps manufacturers, their employees, and partners remain aware of the risks of non-compliance, and protect the ecosystems which make up the domestic and global manufacturing environment.

Application security analysis

The manufacturing industry appears to be lagging behind other industries in application security. This is especially worrisome, since manufacturing is becoming a larger and more attractive target to nation-states. As a result, infrastructure and manufacturing industries are one of the major areas being looked at currently by CISA.

Manufacturing websites want to draw people in. Images and videos have always been a great way to grab a potential customers' attention. In this matter, the primary goal of this integration is quality, and not necessarily security. Yet this is how many applications find themselves in trouble.

> Lack of encryption plagues many sites, but with more than a 15% likelihood of serious exposure, the **manufacturing industry is at greater risk than most in the event of an application-wide attack**.

Top serious vulnerabilities	Likelihood of serious exposure	Likelihood of any exposure
Cross Site Scripting	31%	31%
Insufficient Transport Layer Protection	15%	93%
URL Redirector Abuse	12%	12%
Brute Forcing	10%	26%
Cross Site Request Forgery	10%	11%

Figure 33: Manufacturing's likelihood of exposure to top serious vulnerabilities

Application exposure

On average we are seeing over 11 serious vulnerabilities per site in manufacturing, putting them at the second-highest level of exposure in our focus-industries, just behind technology industries.

Based on analysis of this data, there is a high likelihood a manufacturing organization will have cross-site scripting vulnerabilities. With every exposure being deemed a serious exposure, this can put the entire application at risk, as well as give attackers a foothold to pivot to a more critical target.

Like many other industries, manufacturing applications faced significant risks related to insufficient transport layer protection. Lack of encryption plagues many sites, but with more than a 15% likelihood of serious exposure, the manufacturing industry is at greater risk than most in the event of an application-wide attack. Simple measures such as the inclusion of an HTTP Strict Transport Security (HSTS) header, which will enable web servers to declare browsers should only interact with it using the secure HTTPS protocol, would be very helpful. Using HSTS will force any HTTP traffic to use HTTPS before it hits the server.

Manufacturing sites often use high quality images to show off materials, products, etc. – this exposes them vulnerabilities which target mixed content vulnerabilities. In such an environment, it is critical for access to sourced content to be appropriately encrypted.

15%

Lack of encryption plagues many sites, but with more than a 15% likelihood of serious exposure, the manufacturing industry is at greater risk than most in the event of an application-wide attack.

Recommendations

Security frameworks containing standard recommendations exist to help organizations mitigate risks. NTT Ltd. has conducted consulting engagements and, in the course of providing guidance to our clients, found the MITRE ATT&CK framework to be robust, providing excellent information to help organizations address cybersecurity threats. As it is a strong resource, NTT Ltd. has chosen to align our suggestions for mitigation recommendations:

Mitigation	MITRE ATT&CK ID	Description
Exploit Protection	M1050	Employing web-application firewalls to stop exploit traffic from reaching a potentially vulnerable application.
Multilayer Encryption	M1032	Employ secure communications across multiple levels of application, web sites, and the organizational infrastructure. Ensure sensitive information is provided via secure connection.
Update Software	M1051	Creating a patch management process for internal enterprise endpoints and servers, as well as to check for unused dependencies, previously vulnerable or unmaintained dependencies, and unnecessary files, features, and components. Ensuring web servers which are externally facing are patched regularly.

Figure 34: Recommendations for the manufacturing industry

As the manufacturing industry faced intellectual property theft and other forms of data breaches mentioned above, the retail industry faced a significant amount of DoS/DDoS attacks.

Retail industry

Retail organizations are faced with one of the more complex threat footprints of any industry. While DoS/DDoS attacks were the single largest type of attack against retail organizations, accounting for 42% of all attacks, the retail industry also faced a broad spectrum of other attacks. Attackers targeted users and internal resources with exploits in DNS, Explorer, and Excel. The single most attacked technology in the retail industry was Microsoft SharePoint. Attackers used DoS/DDoS, web-application, and application-specific attacks against web-enabled systems, and targeted internal networks with remote access Trojans (RATs), botnets, and exploit kits to establish and maintain persistence. Attackers targeted brick and mortar stores with point-of-sale (PoS) malware and skimming, and targeted retail customers with malvertising campaigns to directly impact users.

The Payment Card Industry Data Security Standard (PCI-DSS) is one of the most successful standards compliance programs available. It provides guidelines for organizations on protecting card holder data and the systems which are involved in the obtaining and management of that information. Compliance with the PCI-DSS can make an organization more secure, and lack of compliance can result in fines and penalties by the governing body.

NTT Ltd. researchers identified Microsoft products as the most targeted by attackers. Attacks targeted SharePoint, Excel, Windows DNS, Windows Server, and more; in total attacks targeting Microsoft products accounted for over 40% of all attacks targeting retail. This trend was supported directly by the top targeted vulnerabilities – eight of the top 10 targeted vulnerabilities were in Microsoft products, with the remaining two being in Apache Struts and OpenSSL.

Targeting the retail industry

The retail industry manages a wide variety of valuable information, including inventory, pricing, organizational financial, and customer financial, as well as customer identifying information. The variety of information maintained leads to complex environments, from corporate infrastructure to a variety of Point of Sale systems, along with the infrastructure needed to support each environment and effective communications between them. The customer base helps make retail organizations a target for both financial information and the harvesting of credentials, and the subsequent reuse of that information to support resale of financial information, conducting fraudulent transactions, identity theft, and phishing campaigns, The complexity of the retail environments and complexity of the data retail manages helps make retail the focus of complex attacks which use high volumes of denial of service, web-application and application specific attacks, networking attacks, attacks against endpoint systems, and persistent compromise of internal systems via remote access Trojans.

Retail – Cybersecurity Advisory scoring

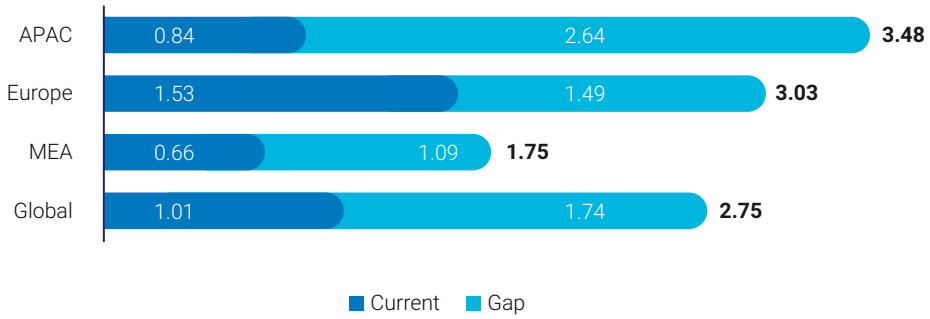

Figure 35: Retail - Cybersecurity Advisory scoring

Exploit kits are bundled toolkits which attackers use in their operations to exploit select vulnerabilities. Generally, exploit kits provide a **management console and additional functions which make it easier for an attacker to carry out their operations.**

As shown in Figure 35, the retail industry had the second lowest maturity score with an average of 1.01. Europe led all regions with an average maturity score of 1.53. The retail industry suffered significant lack of maturity across most assessment areas in almost every region. Risk management showed the lowest maturity score in every region, and globally, with a global average of 0.97.

If retail wants to make significant progress towards their goal, they should emphasize data and system classification and management, focusing on the impact security will have on their business operations.

Activity against retail was marked by three main attack types:

1. Denial of service attacks targeting bind and other external services, especially in APAC.
2. Application-specific and web-application attacks targeting Oracle products, Apache products, WebDAV and IIS services.
3. Persistent use of the Ramnit Trojan, Conficker, and China Chopper to compromise and maintain persistence in manufacturing organizations.

Top attack types	Top vulnerabilities targeted by CVE number	Top products targeted	Top malware categories
DoS/DDoS – 42% Web Application – 31% Application Specific – 16%	CVE-2015-2415 (Microsoft Office) - 14% CVE-2015-6051 (Internet Explorer) – 12% CVE-2017-0171 (Windows DNS) – 10%	Microsoft – 40% Apache – 26% TrendMicro – 11%	Remote Access Trojan – 24% Botnet – 23% Exploit Kit – 15%

Figure 36: Top targeting in the retail industry

Spotlight on: Denial of service

42% of all attacks targeting retail were DoS attacks. The next highest rate of DoS/DDoS attacks was 25% in technology. DoS/DDoS attacks were especially pronounced in EMEA and APAC. These attacks, most commonly flood attacks directed at corporate sites, websites, and applications, were designed to make the services unavailable for extended periods of time. Flood attacks made up over 34% of all attacks directed at retail organizations. Some attackers also used botnets to help sustain high levels of network traffic. While botnets were not the most common malware within retail, NTT Ltd. researchers identified high levels of both IoTroop and Mirai.

Customers who visit a site which is down may return but will often move rapidly to an alternate site. After a sustained DoS attack, some customers may never return to shop. DoS/DDoS attacks are often used for purposes of extortion – to extract payment to stop the attack – or as a distraction from other attacks designed to compromise part of the organizational network while the organization is busy dealing with the more obvious DoS attack.

Spotlight on: Application attacks

In the retail industry, 31% of all attacks were some form of web-application attack. These attacks are designed to compromise the web presence of the organization – in the case of a retail organization, this will often be their online store. In retail, these attacks were 36% buffer overflow attacks and 32% RCE attacks. In either case, the goal of the attack is to allow the attacker to run commands on the system hosting the attack.

For retail, the technologies targeted to enable these attacks were most often Oracle, Apache products, WebDAV, and IIS services.

Application attacks can be complex to mitigate in a complicated environment. Organizations should start by ensuring the underlying systems are patched and hardened, including disabling default accounts. The system and applications should be maintained by an aggressive patch management system. The organization should use good development and code management practices, as well as protect the web-enabled environment with web-application firewalls.

Governance, risk and compliance

The Payment Card Industry Security Standards Council (PCI SSC) developed and maintains the PCI DSS set of security controls. The PCI DSS is comprised of 12 requirements: Install and maintain a firewall configuration to protect cardholder data; do not use vendor-supplied defaults for system passwords and other security parameters; protect stored cardholder data; encrypt transmission of cardholder data across open, public networks; use and regularly update antivirus software; develop and maintain secure systems and applications; restrict access to cardholder data by business need-to know; assign a unique ID to each person with computer access; restrict physical access to cardholder data; track and monitor all access to network resources and cardholder data; regularly test security systems and processes; and maintain a policy which addresses information security.

The PCI DSS is an information security standard for organizations which handles credit cards. Retailers must adhere to the PCI DSS to protect payment card information from data theft and fraud. Complying with the PCI DSS not only helps a retailer protect consumer information, but it can help protect a retail organization from incurring fines and reputation damage. Failure to meet the PCI DSS requirements may result in fines or termination of credit card processing privileges for the retailer. The PCI DSS requires all individuals must be notified in writing if a breach was believed to have occurred. The average cost of a data breach and recovery is an estimated USD 3.8 million. The penalties for non-compliance can range from USD 500,000 per cybersecurity incident to USD 100,000 every month. In addition to fines, class action lawsuits from breached customers could further add to an organization's reputation damage and financial loss.

Retail organizations must strive to protect customer data while protecting their brand reputation by maintaining a continuous state of PCI DSS compliance year-round. Building and implementing an incident response plan which is secure by design, and resilient can help better manage and reduce retail data breach risk, possibly reduce breach recovery costs, and reduce fines levied by the PCI DSS.

Application security analysis

Digital transformation hit this industry hard, with many retail transactions now taking place online. Organizations which would historically have a simple presentation and sales process, like a t-shirt vendor, are building complicated software applications and need to secure them.

Retail sites often have multiple partners with whom they do business. As a result, external links are common within supported sites, applications, and mobile apps. Ensuring the organization is only working with secure, encrypted links is an important step in addressing these risks. URL redirectors do not necessarily represent a direct security vulnerability but can be abused by attackers trying to social engineer victims into believing they are navigating to a site other than the true destination. Retail organizations should consider the following good practices:

- Whitelist safe destinations and validate against the list before redirecting the user.
- Notify the user they will be redirected to the destination and force them to take an action to continue the redirect.

Top serious vulnerabilities	Likelihood of serious exposure	Likelihood of any exposure
Cross Site Scripting	29%	31%
Insufficient Transport Layer Protection	13%	88%
Cross Site Request Forgery	7%	10%
Information Leakage	7%	64%
URL Redirector Abuse	5%	6%

Figure 37: Retail's likelihood of exposure to top serious vulnerabilities

Application exposure

Retail sites saw an average of 10.5 serious vulnerabilities, with a significant number of cross site scripting vulnerabilities among them. With a 28% likelihood of serious exposure to cross site scripting, the retail industry requires more attention to server-side validation of data.

The high level of insufficient transport layer protection is mostly attributed to content being pulled into the page or application over insecure connections. This can easily be avoided by validating all URLs to ensure they contain only safe schemes like HTTPS.

Lastly, general security-best-practices training for developers in these teams will likely go a long way. Many of the findings in this industry are fairly simple to mitigate and could potentially be avoided with proper training, procedures and attention to details on the flaws, what causes them, and corrective action.

The high level of insufficient transport layer protection is mostly attributed to content **being pulled into the page or application over insecure connections**.

Recommendations

Security frameworks containing standard recommendations exist to help organizations mitigate risks. NTT Ltd. has conducted consulting engagements and, in the course of providing guidance to our clients, found the MITRE ATT&CK framework to be robust and provides excellent information to help organizations address cybersecurity threats. As it is a strong resource, NTT Ltd. has chosen to align our suggestions for mitigation recommendations:

28% With a 28% likelihood of serious exposure to cross site scripting, the retail industry requires more attention to server-side validation of data.

Mitigation	MITRE ATT&CK ID	Description
Enable DoS Protection	T1498	Management of flood volumes related to DoS attacks potentially includes both on-premises and upstream filtering of attack traffic.
Protect Public-Facing Applications	T1190	Use web-application firewalls to help limit exposure of applications to prevent exploit traffic from reaching the application.
Protect Data and Credentials	T1078	Ensure applications store sensitive data and credentials in secure manners.

Figure 38: Recommendations for the retail industry

The retail industry is challenged with a variety of security threats and regulatory requirements to balance. As described in the next section, this balance is even harder to achieve in the healthcare industry.

Healthcare industry

Due to the value of personal data and Electronic Medical Records (EMRs), the healthcare industry has an increased risk of being targeted by attackers. As malicious actors can use this information in various ways – for example in identity theft or to purchase and resell medications – this data, and EMRs specifically, are eight to ten times more valuable in the black market than credit card information alone. The value of healthcare data is reflected in the targeting of this industry, as NTT Ltd. researchers found 61% of all hostile activity targeting healthcare was reconnaissance, with a large percentage of activity being related to host discovery and port scanning.

Healthcare organizations must take proactive steps to protect their data, particularly as the Health Insurance Portability and Accountability Act (HIPAA) 2020 mandates organizations and their Business Associates institute safeguards for sensitive medical information. Failure to adequately safeguard data can lead to reputational damage, breach recovery costs, and fines received per HIPAA rule infraction.

NTT Ltd. researchers identified Drupal, Apache, and Microsoft products as accounting for 72% of vulnerabilities targeted in healthcare. Of the top 20 targeted CVEs, attacks on the Drupal CMS accounted for 28%; attacks targeting Apache products accounted for 24%, with attacks on Apache Struts accounting for 14%; and attacks related to Microsoft products accounted for 20%, with Microsoft Windows Server 2003 R2 being the top target accounting for 8%.

Targeting the healthcare industry

The healthcare industry is built around providing healthcare services. To do this, organizations manage a variety of personal health information, and additional information related to financial details, suppliers and service providers. Infrastructures tend to support robust applications which manage high quality data about customers and providers. Healthcare also tends to maintain a significant volume of legacy systems which were designed to provide healthcare relevant services, but may not always have been designed or implemented with a focus on security. The prevalence of electronic healthcare records involves increasing amounts of data-aware technology. Attackers value this information for identity theft, fraudulent use of healthcare services, prescription medicines, and government or assistance payments. High volumes of reconnaissance help make application-specific attacks more targeted and effective, especially when teamed up with the high amounts of spyware discovered in healthcare organizations.

Healthcare – Cybersecurity advisory scoring

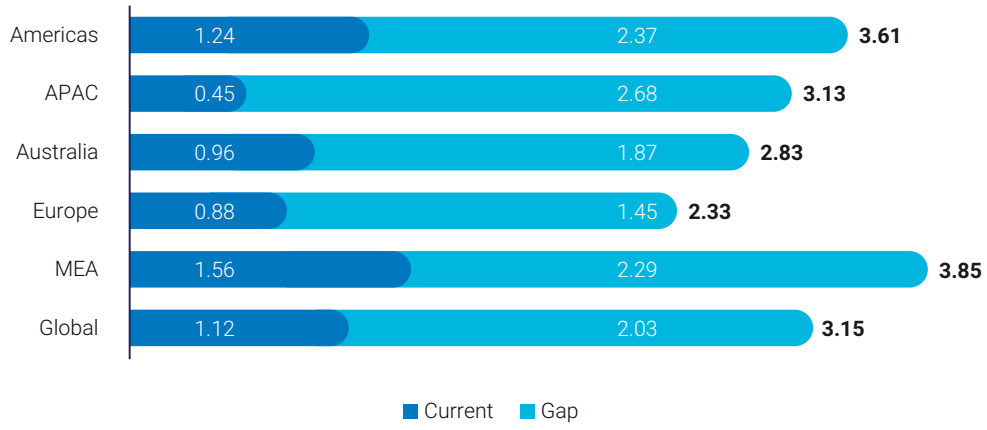

Figure 39: Healthcare - Cybersecurity Advisory scoring

All subcategories in APAC showed **lower maturity scores** than in any other region tested.

As shown in Figure 39, the healthcare industry observed an average maturity level of 1.12. This is a slight increase from 1.03 in 2019. Organizations within MEA lead with a 1.56 average maturity score, ahead of America's 1.24. APAC showed the lowest maturity in healthcare organizations with an average score of 0.45. All subcategories in APAC showed lower maturity scores than in any other region tested. MEA and America both showed the most mature subcategories as Information Security Framework and Risk Management. MEA's maturity in Information Security Framework leads globally with an average of 2.03.

Activity against healthcare was marked by three main attack types:

1. Focused targeting of web technologies like Drupal, Apache products, and Microsoft products.
2. Reconnaissance activity, marked by scanning with automated tools like muieblackcat, and consistent use of IoTroop to discover vulnerable systems.
3. Persistent use of remote access Trojans like doublepulsar, jsp, and gh0st to compromise and maintain persistence in healthcare organizations.

Top attack types	Top vulnerabilities targeted by CVE number	Top products targeted	Top malware categories
Reconnaissance – 61% Application Specific – 32% OS Specific – 2%	CVE-2018-7600 (Drupal) – 28% CVE-2017-7269 (Microsoft Windows Server 2003 R2) – 8% CVE-2018-6961 (VMware NSX SD-WAN Edge by VeloCloud) – 8%	Drupal – 28% Apache – 24% Microsoft – 20%	Spyware/Keylogger – 72% Trojan/Dropper – 19% Virus/Worm – 3%

Figure 40: Top targeting in the healthcare industry

Spotlight on: Drupal

The Drupal vulnerability CVE-2018-7600, first disclosed in March 2018, accounted for 28% of all targeted vulnerabilities in the healthcare industry. Successful exploitation of this vulnerability, which affects Drupal versions before 7.58, 8.x before 8.3.9, 8.4.x before 8.4.6, and 8.5.x before 8.5.1, allows a remote attacker to execute arbitrary code on an affected system. NVD scored the vulnerability with a CVSS score of 9.8. This vulnerability is exploitable on any underlying Linux, Microsoft, or Unix operating system. The combination of the variety of versions affected, the sheer volume of affected systems, the ease with which the vulnerability can be exploited, and automation of the exploit helped make this a significant issue for any organization using Drupal.

Ensuring organizations are regularly performing patching and security testing for these types of vulnerabilities can provide immediate benefits across multiple environments by decreasing the vulnerable attack surface.

Spotlight on: Reconnaissance

NTT Ltd. researchers found 61% of overall malicious activity affecting the healthcare industry was reconnaissance. Additionally, 47% of attack types were host discovery and 10% of attack types were port scanning-related activity. The emphasis on infrastructure reconnaissance within healthcare suggests attackers place value in gaining and maintain access to organizational infrastructure.

Additionally, 72% of all observed malware was in the spyware/keylogger family, with 41% of the top malware variants classified as remote access Trojans (RATs). This suggests a large percentage of threat actors are seeking to gain access to healthcare organizations to maintain persistence and exfiltrate sensitive information over prolonged periods of time.

Governance, risk and compliance

Between 2017 and 2024, the EU healthcare industry is transitioning towards compliance with the 2017 European Union Medical Device Regulation (EU MDR). The EU Commission has regularly published additional guidance and specifications for the regulation, including guidance for medical device cybersecurity in January 2020. In 2019, Australia's Therapeutic Goods Administration (TGA) announced in April 2019 it would increase oversight of new devices to better align with EU MDR, following a promise in 2016 to align medical device requirements with the EU's as much as possible and appropriate.

Within the United States, HIPAA requires healthcare organizations to adhere to standards which will secure Patient Health Information (PHI) and Electronic Patient Health Information (ePHI). PHI and ePHI are information held by a covered healthcare entity which concerns health status, provision of healthcare, or payment for healthcare which can be linked to an individual. The HIPAA Omnibus Rule – published in the Federal Register in April 2019 by the US Health and Human Services Department (HHS) – enhanced the HIPAA Privacy Rules to enforce discretion of HIPAA Civil Money Penalties (CMP) paid by healthcare entities per tier violation. The HIPAA Omnibus Rule also dictates any Business Associate (BA) of a healthcare facility will be subject to HIPAA rules.

HIPAA 2020 mandates organizations and their BAs working with PHI and ePHI implement technical, physical, and administrative safeguards to protect all PHI. The safeguards include six annual self-audits per healthcare organization, and five annual self-audits for their BAs. The self-audits must include Security Risk Assessment (SRA), Security Standards Audit, HITECH Subtitle D Audit, Asset and Device Audit, Physical Site Audit, and Privacy Assessment. Healthcare organizations must ensure they complete a Business Associate security check, including a Vendor Questionnaire to assess the BA's security practices, and complete a Business Associate Agreement (BAA). Should a healthcare data breach occur, both entities would be liable and suffer fines. HIPAA fines for the healthcare industry average around USD 6.45 million. This likely incentivizes security teams to place a high emphasis on data controls and threat modeling, causing them to have one of the lowest occurrences of sensitive data exposure.

HIPAA charges occurred after assessing fines to healthcare organizations totaling USD 23,504,800 in 2016, USD 20,393,200 in 2017, USD 28,683,400 in 2018, and USD 15,270,000 in 2019. To design a secure, HIPAA compliant program, it is imperative to incorporate HIPAA 2020 standards and practices into PHI and ePHI safeguards. Self-audits, employee training, business associate management, and an incident response plan which is secure by design and resilient can help better manage and reduce healthcare data breach risk, breach recovery costs, and fines received per level of HIPAA rule infraction.

Application security analysis

The healthcare industry is amongst the more regulated of the five industries in this analysis. In line with expectations, the healthcare industry applications analysed by WhiteHat security have the second lowest average number of serious vulnerabilities detected per application. They also have the second lowest average number of critical risk vulnerabilities detected per application (.77).

The healthcare industry focuses on ease of use for their customers. They have made great strides, and as noted above healthcare has the second lowest average number of critical risk vulnerabilities detected per application (.77). Balancing the need to protect medical information with ease of use can lead to observed flaws such as URL Redirect. Healthcare sites tend to make extensive use of multiple data sources – all in the effort to simplify the use of that information for the user. These links are high value targets for attackers to test, so must, in turn, be tested heavily by the healthcare organization. In the view of the end user, everything happens on the healthcare organization's website, so any third-party flaws have the potential to be viewed as organizational problems.

Top serious vulnerabilities	Likelihood of serious exposure	Likelihood of any exposure
Insufficient Transport Layer Protection	16%	93%
Cross Site Scripting	14%	15%
URL Redirector Abuse	5%	6%
Insufficient Authorization	4%	15%
Brute Forcing	3%	12%

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

Healthcare applications tested continue to struggle to significantly separate their exposure from the overall average of their peer industries in a number of common and severe vulnerability classes, including SQL injection, where they are underperforming against the global average as well as against 2/5 of the focus industries.

Application exposure

Healthcare sites saw an average of eight serious vulnerabilities per site in 2019. The most prevalent one being Insufficient Transport Layer Protection, with a 16% likelihood of exposure.

The high level of Insufficient Transport Layer Protection findings was likely due to more sophisticated testing becoming available. Better tools were able to locate vulnerabilities which had previously been difficult to confirm. WhiteHat observed thousands of sites which operated completely unencrypted.

Mixed Content, a vulnerability found when content is pulled from an insecure HTTP domain on a secure page, has also been a consistent problem with which organizations continue to struggle. Sites are fully encrypted; however, they collaborate with other sites which are not, thus leaving their application open to exposure via that supporting site in an active or passive method.

Cross Site Scripting, still on the OWASP Top 10 (INJECTION), has continued at a significant level of exposure. Lack of input sanitization and output encoding still reign supreme as the top flaws observed. Although improving, the risk of this vulnerability being exposed to an organization's applications at any level is devastating – ranging from account takeovers to application defacing/redesign.

Healthcare sites saw an average of eight serious vulnerabilities per site in 2019. The most prevalent one being Insufficient Transport Layer Protection, with a 15.84% likelihood of exposure.

Recommendations

Security frameworks containing standard recommendations exist to help organizations mitigate risks. NTT Ltd. has conducted consulting engagements and, in the course of providing guidance to our clients, found the MITRE ATT&CK framework to be robust and provides excellent information to help organizations address cybersecurity threats. As it is a strong resource, NTT Ltd. has chosen to align our suggestions for mitigation recommendations:

Mitigation	MITRE ATT&CK ID	Description
Network intrusion prevention	M1031	Employing network intrusion/ detection to prevent attackers from conducting scans for remote services.
Encrypt sensitive information	M1041	Encrypting all sensitive information at rest in the cloud. Encrypting all important data flows to reduce likelihood and impact of modifying data in transit. Employing encryption on emails to secure sensitive information.
Network segmentation	M1030	Architect sections of the network to isolate critical systems, functions, or resources.

Figure 42: Recommendations for the healthcare industry

Because of the amount and types of data they maintain, organizations in the healthcare industry face some of the strictest regulations of any industry. But, as discussed in the next section, regulatory compliance can be a challenge for any industry.

Governance, risk and compliance

When it comes to evolution, owls are specialists.

Due to asymmetrical ear placement, owls can pinpoint the exact location of sounds emitted several hundred meters away, from under leaves, plants, dirt, and snow.

Unlike most other species of birds, owls are nocturnal and have developed exemplary night vision skills. With the ability to swivel its head 270 degrees and exceptional depth perception, owls can clearly view their entire surroundings.

Governance, risk and compliance

Looking back over the year we have seen an encouraging increase in overall maturity regarding GRC matters, particularly with respect to data privacy and protection.

Governance, risk and compliance

2019 – A year of enforcement

Authorities have gained a greater understanding of their role in holding businesses accountable for their use of personal data (i.e. information about people) and have demonstrated their commitment to enforcing legislation which protects individual rights. In the last year, authorities in the European Union (EU) and the United States, in particular, have issued a number of fines against businesses which have failed to act transparently, fairly, and responsibly in their use of personal data. According to DLA Piper's latest General Data Protection Regulation (GDPR) Data Breach Survey[11], authorities have imposed EUR 114 million (approximately USD 126 million or GBP 97 million) in fines under the GDPR regime for a wide range of GDPR infringements, not just personal data breaches. While the number of fines issued by authorities is promising, authorities and businesses alike have much work to be done to enable data protection.

COVID-19 has impacted everything

Global health emergencies like the COVID-19 outbreak do, and should, affect the way organizations manage security-related initiatives. Health and safety concerns over employees and the public override many compliance initiatives, and should be taken into account when designing and implementing security controls, businesses continuity and disaster recovery plans.

More data privacy professionals driving the business agenda

We have seen a marked increase in maturity on the part of businesses themselves. Before 2018, there were very few data privacy professionals driving the agenda within businesses. Towards the end of 2019, the International Association of Privacy Professionals released research[12] which indicates approximately 500,000 businesses have registered Data Protection Officers (DPOs) under the GDPR in the EU. This number is significant and has the potential to change the way businesses think about data privacy and protection. Much like data protection authorities, businesses and their DPOs are still learning how to navigate data protection laws and regulations.

Emerging technologies also drive the business agenda, as organizations seek to leverage technologies to deepen customer engagement and drive revenue and profits. Businesses will need to be extra vigilant when looking to implement new technologies. Data protection implications can be complex to understand, and data protection authorities are placing increasing pressure on businesses who use these technologies to act responsibly and ethically. In the last year, several questions have been raised regarding artificial intelligence and machine learning, facial recognition and biometrics, and the ongoing extraction of personal data for big data analytics and the profiling of individuals' everyday lives and behaviours. Decisional interference has become a key concern for data protection authorities as choice architecture, design, and targeted messaging direct what people buy, where they eat, whom they date, how they vote, and what they think.

The questions being asked are becoming increasingly more complex as many businesses seek to gain a competitive advantage by using new technologies. If an organization does not have a strong data protection culture, as well as the right skills and expertise in place, the organization might not be able to foresee data protection implications. Identifying data protection challenges for new technology is a difficult task to achieve. For businesses which operate within the United Kingdom (UK), Brexit has affected business decisions and has impacted the way businesses approach data protection, particularly if personal data is shared between the EU and the UK.

Data protection implications can be complex to understand, and data protection authorities are **placing increasing pressure on businesses who use these technologies to act responsibly** and ethically.

[11] *denmark.dlapiper.com/en/news/eu114-million-fines-have-been-imposed-european-authorities-under-gdpr-0*

[12] *iapp.org/news/a/study-an-estimated-500k-organizations-have-registered-dpos-across-europe/*

Brexit has four primary implications for data protection:

1. **The GDPR no longer applies directly to UK businesses:** The GDPR is an EU regulation which applies to EU countries. Following its exit from the EU at the end of January 2020, the UK entered an 11-month transition period. During this period, the UK effectively remains in the EU's customs union, and single market, and continues to obey EU rules. Once the transition period has ended, the GDPR will no longer apply to the UK. However, the UK government intends to incorporate the GDPR into UK data protection law once the transition period is over. In addition, the GDPR may continue to apply to businesses who fall within its broad territorial scope.
2. **The UK is not recognized as a country with adequate data protection laws:** Businesses which share or transfer personal data from the EU to the UK will no longer be able to do so, without first putting into place specific transfer mechanisms to support the cross-border transfer, in a lawful way. Such mechanisms may include agreeing to Standard Contractual Clauses or implementing Binding Corporate Rules. However, businesses sharing or transferring personal data from the UK to the EU may continue to do so, as countries in the EU are considered adequate under UK adequacy regulations.
3. **Appointing EU Representatives:** Businesses which offer goods and services and/or monitor the behaviour of individuals in the EU, but do not have offices, branches, or other establishments within the EU, will need to formally appoint an EU Representative to act as a key contact point for Supervisory Authorities (data protection authorities) and individuals whose personal data it processes in the EU.
4. **'One-Stop-Shop':** The 'One-Stop-Shop' mechanism, under the GDPR, enables businesses within the EU which use the personal data of individuals in more than one EU member state to identify a lead Supervisory Authority. This enables businesses to only deal with one Supervisory Authority. Businesses who previously referred to the UK Information Commissioner's Office (ICO) as their lead Supervisory Authority will need to identify a new lead Supervisory Authority within the EU. The ICO will continue to regulate the UK's data protection laws and businesses who use personal data within the UK.

GDPR set a high standard for the rest of the world

The GDPR set a high standard of what data protection really means for businesses and individuals.

The essential message the GDPR sent out is: 'If you want to do business in the EU – regardless of where else in the world you may be – these are the rules.' Many businesses across the globe have interests in the EU, and consequently, have had to improve their standards to ensure they abide by the GDPR rules. Beyond its broad territorial scope, the GDPR has pushed many countries to rethink how they support their citizens' right to privacy, as well as create a business environment which both enables the free flow of information and promotes relationships with businesses or customers in the EU. Many countries are introducing new data protection laws or strengthening existing ones.

Introducing and strengthening new data protection laws provides a level of assurance to businesses and individuals, in that it does not matter where personal data is located or who uses it. The data will be protected to the same standard of care.

Other new regulations on the horizon

The United States continues to be an interesting territory to watch, and we expect to see a greater emphasis on data protection law and regulation in 2020. Many states in the US have some form of new data protection legislation in place, being developed, or refined to further the privacy rights of individuals.

The California Consumer Privacy Act (CCPA), which came into effect at the start of January 2020, is a state statute intended to enhance privacy rights and consumer protection for residents of California. If a business makes use of a California resident's personal information, that business is subject to the rules of this Act – regardless of whether they are based in California or not. The CCPA has interesting nuances when compared to the GDPR, but essentially it upholds individuals' rights to be informed about how their personal information is used, allows the individual to access, correct, and delete their personal information, as well as request their personal information not be sold to other parties.

In South America, the Brazilian General Data Protection Law (LGPD) is set to be launched in August 2020. The LGPD is very closely aligned to the GDPR, with a strong focus on respecting the individual's right to privacy and ensuring their data is protected with businesses and the state. Furthermore, revisions to Argentina's Personal Data Protection Act, and Colombia's increased focus on achieving adequacy under the GDPR, will be key developments in the region.

Following notable revisions at the end of 2019, India's long-anticipated, and highly contested Personal Data Protection Bill is expected to pass this year, as well as South Africa's Protection of Personal Information Act, which originally passed in 2013. Amendments to New Zealand's Privacy Act are also expected to be enforced in 2020, mandating breach notifications, increased powers for the Privacy Commissioner, and increased fines. Likewise, Singapore sought feedback in 2019 for proposed amendments to its Personal Data Protection Act. The amendments include increased data portability to give individuals greater control over the data and data innovation provisions which would allow organizations to use personal data without consent for designated business purposes.

Hong Kong's Panel on Constitutional Affairs also sought feedback on proposed changes to its Personal Data (Privacy) Ordinance (PDPO), which was first enforced in 1995. Changes to the PDPO include mandatory breach notifications and fines based on the revenue of the impacted organization.

In 2020, we expect to see the introduction of new data protection legislation around the world, and increased data protection enforcement by authorities.

Compliance and complacency don't mix

Unfortunately, despite the increase in data protection legislation and enforcement globally, some businesses – particularly those who have taken some actions to comply with the GDPR – are shifting their focus elsewhere, despite 28% of businesses stating they are compliant[13]. This is not unexpected, given the pace of change in business today and the number of competing priorities which divert management attention.

Businesses evolve and morph quickly, whether changing the way they do business, adopting new and emerging technologies, building new processes, bringing in new business partners or third parties, or undergoing integrations, mergers, or acquisitions. However, all these things change the way businesses use data, as well as changing who has access to it, what they do with it, and where it is located. Individuals are becoming more aware of their privacy rights and want to engage with businesses who will not use their personal data in unethical ways or let it fall into the wrong hands.

Therefore, complacency can lead to serious consequences and put your business, employees, and customers at risk. Moving forward steadfastly and continuing to make the appropriate investments is critical.

Businesses evolve and morph quickly, whether changing the way they do business, adopting new and emerging technologies, building new processes, bringing in **new business partners or third parties, or undergoing integrations, mergers, or acquisitions.**

Recommendations

- **Gain an understanding of what data you currently have.** Scrutinize what kind of information you have. Determine where you store it, know who has access to it, what you do with it, how you use it, with whom you share it, why you need it, and how you need to protect it.
- **Employ the appropriate persons for the job.** Appoint appropriately qualified and skilled data protection professionals, and engage trusted partners, as they will work with you to transform data protection legislation into business practices which support compliance.
- **Implement strong data governance mechanisms.** Ultimately, data protection is about managing the personal data you use in your business, and ensuring you have appropriate controls and oversight, as well as reporting compliance to validate the effectiveness of your controls. Ask yourself: 'Do we apply rules relating to data classification and quality? Do we have master data records management? Are robust retention and records management policies and procedures in place?'
- **Drive towards continuous security.** Data protection is not a one-time implementation, but an ongoing practice of data protection processes integrated into the business' daily operations.

[12] *www.helpnetsecurity.com/2019/09/30/companies-gdpr-readiness/*

Individuals are becoming more aware of their privacy rights and want to engage with businesses who will not use their personal data in unethical ways or let it fall into the wrong hands.

Conclusions

Hummingbirds are amongst the fastest and most agile species in nature.

They are the only genus of bird that can sustain long-term hovering - and even fly upside down when required. They've developed a long bill in order to extract nectar with precision. And when resources are scarce, they can enter near-hibernation – known as torpor - to protect their reserves.

Conclusions

Constant pressures in the market and the need to deliver consistent, reliable services is much more than having the ability to recover from disruptions. Cyber-attacks can take weeks, if not years, to recover from, which is a key reason why organizations must have the ability to anticipate and prevent disruptions. Successful organizations account for all aspects of business operations, technology, people, and controls to actively manage disruptive events – before the event impacts regular operations.

Conclusions

Based on the observations related to current and emerging threats presented within this report, organizations should focus effort in the following areas:

Organization's must implement infrastructure, applications, and operations which are secure by design, meaning including security is a key and conscious decision in the approach to designing business solutions end-to-end. Evaluate your current state of cyber-resiliency and define the desired future state. Ensure inclusion of key performance indicators and proper reporting to maximize feedback and to identify potential issues. Place cyber-resiliency at the top of your organization's priority list, and ensure it is part of your leadership team, and board discussions.

Leverage intelligent cybersecurity in support of business agility and maintain an acceptable risk level for the organization. Leverage proactive threat intelligence capabilities to identify and rapidly make decisions to manage risk. Organizations should also consider leveraging guidance from frameworks such as MITRE ATT&CK, to help guide and enhance their cybersecurity posture.

Ensure your organization has proper visibility across the information and communication technology environment. A vital part of being able to manage risk and mitigate threats is having proper real-time visibility into activities happening within the ICT environment, so rapid decisions can be made on how to best address the threat.

Conduct regular penetration testing activities, which include application testing and social engineering. Leverage intelligence services to help add a realistic approach from an attacker's perspective.

Continue evolving defenses around managing risks related to malware. As discussed in this report, malware continues to mature. A single malware detection capability is also often a single point of failure as no individual product can detect all types of malware. Ensure your malware defenses are designed appropriately and measure their effectiveness to ensure maximum benefit.

GRC must be part of your organization's regular agenda. Conduct regular technical and non-technical assessments to identify potential weak areas of your program. Abandoning traditional approaches to cybersecurity is important to consider as threats continue to become more complex. Organizations who fail to adopt a new mindset will suffer from the continued evolution of the threat landscape, constantly changing regulations, and standards.

As the cybersecurity landscape continues to evolve, and based on the trends and behaviours identified, in the year ahead we are likely to observe the following activity throughout 2020:

- **Evolution of the sophistication** of malware capabilities related to targeted ransomware. The threat of ransomware is still very real, and attackers will leverage compromised systems in ways which are more beneficial to them. Focused attacks on industries will prove to be valuable to attackers as it will provide the capability of maximum disruption to the organization.
- **Additional reconnaissance**, compromise, propagation and botnet activity related to IoT devices. With the deployment of 5G networks and associated devices, we will likely observe as significant increase in attacks against IoT.
- **Continued deployment of spyware** and keyloggers as attacker toolkits and techniques evolve. Collection of critical information, including credentials and other types of data will support attackers' efforts in automation and gaining further access to organizations.
- **Malicious actors utilizing** machine learning and artificial intelligence to support targeted phishing campaigns. As legitimate businesses are making use of artificial intelligence to spread development, research, and task automation, attackers will leverage the same types of capabilities to accelerate their operations.

Above all, remember that the true purpose of cybersecurity controls within an organization is to enable that organization to meet its operational goals in a safe, secure, and resilient manner.

NTT Ltd. global data analysis methodology

The NTT Ltd. 2020 Global Threat Intelligence Report contains global attack data gathered from NTT Ltd. and supported operating companies from October 1, 2018 to September 31, 2019. The analysis is based on log, event, attack, incident, and vulnerability data from clients. 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.

NTT Ltd. gathers security log, alert, event, and attack information from which it enriches and analyses contextualized data. This process enables real-time global threat intelligence and alerting. The size and diversity of our client base, with over 10,000 security clients on six continents, provides NTT Ltd. 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 the 10 SOCs and seven research and development centers of NTT Ltd. provides a highly accurate representation of the ever-evolving global threat landscape.

The Cybersecurity Advisory data used within this report includes sanitized current and target state maturity levels analysed globally 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 over 150 assessments used to measure client the maturity of processes, metrics, and tools. The focus areas for the evaluation include:

Security Vision and Strategy, Information Security Framework, Risk Management, Operations, Applications, Devices, and Infrastructure.

The application security data and analysis are provided by WhiteHat Security. This data is collected from our Dynamic Application Security Testing (DAST) 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 Open Web Application Security Project (OWASP). Vulnerabilities are rated on five levels of risk – Critical, High, Medium, Low and Note. Critical and high-risk vulnerabilities taken together are referred to as 'serious' vulnerabilities. Vulnerability classes are based on the threat classification of Web Application Security Consortium (WASC).

NTT Ltd. resource information

Global Threat Intelligence Center

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

- Threat research
- Vulnerability research
- Intelligence fusion and analytics
- Communication to NTT Group clients

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

Leveraging intelligence capabilities and resources from around the world, NTT Ltd.'s 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 (TTP) used by attackers.

Vulnerability research pre-emptively uncovers zero-day vulnerabilities which are likely to become the newest attack vector, while maintaining a deep understanding of published vulnerabilities. With this knowledge, NTT Ltd.'s security monitoring services can more accurately identify malicious activity which is 'on-target' to NTT Group 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; and works to understand, analyse, and enrich those threats using advanced analysis techniques and proprietary tools; and curates and publishes them using the Global Threat Intelligence Platform (GTIP).

NTT-CERT

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 NTT Ltd. companies' capabilities in the security services and secure network services fields. To learn more about NTT-CERT, please visit www.ntt-cert.org.

How can we help you?

Get in touch with us today for a **Cybersecurity Advisory engagement.** We'll help you to **understand your current risk-profile** to chart your **future security strategy.** Or, if you're ready to work with a **partner to manage, monitor and optimize** your security posture, **reach out to us** and one of our **Managed Security Services** experts will be in touch.

Together we do great things