
2018
GLOBAL THREAT INTELLIGENCE REPORT
NTT Security

PARTNERING FOR GLOBAL SECURITY

www.ntt.com

www.nttdataservices.com

www2.dimensiondata.com

Table of Contents

Note from our CEO

At NTT Security, we don't separate Information and Communication Technology (ICT) from cybersecurity because adversaries certainly do not. Cyber criminals collaborate to perpetrate crime, and in contrast organizations must also break down internal silos to address threats. As a leading provider of cloud computing services in multiple data centers globally, we understand the power of technology is fundamentally transforming our economy and as organizations look to cloud infrastructure to leverage its capabilities, they must remain resilient in the face of these threats. The cybercriminal underground is an environment in which cyber criminals rely on each other for goods and services, operating globally, completely unhampered by government security revelations. This threat landscape continues to evolve, as adversaries exploit mobile devices, cloud technology, and devices intended to be used as part of the Internet of Things (IoT) in all levels of attacks. This report illustrates shifts in attacker focus across geographic regions and industry sectors, helping provide a deeper understanding of what organizations should consider during business operations, as well as for business continuity and disaster recovery planning. Some of the attacks we highlight in the report include malware such as WannaCry and NotPetya, denial of service and web application attacks and their direct focus on particular regions and industries. NTT Security provides a world class threat intelligence service to help you get a view of your security posture because you simply cannot measure what you cannot see. As a full stack ICT provider/internet service provider with partners like Dimension Data, NTT Communications and NTT DATA, we continue working together to provide cyber resilience using a combination of consulting, managed, cloud, and hybrid services.

Jun Sawada

Chief Executive Officer

NTT Security

The cyber world continues to expand, uniting information and operational technology, industrial controls and the Internet of Things into an ever-evolving environment across on-premise, cloud and mobile devices. The NTT Security 2018 Global Threat Intelligence Report highlights notable threats, incidents and trends observed during the previous year.

In this report, we analyze attacks against 18 industry sectors and share our observations on some of the more highly targeted sectors in each region. Starting with the Europe, Middle East and Africa (EMEA) section of the report, we follow each region's highlights with an exploration into an industry sector which was highly targeted within the region, as well as provide an overview of what we believe will have the biggest regional impacts in 2018. We also included independent analysis for Japan, which is not included in the APAC regional results of the report. This is due to our special focus on the upcoming 2020 Olympic Games to be hosted in Japan and resulted in separate data analysis focusing on threats affecting the country. For you, the reader, this may a provide a valuable look at specific threats, helping you prepare for the year ahead.

NTT Security leveraged our visibility into global internet traffic and threats faced by thousands of customers across many industries. Security research and investigations provide threat intelligence from our global security operations centers (SOCs) and research centers with thousands of security analysts analyzing millions of attacks. Our aim is to share our findings, without using highly technical language, to satisfy a wide range of readers – security is everyone's responsibility.

As in previous years, we observed shifts between attack targets, source and destination attack profiles, and even types of technologies attacked. While attack types and targets can be revealing, attack sources continue to be problematic because of the difficulties in assigning attribution for a specific attack. NTT Security regularly identifies attack sources as an IP address from which a specific attack was launched. More often than not, that source is an offensive base or launch point used by the attacker, who is often located somewhere else entirely. NTT Security researchers have come to expect shifts in attacks, as technologies change and so do adversaries' tools, tactics and procedures. Where there were significant changes in focus, we have highlighted reasons why we believe the shift occurred. The lessons learned from our observations are directly reflected in our recommendations.

With standards groups, industries and governments implementing new and revised policies, many organizations will continue to face an uphill battle in achieving an optimal balance between operational security and compliance initiatives. The successful chief information security officer (CISO) needs to comply with those initiatives, while requiring a firm grasp on what it takes to remain secure, realizing security is a fundamental requirement for business today. And good CISOs realize they cannot do it alone. Given the

Executive Summary

nature of threats faced in today's world, we should be embracing the fundamental principal that we are all, by default, part of the organization's security team. Those who embrace this understanding will excel and increase resilience against both cybercriminals and traditional threats. Over the last 10 years, one observation remains steadfast: our adversaries operate on a global level, and we must invest in capabilities, people, processes and controls which scale.

A key part of any organization's capability to detect and mitigate threat is its ability to apply intelligence. NTT Security focuses on the production and application of threat intelligence because it provides significant value to our clients. Threat intelligence platforms and collaboration tools supercharge NTT Security's capability to provide intelligence derived from our global relationships. We provide our clients with valuable threat intelligence, supporting strategic decisions to help balance budget, risk and attack mitigation.

Compelling research illustrates ransomware and other endpoint attacks are still on the rise, and systems directly exposed to the internet remain prime targets for cyberthreats. To address this, organizations should take a multi-prong approach, including making the best use of information and intelligence sources to help recognize and prioritize threats in an effective manner, and to increase opportunities for an organization to mitigate threats before they result in a significant impact. Additionally, organizations should apply a fair balance of endpoint and network-based controls, as well as ensure incident response capabilities are suited to handle a wide range of scenarios. Along with these proactive controls, organizations should continue to monitor network and host activity, to address threats traversing their environments.

LEADERSHIP PRINCIPLES FOR ADDRESSING CHALLENGES:

Security must allow the business to move at market speed – safely

Global reach, time to market, and having a product or service which outpaces your competition are often the core focus of organizations today. There is tremendous value in being flexible and having the drive to constantly be on top of the latest trends. Even cutting-edge businesses have fallen victim to the most elementary of attacks, highlighting the importance of scaled growth between their market prowess and their approach to security.

Large breaches and constant security challenges must not cause complacency

Even with many of the world's top enterprises being breached and publicized on the evening news, we cannot consider this to be the "new normal." This rationale leads to a lax attitude towards security, with only compliance keeping us engaged in the practice. It is not "normal" to be compromised, and in the eyes of stakeholders, it is certainly unacceptable. First class organizations will learn from the faults of others and use this knowledge to constantly improve their own resilience.

Security is still everyone's responsibility and must be usable by people

Lastly, security is still everyone's responsibility, from the janitor to the Board of Directors and entire C-Suite. Fail to train everyone within the chain of command and you will surely find weak links, regardless of salary and title. Empower your employees to do the right thing. Educate them that it is okay to question something if it "just doesn't seem right." Just as there are no dumb questions, there are no insignificant events. If an employee observes suspicious or fraudulent activity, it is far more cost-effective to identify and stop a potential threat than to respond to one which has already occurred.

Our intention is that this report will enable you to adjust your strategic vision, improve your own daily security practices, and help you with data points and citations in your business conversations. All organizations have different risk thresholds, and although the recommendations included in this report apply to many, it is best to refer to your own risk profile and implement defensive measures as appropriate.

NTT Security's analysis of global monitoring data, vulnerability data, and incident response data revealed a variety of findings about attacks and organizational experiences. This section highlights some of the more interesting findings.

Global Findings

Industry Sectors

- Finance became the most attacked sector, with 26 percent of all attacks. This was an increase from 14 percent of all attacks in 2016. Finance also ranked as the first or second most attacked sector in all regions except Japan.
- Attacks against the technology sector increased about 25 percent from 2016 levels. This helped make technology the only sector to rank in the top five attacked industries for all regions, while ranking second globally for volume of attacks, at 19 percent.
- The business and professional services sector was new to the list of top five globally attacked industry sectors. It ranked third with 10 percent of global attacks.
- The retail, manufacturing and finance sectors were in the top five attacked industry sectors in four of the five regions.
- Financial services (18 percent) and health care (15 percent) were the two most common sectors to seek incident response services.

Malware Types

- Spyware/keyloggers ranked first in volume of malware, at 26 percent. Regional differences were significant, with spyware/keyloggers at 39 percent of malware in the Americas but only three percent in EMEA.
- Trojans/droppers ranked second globally at 25 percent; however, they represented 62 percent of malware in Japan.
- Globally, virus/worms were the third most common form of malware at 23 percent, but spiked to 66 percent in the Asia Pacific (APAC) region.
- Ransomware volume was up 350 percent, rising from less than one percent of global malware in 2016, to nearly seven percent. But in EMEA, ransomware was the leading malware type at 29 percent, focusing mainly on gaming, business and professional services, and health care industry sectors.
- Ransomware-related incident response engagements dropped from 22 percent in 2016 to five percent in 2017.
- Globally, 75 percent of ransomware detected was Locky (45 percent) or WannaCry (30 percent).

Attack Source Countries

- The United States ranked as the first or second most common attack source in all five regions.
- China ranked first as an attack source country only for EMEA, and second or third for the remaining regions.
- The Netherlands ranked among the top five attack source countries in four regions, missing the EMEA region by less than a quarter percent.
- Top attack sources were often located in the same region as their victims, except that the Russian Federation was ranked fourth in the Americas, Romania was ranked fourth in APAC, and Ukraine was ranked fourth in Japan.

EMEA Findings

- Ransomware ranked first on the list of top malware in EMEA, at 29 percent, in sharp contrast to only seven percent of global malware.
- Business and professional services became the most attacked sector in EMEA with just over 20 percent of attacks.

- A 25 percent increase in the volume of attacks against the technology sector resulted in a jump from two percent of attacks in 2016 to 14 percent of attacks in 2017. Technology entered the top five most targeted sectors in EMEA.
- The leading attack source countries were China at 21 percent, followed by the United States at 18 percent. EMEA was the only region where China ranked ahead of the United States as a source of attacks.
- China was the attack source country for 67 percent of hostile activity targeting the manufacturing sector in EMEA.

Americas Findings

- Finance sector attacks increased to 43 percent of attacks in the Americas, up from 15 percent in 2016.
- Finance faced 59 percent of phishing attacks in the Americas. Over three quarters of phishing campaign attachments were malicious Microsoft Word documents.
- Increased attacks against technology raised that sector to 27 percent of attacks in the Americas, up from the 11 percent observed in 2016.
- The finance and technology sectors together accounted for 70 percent of all attacks against targets in the Americas.
- Manufacturing attacks dropped from 23 percent to five percent of attacks.
- Activity from two source countries – the United States and China – accounted for 62 percent of attacks in the Americas. In the finance sector, 70 percent of attacks came from the United States.

APAC Findings

- Attacks against the finance sector decreased from 46 percent in 2016 to 26 percent in 2017, but it remained the most attacked sector in APAC.
- Australia was the source country for 66 percent of the attacks against the finance sector.
- Increased attacks against education resulted in the sector jumping from nine percent of attacks in 2016 to 18 percent of attacks in 2017. With 64 percent of hostile activity, brute force attacks dominated the education sector in APAC.
- For retail targets within APAC, the United States and Australia were the sources of 93 percent of attacks, and brute force attacks led with 64 percent of the hostile activity.
- For the government sector, 84 percent of attacks originated from Australia-based IP addresses.
- Virus/worms accounted for 66 percent of malware in APAC, compared to 23 percent globally, nearly triple the percentage.

Japan Findings

- Japan accounted for 26 percent of all attacks against Japanese targets and was the leading attack source country for all five top industry sectors in Japan. Japan was the only region which did not show the U.S. and China as the top two attack sources.
- Trojans/droppers accounted for 62 percent of malware in Japan, more than double the global percentage and five times the percentage in APAC.
- With 24 percent of all attacks, manufacturing was the most attacked industry sector in Japan, with reconnaissance as the leading hostile activity at 47 percent.
- Brute force attacks were common in Japan, making up nearly 17 percent of all attacks, but also accounting for over 22 percent of attacks against manufacturing, and 41 percent of attacks against the media sector.
- The technology sector ranked as the third most attacked sector, with 17 percent of attacks.

Focus on Global

The global cybersecurity landscape was dominated by change. This included changes in attack sources; changes in the types of attacks being executed; and changes in the targets of those attacks, as ransomware escalated, attacks against finance and technology jumped, and government targets were deprioritized.

These changes include updates to the topmost attacked industries. Finance became the most attacked sector during the year, but this was not as much because of a dramatic increase in attacks against finance as it was because of a relative decline in attacks against other sectors, like government. The bigger news is the 25 percent increase in attacks against the technology sector, which made it the only sector to appear in the top five most attacked sectors in every geographic region.

Attacks against applications dominate most of the activity, but that is also not a significant difference from the previous year. Ransomware detection, on the other hand, was up about 350 percent, representing an increase in ransomware in nearly every region.

Despite the evolutions in attacks, one trend has remained the same year after year; attackers tend to attack using regional resources. Globally, and within each region, a significant number of attacks originate within the same region and often the same country as the victim. Attack sources continue to be problematic because of the difficulties in assigning attribution for a specific attack. NTT Security regularly identifies attack sources as an IP address from which a specific attack was launched. More often than not, that happens to be an offensive base or launch pad used by the attacker, who is often located somewhere else entirely. Observing sources like the Netherlands appearing in the top six attack sources in every region is a perfect example of this. There are not millions of cybercriminals in the Netherlands attacking targets around the world. There are, however, many cybercriminals located at various locations around the world, who are using remote computing resources within the Netherlands. Compromised systems, purchased hosting, outsourced exploit kits or botnets are making it easier than ever for attackers to maximize local resources, and obfuscate their trail.

Global Key Findings

Global Attacks Source Countries

- The United States ranked as the first or second most common attack source country for all five regions, with the likelihood that U.S. resources are being misused by outside attackers.
- China ranked first only for attacks against EMEA, but second or third for the remaining regions.
- The Netherlands ranked in the top five attack source countries in four regions, missing the fifth region by less than a quarter of one percent.

Global Industry Sector Attacks

- Financial industry attacks totaled 26 percent, up from 14 percent in the previous year.
- Business and professional services is a new member of the top five most attacked sectors, ranking third with 10 percent of attacks, consistent with the previous year.
- Government-focused attacks totaled five percent, down from 14 percent last year. The trend shows a de-prioritization of government targets compared to other targets, as government targets fell to seventh globally.

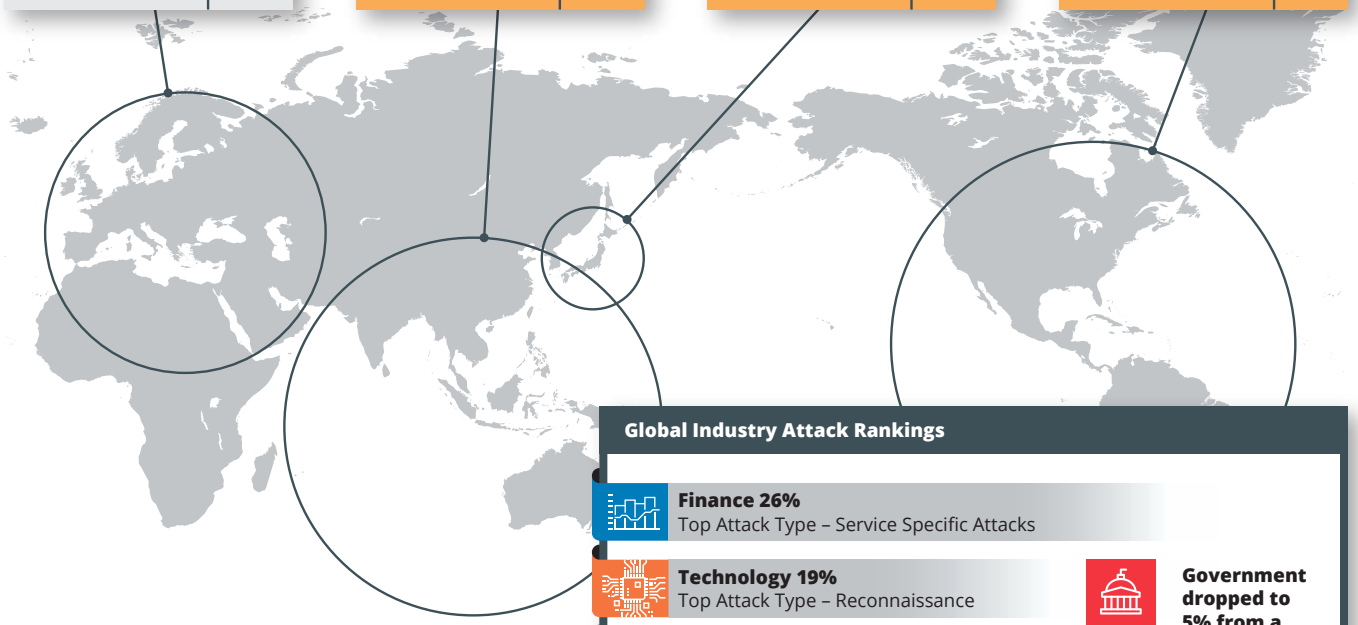
Top Five Attack Source Countries by Region

EMEA	
China	21%
United States	18%
United Kingdom	5%
Norway	4%
Germany	4%

APAC	
United States	31%
China	12%
Australia	10%
Romania	6%
Netherlands	4%

Japan	
Japan	26%
United States	21%
China	11%
Ukraine	3%
Netherlands	3%

Americas	
United States	39%
China	23%
France	3%
Russian Federation	3%
Netherlands	3%



Global	
United States	27%
China	19%
Netherlands	4%
France	4%
Germany	3%

Global Industry Attack Rankings

- **Finance 26%** Top Attack Type – Service Specific Attacks
- **Technology 19%** Top Attack Type – Reconnaissance
- **Business & Professional Services 10%** Top Attack Type – Known Bad Source — New Top 5
- **Manufacturing 9%** Top Attack Type – Known Bad Source
- **Retail 8%** Top Attack Type – Brute Forcing

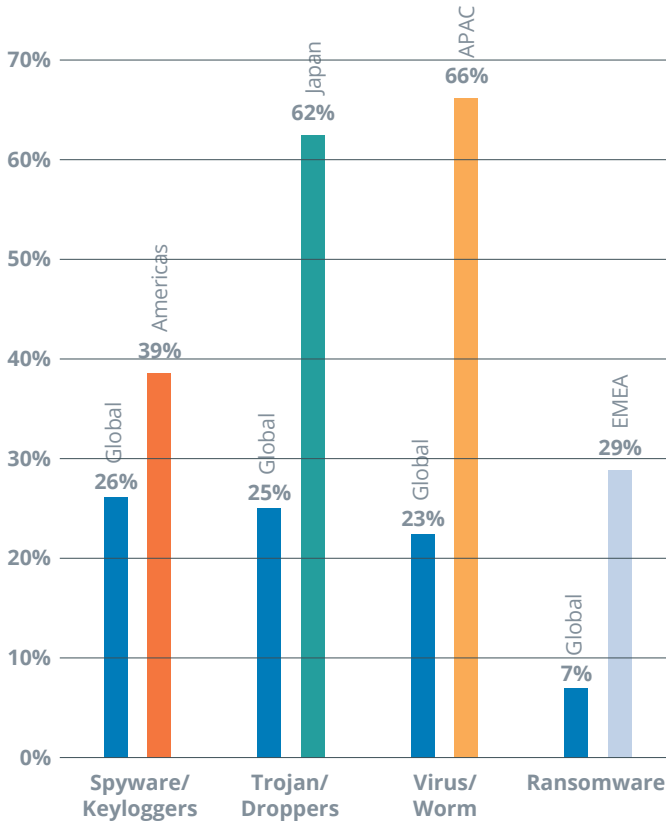
Government dropped to 5% from a previous year of 14% Top Attack Type – Network Manipulation

- Technology was the only sector ranked in the top five attacked industries for all regions.
- Finance ranked as the first or second most attacked sector in all regions except Japan.
- Finance, retail, and manufacturing sectors were among the top five attacked industry sectors in four of the five regions.

Global Top Malware

- Spyware/keyloggers ranked first at 26 percent of observed malware.
- Regional differences are significant with spyware/keyloggers at 39 percent in the Americas while only three percent for EMEA.
- Trojan/droppers were second globally at 25 percent, but accounted for 62 percent of malware in Japan.
- Virus/worms were third globally at 23 percent, but spiked to 66 percent in APAC.
- Ransomware was seven percent of global malware, up from one percent the prior year; however, at 29 percent, it was the leading malware type for EMEA, targeting mainly the gaming, business and professional services, and health care industry sectors.

Top Malware



Global Threat Highlights

Finance sector regained the top of the "most targeted" list, but technology is not far behind

Global attacks on the finance sector nearly doubled to 26 percent from 14 percent the previous year.

Spyware/keyloggers ranked first in global malware at 26 percent, indicating attackers' desire for a long-term presence. Finance, retail, and manufacturing were among the top five most frequently attacked sectors in four of the five regions, while technology was in the top five for all regions.

Finance ranked as the first or second most attacked sector in most regions, with attacks in the Americas (43 percent), EMEA (20 percent) and APAC (26 percent). Attacks against the financial sector were characterized by extensive use of spyware and keyloggers. For the year, spyware and keyloggers accounted for nearly 26 percent of all detected malware.

Attacks were weaponized faster as attackers developed reliable exploits for high profile vulnerabilities. WannaCry spread around

Apache Struts is a free, open-sourced framework to support Java web applications. Struts is widely used around the world by many organizations in many countries. In March 2017, Apache released two security bulletins (S2-045 and S2-046) which described how attackers could compromise affected systems with the related flaws.

Rank	Global	EMEA	Americas	APAC	Japan
#1	Finance 26%	Business & Professional Services 20%	Finance 43%	Finance 26%	Manufacturing 24%
#2	Technology 19%	Finance 20%	Technology 27%	Education 18%	Retail 18%
#3	Business & Professional Services 10%	Manufacturing 18%	Business & Professional Services 9%	Technology 16%	Technology 17%
#4	Manufacturing 9%	Technology 14%	Manufacturing 5%	Retail 15%	Media 11%
#5	Retail 8%	Government 9%	Retail 5%	Government 13%	Education 8%

the world, setting a new standard for the speed with which it spread. Soon afterward, vulnerabilities in Apache Struts were announced. Effective attacks led the Apache Struts vulnerabilities to become the most exploited vulnerabilities for several months, well after patches were available.

Ransomware increases and turns destructive

Cybercriminals continued to search for exploitable vulnerabilities and use social engineering as a core tactic. They expanded into supply chain infections and the widespread use of destructive malware masquerading as ransomware. Globally, ransomware represented seven percent of malware, up from one percent a year ago. Leaks of classified government hacking tools have only made ransomware more dangerous, as seen by the greater sophistication of attacks, tools, and automation. As ransomware attackers shift their focus towards businesses and away from consumers, performing data backups and developing plans for incident response and disaster recovery become even more critical.

Security is not a stand-alone silo

In the NTT Security 2017 Risk:Value Report, we interviewed over 1,300 business decision-makers globally, gaining insight into how they perceived risk and what steps they are taking to mitigate potential impact.

According to data from the NTT Security 2017 Risk: Value Report, poor information security is ranked fifth at 12 percent for top risk concerns, down from 18 percent in the 2015 report. The number one risk concern globally was competitors taking market share, followed by lack of employee skills and the increase of global competition.

Security continues to evolve and instead of maintaining a perimeter mindset and a siloed approach, organizations are making security part of key processes for business enablement and risk assessment. But the digital transformation of business to cloud and mobile apps has increased development cycle times, strained operations, and introduced new vulnerabilities which offer opportunities for cybercriminals. The topic of security is often not part of software developers' training, nor historically included in development lifecycles. This is changing as security becomes more integrated with development and operations. More integrated security processes can help teams identify vulnerabilities within applications and supply chains, secure access credentials and confidential information, and leverage automation to maximize security and support operations.

Service-specific attacks are attacks directed at services running on a server, desktop or mobile device. Such attacks attempt to take advantage of non-authentication related vulnerabilities. The most frequent of these are exploits against common services such as SMTP, DNS and SMB, but they often target database and remote access services like FTP and Telnet. Such attacks often provide the attacker access to the underlying system with permissions based on the logged-on user or of the targeted service, and can allow the attacker to install additional malware for further exploitation.

The attack surface continues to expand rapidly

One proactive step all organizations can benefit from is adopting multi-factor authentication, as identity becomes a new perimeter driven by cloud and mobility. While there is constant flux in the number of zero-day vulnerabilities, web attacks using known vulnerabilities remain a problem. The Internet of Things (IoT) and industrial control systems, plus mobile and non-Windows operating systems, are increasing the attack surface area and should not be ignored.

With 19 percent of global attacks in 2017, technology was the second most attacked sector. Technology ranked in the top four in EMEA, the Americas, APAC and Japan, and was number two globally. Attack volume against the technology sector increased by about 25 percent overall. This was enough to increase the percentage of attacks against technology in every region – in most cases, as much as four to five times.

Attacks in finance and technology were marked by attempts to further attackers' existing control and maintain long-term access for information gathering.

Both finance and technology industries were highly targeted during 2017 compared to 2016, but attackers focused on the industries in different ways. Attacks against finance were characterized by service-specific attacks (23 percent), web application attacks (19 percent), and application-specific attacks (17 percent). This means 59 percent of hostile activity was related to specific, known attacks against the organization's web presence.

The technology sector was characterized by more reconnaissance activity (18 percent) and known bad sources (16 percent). Reconnaissance activity is not necessarily hostile, though it is often a precursor to more hostile attacks. Activity from known bad sources is also not necessarily hostile, but is identified as activity from sites which are previously known to be associated with hostile activity.

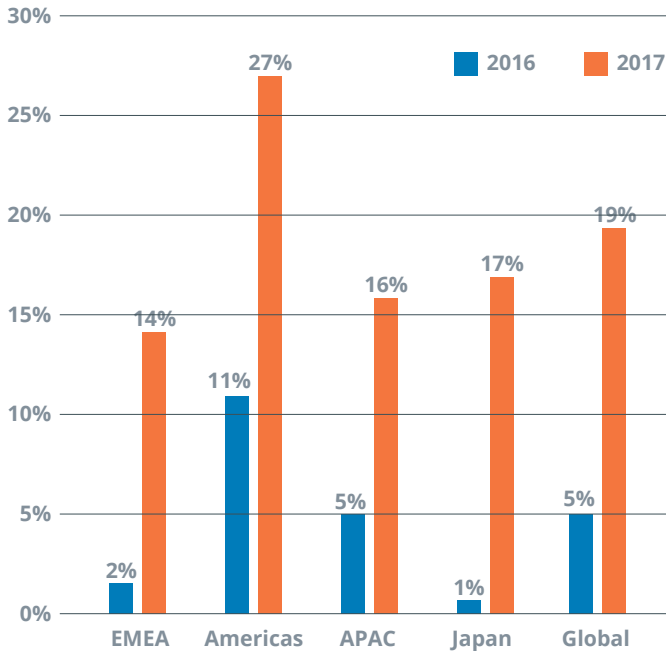
Ransomware increases over 350 percent but is handled better

Ransomware was still a relatively new attack vector in 2016, accounting for less than one percent of all malware detections. During 2017, ransomware rose to nearly seven percent of all malware, a significant increase. Compared to other malware volumes, this was over a 350 percent increase in ransomware detections from 2016.

While the volume of ransomware was rising, ransomware incident response engagement fell from over 22 percent of incidents in 2016 to just over five percent in 2017. Better vendor response, better detection, more effective policies and procedures, improved awareness, and better incident response plans resulted in a decrease in ransomware incidents, despite the 350 percent increase in ransomware detections.

> Analysis reveals that while payment of ransomware demands does explain some of the decrease in incident response engagements, more of that drop is due to better preparation.

Attacks Against Technology



In the NTT Security Risk:Value Report, 48 percent of respondents indicated they have an incident response plan in place today, with another 31 percent currently working on such plans. On the other hand, eight percent indicated they do not know if they have a plan and two percent indicated "No, and we have no plans to implement one." So, while the decrease in ransomware incidents response suggests organizations are better managing some incidents, no one should be lulled into a false sense of accomplishment. In general, incident response plans must continue maturing to be as effective as possible.

The gaming sector was the most targeted by ransomware during 2017. Several of the sectors most targeted by ransomware are characterized by high uptime requirements as they have operations which are time sensitive, or outages could lead directly to losses of revenue. Some other sectors are highly sensitive to theft of intellectual property because of the nature or private information, or specific information which gives that company a competitive advantage. While NTT Security detected ransomware attacks in every industry sector, the top five targeted sectors accounted for 72 percent of all ransomware detections.

Seventy-five percent of detected ransomware was either Locky (45 percent) or WannaCry (30 percent), with all other varieties of ransomware combined making up the remaining 25 percent.

Recommendations based on global trends

- **Mitigate the impact of ransomware.** Minimize the amount of data which can be impacted by enforcing "need to know" and implementing data and network segregation. Enforce good endpoint hygiene, including responsible computing usage and end-user training to reduce the chances users will execute hostile attachments. Maximize the effectiveness of monitoring to identify ransomware infections as soon as possible. Enforce good backup strategies and store some backups offline.

- **Consider advancing your security program.** Businesses are moving with faster development cycles for web and mobile applications to enable their digital transformation, first driving agility into DevOps and secondly security into DevSecOps. The attack surface today is fed by continuous releases of features and application components exposing new vulnerabilities daily versus traditional release cycles with vulnerabilities only occurring at longer intervals. According to NTT Security analysis of detected attacks, once a vulnerability was identified, the average timeframe required for attackers to field an exploit was just over 48 days. To manage the evolution of new threats in a timeframe this short, an organization's development and environment management practices need to be agile. Evolving towards effective DevSecOps can significantly advance the effectiveness of an organization's security program.

- **Make the best use of information and intelligence sources.** For many organizations, it is hard to keep up with current attack techniques, exploits and campaigns. Use threat intelligence capabilities to identify threats to your organization and its resources. Threat intelligence services can help prioritize security resources in an effective manner, and potentially mitigate threats before they result in a significant impact.

The "gaming" sector is primarily gambling (poker, casinos, and sports betting) and associated supporting businesses.

DevSecOps is a security management philosophy which strives to embed security methodology, controls and tasks into a dynamic development workflow which encompasses application security, automated testing and is designed to be operations-aware so that end products can be more easily implemented in a secure manner.

Global Targets of Ransomware

- **20%** Gaming
- **17%** Business and Professional Services
- **12%** Health Care
- **12%** Manufacturing
- **11%** Technology
- **28%** All Others

Ransomware Varieties

- **45%** Locky
- **30%** WannaCry
- **25%** All Others

Focus on Global

2018

NTT Security

Global Industry by Attack Source Country and Attack Type

Finance 26%

United States	39%	Application-Specific Attacks 24% Web Application Attacks 19% Brute Forcing 14%
Australia	29%	Service-Specific Attacks 55% Web Application Attacks 15% Application-Specific Attacks 13%
China	5%	Reconnaissance 37% Known Bad Source 33% Application-Specific Attacks 12%
Sweden	3%	Network Manipulation 46% Denial of Service Attacks 13% Web Application Attacks 11%
Germany	2%	Web Application Attacks 25% Reconnaissance 19% Application-Specific Attacks 16%

Finance returned to its position as the most attacked industry for the first time since 2014.

Technology 19%

United States	26%	Service-Specific Attacks 20% Known Bad Source 18% Application-Specific Attacks 16%
Australia	17%	Service-Specific Attacks 43% Web Application Attacks 30% Network Manipulation 12%
China	11%	Known Bad Source 32% Reconnaissance 25% Application-Specific Attacks 23%
India	4%	Evasion Attempts 78% Application-Specific Attacks 6% Web Application Attacks 5%
Japan	4%	Network Manipulation 35% Web Application Attacks 24% Reconnaissance 16%

Due to a 25 percent increase in attack volume, technology jumped in every region, as well as globally.

Business & Professional Services 10%

United States	34%	Web Application Attacks 26% Service-Specific Attacks 19% Denial of Service Attacks 17%
China	23%	Known Bad Source 86% Denial of Service Attacks 6% Reconnaissance 5%
Netherlands	5%	Denial of Service Attacks 29% Service-Specific Attacks 27% Known Bad Source 20%
Australia	4%	Service-Specific Attacks 46% Web Application Attacks 39% Application-Specific Attacks 7%
Norway	3%	Web Application Attacks 36% Application-Specific Attacks 35% Denial of Service Attacks 20%

Known bad sources led all hostile activity against business and professional services globally, with 34 percent, and web application attacks second at 21 percent.

Manufacturing 9%

Australia	34%	Network Manipulation 33% Web Application Attacks 17% Application-Specific Attacks 15%
United States	18%	Service-Specific Attacks 28% Web Application Attacks 27% Known Bad Source 12%
China	18%	Known Bad Source 85% Reconnaissance 7% Application-Specific Attacks 4%
Japan	9%	Reconnaissance 58% Known Bad Source 21% Brute Forcing 6%
Netherlands	2%	Network Manipulation 37% Service-Specific Attacks 29% Known Bad Source 9%

Known bad sources led hostile activity against manufacturing at 24 percent, followed by reconnaissance activity at 17 percent and web application attacks at 14 percent. Australia was the lead attack source for the manufacturing sector, but was not within the top five source countries for targets within EMEA or the Americas.

Retail 8%

United States	39%	Brute Forcing 79% Web Application Attacks 14% Reconnaissance 2%
Australia	31%	Brute Forcing 60% Application-Specific Attacks 26% Service-Specific Attacks 12%
Japan	10%	Denial of Service Attacks 54% Application-Specific Attacks 36% Web Application Attacks 5%
China	3%	Brute Forcing 39% Reconnaissance 26% Known Bad Source 16%
Netherlands	3%	Brute Forcing 69% Web Application Attacks 11% Known Bad Source 7%

Brute force attacks represented 55 percent of hostile activity targeting retail.

Focus on Europe, the Middle East and Africa (EMEA)

The General Data Protection Regulation (GDPR) was one of the most significant cyber topics within Europe, the Middle East and Africa throughout 2017. With defined intermediate goals, and full compliance required by May 2018, GDPR is large and complex. Any large-scale compliance initiative has the potential to consume resources which would normally be assigned to other security-related projects.

According to the 2017 NTT Security Risk:Value Report, there is a large misconception among business leaders that the impact of GDPR only affects companies residing in European Union (EU) countries. This is false, as the scope affects any company processing data about EU citizens. From survey results, only 58 percent of respondents from Switzerland were aware of the requirements, followed closely by Germany and Austria at 53 percent. In the UK, only about 39 percent of respondents were aware that GDPR is a compliance issue. Later in this section, we provide an overview of GDPR to highlight the importance of the regulation for EMEA organizations and organizations in other regions that may be doing business with them.

The targeting of personally identifiable information (PII) remains a top priority for threat actors focusing on targets within EMEA. Protection of PII will likely become even more important as GDPR evolves the perception of PII. Public breaches like those of a well-known ride-sharing service and a global credit monitoring company elevated these concerns and raised significant discussions in the United Kingdom, Italy, and several other countries within EMEA.

EMEA also suffered through several ransomware campaigns, including WannaCry. Those campaigns, and other attacks, were felt by all 18 industry sectors which NTT Security analyzes on a regular basis, but over 82 percent of those attacks were directed at business and professional services. While NTT Security analysis focused on multiple sectors, this report specifically includes a highlight on business and professional services, as the target of over 20 percent of attacks, it was the most attacked sector in EMEA in 2017.

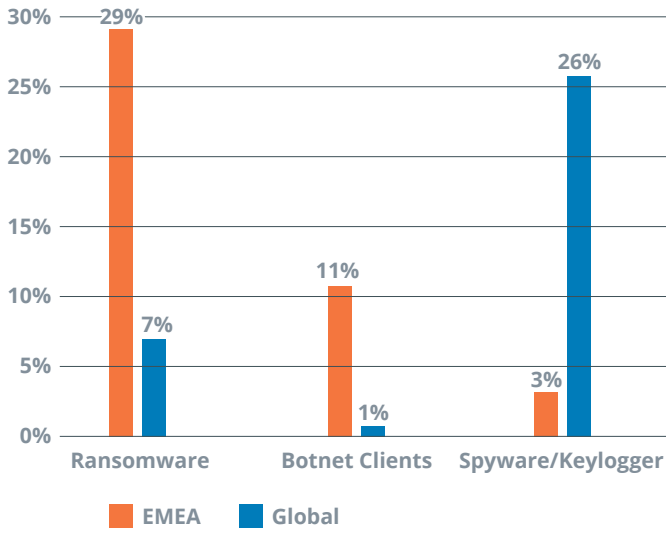
Focus on Europe, the Middle East and Africa (EMEA)

NTT Security

EMEA Key Findings

EMEA Top Malware

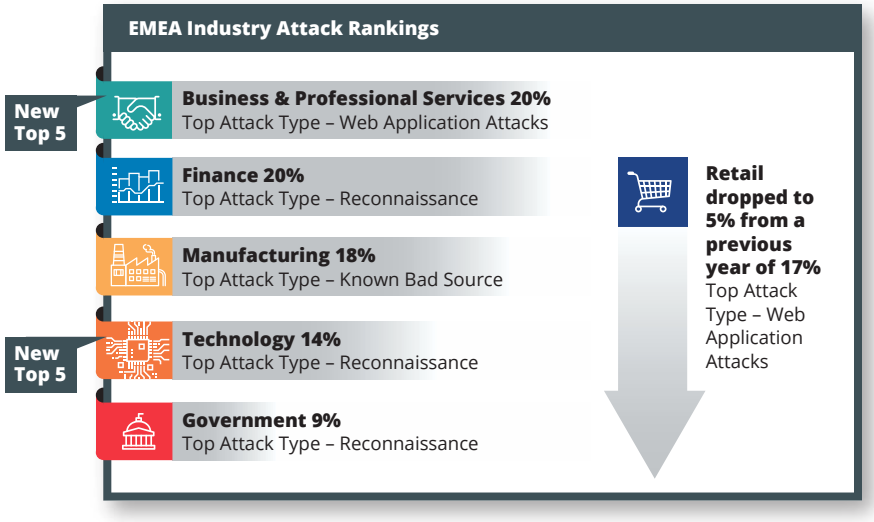
- Ransomware accounted for 29 percent of malware detections in EMEA, but only seven percent of global malware. Additionally, EMEA was the only region in which ransomware was the number one type of malware.
- Spyware/keyloggers made up only three percent of malware in EMEA, in sharp contrast to 26 percent globally.
- EMEA observed notably high volume of botnet client activity compared to global results (11 percent of malware vs. one percent of malware).



EMEA Industry Sector Attacks

- Business and professional services became the most attacked sector in EMEA, being the target of just over 20 percent of attacks.
- Technology totaled 14 percent of all attacks in the region and entered the top five sectors.
- Reconnaissance was the top hostile activity for finance, technology and government within EMEA and ranked second for almost every other industry sector for EMEA.
- The leading attack source countries were China at 21 percent followed by the United States at 18 percent and EMEA was the only region to observe more attacks from China than from the United States.
- For the manufacturing sector, China was the attack source country for 67 percent of attacks, mainly originating from known bad sources.

"Known Bad Sources" indicates that the site was labeled as a bad actor due to a variety of indicators, including internally identified hostile sites, sites which have repeatedly been responsible for attacks, or signatures and blacklists published by NTT Security threat research teams and from our trusted partners.



Focus on Europe, the Middle East and Africa (EMEA)

NTT Security

EMEA Industry by Attack Source Country and Attack Type

Business & Professional Services 20%

United States	18%	Reconnaissance 36% Web Application Attacks 33% Known Bad Source 16%
Norway	10%	Web Application Attacks 42% Application-Specific Attacks 31% Denial of Service Attacks 19%
Netherlands	9%	Denial of Service Attacks 61% Web Application Attacks 19% Application-Specific Attacks 15%
China	8%	Denial of Service Attacks 40% Application-Specific Attacks 23% Reconnaissance 20%
Switzerland	6%	Web Application Attacks 44% Application-Specific Attacks 44% Service-Specific Attacks 6%

Increased attacks pushed business and professional services to the most attacked industry in EMEA with 20 percent of all attacks. This is up from the 2017 GTIR, which showed the sector as the fourth most attacked industry in EMEA with just over 16 percent of attacks.

Finance 20%

United States	28%	Reconnaissance 38% Denial of Service Attacks 22% Known Bad Source 19%
China	10%	Reconnaissance 66% Known Bad Source 13% Web Application Attacks 8%
Sweden	5%	Denial of Service Attacks 24% Network Manipulation 20% Web Application Attacks 17%
Germany	5%	Reconnaissance 30% Denial of Service Attacks 22% Service-Specific Attacks 16%
France	4%	Reconnaissance 42% Denial of Service Attacks 27% Web Application Attacks 16%

Reconnaissance accounted for 40 percent of hostile activity against finance in EMEA, followed by DoS attacks at 17 percent. As with finance in most regions, web application attacks were also common, with 15 percent of all attacks.

Manufacturing 18%

China	67%	Known Bad Source 96% Reconnaissance 3% Application-Specific Attacks <1%
United States	7%	Known Bad Source 40% Reconnaissance 37% Web Application Attacks 12%
Germany	3%	Reconnaissance 76% Known Bad Source 12% Web Application Attacks 6%
France	2%	Reconnaissance 43% Known Bad Source 29% Application-Specific Attacks 13%
United Kingdom	2%	Web Application Attacks 30% Application-Specific Attacks 25% Reconnaissance 21%

Activity from China led all sources with 67 percent of attacks, with activity originating from a known bad source 96 percent of the time. This indicates a clear emphasis on manufacturing targets within EMEA from Chinese-sourced IP addresses.

Technology 14%

United States	24%	Reconnaissance 81% Known Bad Source 9% Network Manipulation 3%
China	13%	Reconnaissance 88% Known Bad Source 9% Application-Specific Attacks 1%
Russian Federation	6%	Reconnaissance 87% Known Bad Source 5% Denial of Service Attacks 3%
Sweden	5%	Reconnaissance 40% Web Application Attacks 29% Application-Specific Attacks 25%
United Kingdom	5%	Reconnaissance 32% Known Bad Source 22% Web Application Attacks 19%

Reconnaissance accounted for 71 percent of hostile activity against technology in EMEA. This is the highest level of reconnaissance for any industry sector in any region analyzed.

Government 9%

United States	11%	Reconnaissance 57% Known Bad Source 21% Application-Specific Attacks 7%
China	8%	Reconnaissance 64% Known Bad Source 27% Evasion Attempts 4%
Australia	8%	Evasion Attempts 79% Reconnaissance 15% Application-Specific Attacks 2%
United Kingdom	5%	Reconnaissance 75% Network Manipulation 9% Web Application Attacks 5%
Ukraine	4%	Reconnaissance 56% Web Application Attacks 26% Service-Specific Attacks 6%

While activity against government targets shows more variety than some other industry sectors, reconnaissance clearly stands out as the number one type of hostile activity.

EMEA Threat Highlights

Business and professional services became the top target within EMEA

With over 20 percent of attacks, business and professional services gained enough attention to take over the spot as the most attacked sector within EMEA. Attacks against financial services and manufacturing remained at levels comparable to our 2017 report. Technology and government rounded out the top five most attacked sectors.

Web application and application-specific attacks dominated activity against business and professional services in EMEA, often appearing as the most common attack types regardless of the source country.

Since NTT Security identified the business and professional services industry sector was highly targeted in this region, we discuss some additional specific observations and provide guidance that may help defend against evolving threats.

Ransomware attacks increase while spyware and keyloggers remain low

Within EMEA, ransomware accounted for 29 percent of all detected malware, well above the global rate of seven percent. As an example, health services within the United Kingdom were targeted by WannaCry. A variety of organizations providing health services were impacted to the point where patient appointments were canceled or diverted to alternate medical facilities.

Ransomware became a weapon of choice within EMEA, as the gaming sector (gambling and associated entertainment) experienced 36 percent of ransomware attacks, followed by business and professional services at over 15 percent. The high detection rates in EMEA were no doubt bolstered by the fact that significant ransomware incidents like WannaCry and Petya originated in EMEA.

Interestingly, spyware and keyloggers led global malware at 26 percent while accounting for only three percent of malware within EMEA. This suggests campaigns in EMEA focused more on the quick wins of ransomware rather than establishing the long-term access which spyware and keyloggers might provide.

Ransomware activity was focused on several sectors, most notably the gaming sector, followed by business and professional services, health care, manufacturing and technology.

Retail drops out of top five attacked industries for EMEA

Retail moved out of the top five most attacked sectors in EMEA to sixth place with five percent of attacks (from 17 percent of attacks observed in last year's 2017 GTIR). The types of attacks being employed remain consistent, as web application attacks accounted for nearly 72 percent of all retail attacks. While the attack types may be easily identified, attack sources remain harder to isolate. For retail, like many industry sectors, the use of similar tools, tactics and techniques are blurring the lines between cybercriminals and nation-state actors, making attribution increasingly difficult.

China was the number one attack source against EMEA

Chinese sources led the number of attacks against targets in EMEA during 2017. In fact, EMEA was the only region in which U.S. attack sources fell behind Chinese sources. This is a change from 2016 data which revealed China as the ninth most prominent attack source, accounting for less than three percent of all attacks against EMEA. Attacks from Chinese sources have escalated to the point that China was a top five attack source in each of the top five most attacked industries in EMEA, and Chinese sources accounted for 67 percent of all attacks against manufacturing targets within EMEA. Attack techniques from China were diverse but included a variety of application-specific and web application attacks, with a heavy concentration on reconnaissance activities. A significant amount of this hostile activity was identified due to it being associated with a known bad source, meaning the activity originated from IP addresses within China previously identified as hostile.

Industry Highlights: Business and Professional Services Sector

Business and professional services describe work supporting a business, but not necessarily producing a tangible commodity as found with manufacturing. Professional service firms can be any business offering customized, knowledge-based services to clients of which some examples include outsourced information technology, lawyers, advertising professionals, architects, accountants, financial advisers, and consultants, among others. In our modern independent services economy, outsourcing of business and professional services is very common, and this practice extends the attack surface area available to attackers.

Historically, attackers have focused on business and professional services not only to steal information directly, but also to steal information about that organization's clients and partners, as this sector includes a large number of service providers or outsourcers.

Business and Professional Services rises to the most attacked sector in EMEA and third globally

Given the modern services economy, it was not surprising business and professional services was the most attacked sector within EMEA at 20 percent, in the Americas (9 percent) and globally (10 percent) where it ranked third. In all three cases, this

Web application attacks usually target internet-facing applications to gain access to underlying data and host systems used by the application. They often include attempts to make the application or backend system execute attacker generated commands to steal data or gain further access.

Distributed denial of service (DDoS): when a hacker uses multiple distributed systems in a coordinated attack against a specific target, flooding the target with traffic or otherwise consume available resources so the targeted system becomes unavailable.

sector was a new entry to the top five most attacked sectors. In EMEA, the leading attacks were against web applications at 42 percent. Within the Americas, activity from known bad sources accounted for 69 percent of activity against business and professional services, and 74 percent of that sourced from Chinese and United States internet address space. Globally for this sector, known bad sources also ranked first at 34 percent, with web application attacks second at 21 percent.

Web-application attacks often map to large data breaches

Web application attacks in the business and professional services sector are often associated with data breaches. Hackers may use web application attacks against a professional services vendor to gain unauthorized access to their clients' information, potentially including access credentials of their clients' online resources. The attacker perspective on this may be "Why attack a target directly when I can access it indirectly through business and professional services?" This method was seen publicly years ago, when a large retailer was breached indirectly after their heating and cooling services vendor was compromised and the attackers to took advantage of the connectivity between and data associated with the mutual systems. Our point here is that ecosystems of business partnerships and services extend attack surface areas and increase risk.

Visible attacks provide deception of underlying attack motives

The combination of known bad sources, web application attacks and denial of service attacks is not surprising when reviewing attacker methods and objectives. Researchers report distributed denial of service (DDoS) attacks have doubled from the previous year, and NTT Security analysis shows DDoS among the most common attacks targeting several industries. DDoS attacks are often used as a smokescreen to cover up an underlying attack. Behind the smokescreen of such an attack is often malware insertion, data exfiltration, network intrusion or financial theft.

Not only does the denial of service attack cripple a target's online business, but it also acts as a tool to generate misdirection for an underlying attack. There are also dark websites providing denial of service attacks as a service via botnets for rent which are inexpensive to invoke, yet expensive to defend against.

Regional Impact: Highlighting the General Data Protection Regulation (GDPR)

The time to comply with guidelines of the General Data Protection Regulation (GDPR)[1] is upon us. Effective May 25, 2018, the GDPR has global implications, affecting every organization or company which collects, retains, or processes data about residents or individuals present in the European Union (EU).

What is the GDPR?

In a nutshell, the GDPR is a set of data protection rules, requiring those who touch data relating to EU residents to protect the personal data and privacy of individuals within its borders, no matter where the actual processing takes place. These regulations are not optional, and strict fines – up to €20 million (approximately $23 million U.S.) or four percent of the offending firm's annual revenue – can be imposed for non-compliance.

The primary driving forces behind the GDPR are twofold: to provide people with more control over how their personal data is being used, and to give business a simpler, clearer legal environment in which to operate.

What types of data is protected by the GDPR?

The new rules also require this data to be maintained within the borders of the European Economic Area, unless specific pre-conditions are met. Individuals also have the right to know and access data stored about themselves, have it transferred to a third-party, or even have their data deleted. The new rules also require this data to be maintained in the individual's home country, should their data be collected and maintained.

[1] https://www.eugdpr.org/

What are the potential impacts?

Many global companies still are not fully aware of how they will be affected by GDPR, and may not fully understand the implications of the new regulations, several of which are highlighted below:

- Organizations and businesses must inform customers of their rights under the GDPR.
- Organizations and businesses may be required to appoint a Data Protection Officer (DPO), responsible for overseeing privacy within the organization.
- Organizations are required to prove they have adopted these data and privacy protection measures within their processing environment, and conduct specific risk assessments of higher risk activities.

The GDPR also affects third-party contracts, placing liability on organizations that own the data and organizations that process or manage the data. Third-party organizations or contracts with your organization which are not in compliance with the GDPR regulations means that your organization is not in compliance.

And, under the GDPR, organizations are obligated to report high-risk breaches, and every other organization in its chain must also comply.

While these regulations continue existing restrictions on what data is transferred internationally, GDPR principles may be a milestone in these efforts, as they align with – and build upon – other countries' and regions' efforts to date. Such efforts include the Australian Privacy Act of 1988 and Notifiable Data Breach Regulation of 2017, South Africa's 2013 Protection of Personal Information Act (PoPI), and Japan's Act on the Protection of Personal Information (APPI). While there are differences in methods, along with levels of legal development, there are signs of progress in meeting data protection principles worldwide.

Perhaps the greatest risk, though, is lack of compliance with the regulations. Until now, organizations could accept the risk and clean up any leaks resulting should a compromise occur. Beginning 25 May 2018, however, penalties could be severe. To make matters more complicated, lack of compliance with GDPR – and industry – regulations could put an organization's cyber-risk insurance at risk of being deemed invalid.

Despite the length of time these rules have been in the works, unfortunately, NTT Security's 2017 Risk:Value report shows that many companies are not ready for the GDPR. NTT Security interviewed 1,350 businesses across the globe to understand their approach to cybersecurity. Across the board, awareness was low. In the US, just a quarter of businesses understood the GDPR would affect them. Things were not much better in the Asia-Pacific region, where 26 percent of businesses in Australia were aware, 29 percent in Hong Kong, and just a third of respondents in Singapore.

There are several steps your organization can take to move forward in compliance efforts:

- Instill a sense of urgency – this must come from the upper security and management echelons down.
- Conduct a risk assessment. This should include where data is stored and processed, particularly regarding that of citizens of the European Union.
- From the results of this risk assessment, create a data protection plan and apply risk mitigation measures accordingly.
- Report GDPR progress.
- Test your organization's incident response plans, and continually assess plans and overall progress.

The bottom line is this: although these regulations appear to be constrictive and, well, regulatory, keep in mind that increased data privacy will ultimately boost consumer confidence. Strong data protection shows clients that the companies' they've entrusted their data to are concerned with their privacy and data handling. Better still, enhancements to become GDPR-compliant could very well assist in the efficiency of your organization's storage and data management efforts.

The above aside, the GDPR regulations are upon us. It's understood that organizations are at varying readiness stages of GDPR compliance – from identifying requirements to reviewing current controls. That said, wherever you are on your journey, security and DPO executives need to work together on assessing their GDPR readiness. And, whatever stage of compliance your organization is at, international businesses wishing to operate in the global digital market must consider the impact of GDPR to capture its commercial opportunities, as well as mitigate its risk.

So, what will change under GDPR?

What's New in GDPR at a Glance[2]:

Applies to data processors[+] not just data controllers[++]	Data processors can be held directly liable if the company is found responsible for a breach. This was limited to data controllers under the EU Directive.
Records of processing activities	Data controllers must maintain records of their processing activities.
Accountability	Organizations must demonstrate how they comply with GDPR and document what personal identifiable data they have and why.
Data protection impact assessments	These must be carried out to consider an individual's privacy when an organization is creating or updating a product or service that includes processing likely to result in a high risk to the rights and freedoms of data subjects.
Higher standards of consent	Consent by a data subject must be freely given and based on clear, easily available information about what they are agreeing to. It must be as easy to withdraw consent as it is to give it.
Enhanced rights for individuals (data subjects resident and /or citizens in the EU)	Individuals have the right to be informed, object to processing and be forgotten (through erasure) – as well as rights regarding access, rectification, restrictions on processing, data portability and automated decision making.
Data Protection Officer (DPO)	A DPO is not mandatory for all organizations but a senior individual must be made responsible for GDPR compliance.
Breach notification	Organizations have a duty to report a breach of personal data within 72 hours and failure to do so may result in a fine.
Level of fines	GDPR sees a significant increase in fines – up to 4% of global annual revenue.

\+ *Processor – 'means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller' (Article 4 EU GDPR 'Definitions')*
++ *Controller – 'means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data' (Article 4 EU GDPR 'Definitions')*

Recommendations based on trends in EMEA

1. **Focus on GDPR compliance and integrating GDPR requirements into operations.** Enhance GDPR compliance, but not to the exclusion of other security initiatives. It is tempting to "do GDPR" and limit other activities, but falling behind on patches or backups can have a seriously negative impact, and could actively undermine GDPR compliance.

2. **Protect against web application attacks.** Implement a Web Application Firewall (WAF) and other technology to help detect and prevent web application attacks. Establish and enhance secure development training initiatives, procedures, tools and validation to minimize vulnerabilities. Use penetration and application testing to identify system and application misconfigurations and other vulnerabilities.

3. **Implement a formal vendor management program.** If your organization makes use of outsourcers, suppliers and other vendors, it is inheriting risk from those connections. Attacks which use entry points from partner organizations which may have a trusted connection have become a common way of attacking a target. Implementation of a formal vendor management program would include ensuring vendors understand the security goals of your organization, and increase confidence that those organizations are taking security measures which not only protect themselves but protect other partner/vendor organizations. A vendor management program is a formal mechanism to ensure organizations clearly and concisely communicate legal, regulatory, security and business objectives, and helps define how vendors will fulfill those objectives.

[2] https://www.nttsecurity.com/docs/librariesprovider3/resources/global_thought_leadership_gdpr_uea_v4.pdf

Focus on Americas

Attacks against the Americas resulted in finance and technology jumping to the top of the most attacked sectors. The influence of technology companies surged in the Americas in 2017, demonstrated by a 25 percent increase in the U.S. stock market – with technology companies like Apple, Alphabet, Facebook, Amazon and Microsoft accounting for close to half of that increase. Technology companies are succeeding at driving the market and driving market value, and because of that, their value as targets has increased.

That is not to suggest that targets are always attacked for theft of funds. Along with targeting sources of direct income, attackers target proprietary information, trade secrets, personal financial information, and they target systems as well. NTT Security has observed not just the compromise of systems to launch additional attacks, but high levels of attacks focused on installing coin mining software in organizational environments, so that company resources can be used to support the goals of the attacker. All these attacks have direct, immediate impacts on the organizations, and their ability to establish and maintain secure operations.

Many organizations use standards or compliance-based frameworks to help drive their security programs. Such a program is driven by standards defined to meet either specific security goals (like the protection of personally identifiable information within the Payment Card Industry Data Security Standard – PCI-DSS) or program standards such as U.S. National Institute of Standards and Technology (NIST). NIST has announced updates to its Framework for Improving Critical Infrastructure Cybersecurity. The goal of the update was to simplify risk assessments for U.S. agencies using NIST security program standards. Later in this section we provide a brief overview of the changes that may affect your organization if it has adopted NIST security guidelines.

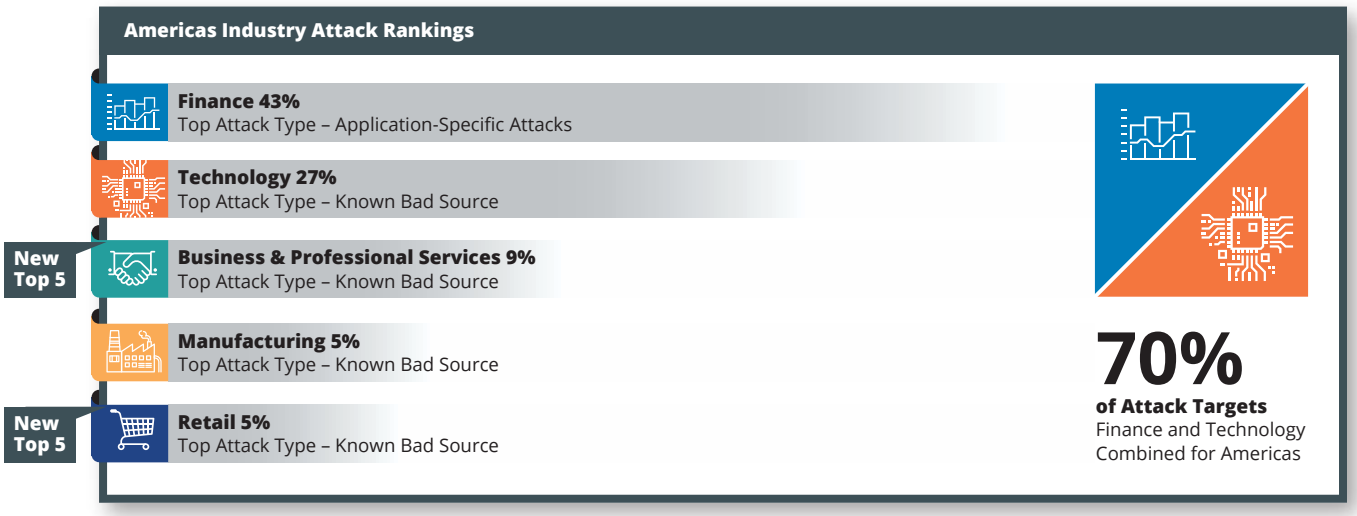
Americas Key Findings

Americas Top Malware

- Spyware/keyloggers accounted for 39 percent of malware targeting the Americas, significantly higher than 26 percent globally.
- Malware (35 percent) was the primary driver for engaging advanced incident response services.
- For retail, 71 percent of incident response engagements resulted from malware.
- Trojan/dropper malware ranked first at 57 percent for both technology and business and professional services sectors.
- Virus/worms lead the manufacturing sector with 49 percent of detected malware.

Americas Industry Sector Attacks

- Technology and finance sectors together account for 70 percent of all attack targets within the Americas.
- Finance sector observed an increase to 43 percent of attacks, up from 15 percent in the previous year.
- Technology sector increased to 27 percent of attacks which was up from 11 percent the previous year.
- Manufacturing dropped from the most attacked sector in 2016, with 23 percent of attacks, to five percent in 2017.
- Known bad sources accounted for 36 percent of hostile activity against targets in the Americas, yet did not exceed 18 percent in any other region.
- U.S. and Chinese sources accounted for 62 percent of the attacks against countries in the Americas.
- The Russian Federation only appeared in the top five attack sources against targets in the Americas, while ranking no higher than tenth in any other region.



Americas Industry by Attack Source Country and Attack Type

Finance 43%

United States	70%	Application-Specific Attacks	49%
		Known Bad Source	13%
		Web Application Attacks	10%
China	7%	Known Bad Source	45%
		Reconnaissance	16%
		Brute Forcing	15%
Sweden	2%	Network Manipuluation	80%
		Known Bad Source	9%
		Reconnaissance	4%
France	1%	Known Bad Source	53%
		Web Application Attacks	23%
		Reconnaissance	11%
China/ Hong Kong	1%	Reconnaissance	75%
		Service-Specific Attacks	13%
		Web Application Attacks	7%

The United States was the attack source country for 70 percent of attacks in the finance sector for the Americas, likely due to compromised resources controlled from outside of the United States.

Technology 27%

United States	29%	Known Bad Source	64%
		Web Application Attacks	20%
		Reconnaissance	10%
China	20%	Known Bad Source	78%
		Reconnaissance	19%
		Application-Specific Attacks	1%
France	5%	Known Bad Source	83%
		Reconnaissance	14%
		Web Application Attacks	2%
Russian Federation	4%	Known Bad Source	76%
		Reconnaissance	15%
		Web Application Attacks	4%
Netherlands	4%	Known Bad Source	84%
		Reconnaissance	14%
		Web Application Attacks	2%

The technology industry sector was highly targeted in the Americas. We discuss additional observations and guidance that may aid in defense against evolving threats in the Industry Highlights: Technology section of this report.

Business & Professional Services 9%

China	46%	Known Bad Source	95%
		Denial of Service Attacks	3%
		Reconnaissance	2%
United States	28%	Denial of Service Attacks	45%
		Known Bad Source	29%
		Application-Specific Attacks	13%
France	3%	Known Bad Source	95%
		Reconnaissance	3%
		Application-Specific Attacks	1%
Netherlands	2%	Known Bad Source	93%
		Reconnaissance	5%
		Web Application Attacks	1%
Russian Federation	2%	Known Bad Source	74%
		Denial of Service Attacks	16%
		Reconnaissance	6%

With 26 percent of ransomware attacks within the Americas, business and professional services was the industry most targeted by ransomware.

Manufacturing 5%

United States	32%	Known Bad Source	30%
		Web Application Attacks	27%
		Application-Specific Attacks	15%
China	21%	Reconnaissance	47%
		Known Bad Source	40%
		Application-Specific Attacks	8%
France	4%	Known Bad Source	39%
		Reconnaissance	39%
		Application-Specific Attacks	11%
Russian Federation	3%	Known Bad Source	50%
		Reconnaissance	38%
		Application-Specific Attacks	8%
United Kingdom	3%	Web Application Attacks	49%
		Application-Specific Attacks	16%
		Reconnaissance	16%

Manufacturing fell from the most attacked sector in the Americas in the 2017 GTIR with 23 percent of attacks.

Retail 5%

United States	24%	Known Bad Source	39%
		Web Application Attacks	31%
		Reconnaissance	22%
China	17%	Reconnaissance	69%
		Known Bad Source	31%
		Application-Specific Attacks	<1%
France	7%	Known Bad Source	60%
		Reconnaissance	38%
		Brute Forcing	2%
Netherlands	5%	Known Bad Source	70%
		Reconnaissance	28%
		Application-Specific Attacks	1%
Japan	4%	Known Bad Source	54%
		Denial of Service Attacks	32%
		Reconnaissance	5%

Within the retail sector, 71 percent of incident response engagements were in response to malware infections.

Americas Threat Highlights

Technology sector gained significant attention

Attacks against the technology sector jumped from under 11 percent in 2016 to 27 percent in 2017. This was enough to move technology from the eighth most attacked sector in 2016 to the second most attacked during 2017. Finance and technology accounted for 70 percent of all attacks within the Americas. While sources within the United States (29 percent) and China (20 percent) were more commonly focused on technology, Russian sources, at just under four percent, also made an appearance.

Like most sectors in the Americas, "known bad source" was the largest indicator of hostile activity against this sector, indicating attackers are reusing known hostile IP address ranges. Reconnaissance activity against technology organizations was also common, with Chinese, French and Russian sources following activity from the United States.

Finance becomes the number one target in the Americas

With 43 percent of attacks, finance became the most attacked sector in the Americas. This is up from the 2017 GTIR which showed finance as the third most attacked with 15 percent of all attacks. This indicates increased focus on finance as an attack target as much as it indicates reprioritization of other industries. Based on the types of attacks and targets observed by NTT Security during 2017, it appears attackers focused effort on industries which could result in short-term financial gain.

Attacks against financial targets in the Americas demonstrated the ability of attackers to establish internal compromise of targeted victims and to maintain those footholds, potentially even using compromised systems in additional attacks against other targets in the financial sector.

Spyware/keyloggers accounted for 39 percent of malware detected within the Americas. NTT Security observed several campaigns with increased occurrences of spyware and keyloggers targeting financial firms during 2017. These types of malware suggest attackers were working on short-term attacks, stealing credentials, targeting funds, and often sustaining long-term access to compromised environments.

The United States was the number one source of attacks across the globe, responsible for about 27 percent of attacks. Seventy percent of attacks against finance organizations in the Americas originated from the United States.

Americas experienced more Russian Federation activity

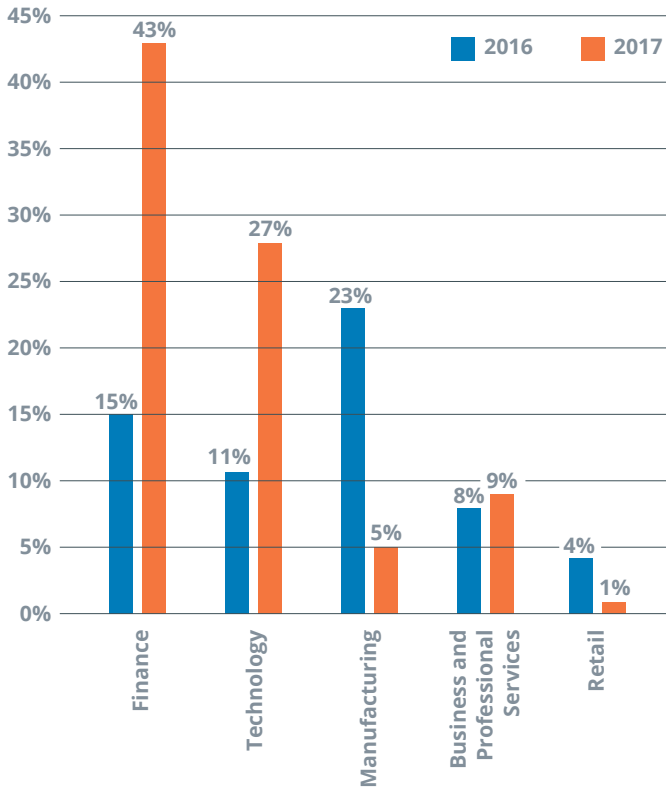
Within the Americas, Russian sources appeared in the top five attack sources in business and professional services, technology and manufacturing. In general, attacks from Russian sources did not dominate any specific region or industry around the globe, and Russia did not appear at the top of the attack source list in any region except for attacks targeting the Americas. With three percent of all attacks against targets within the Americas, Russia was the fourth most common attack source during 2017.

While in the scheme of cyberattacks, three percent does not sound like the high end of the scale, it is worth pointing out that Russia did not appear in the top 10 most active attack sources in any region other than the Americas.

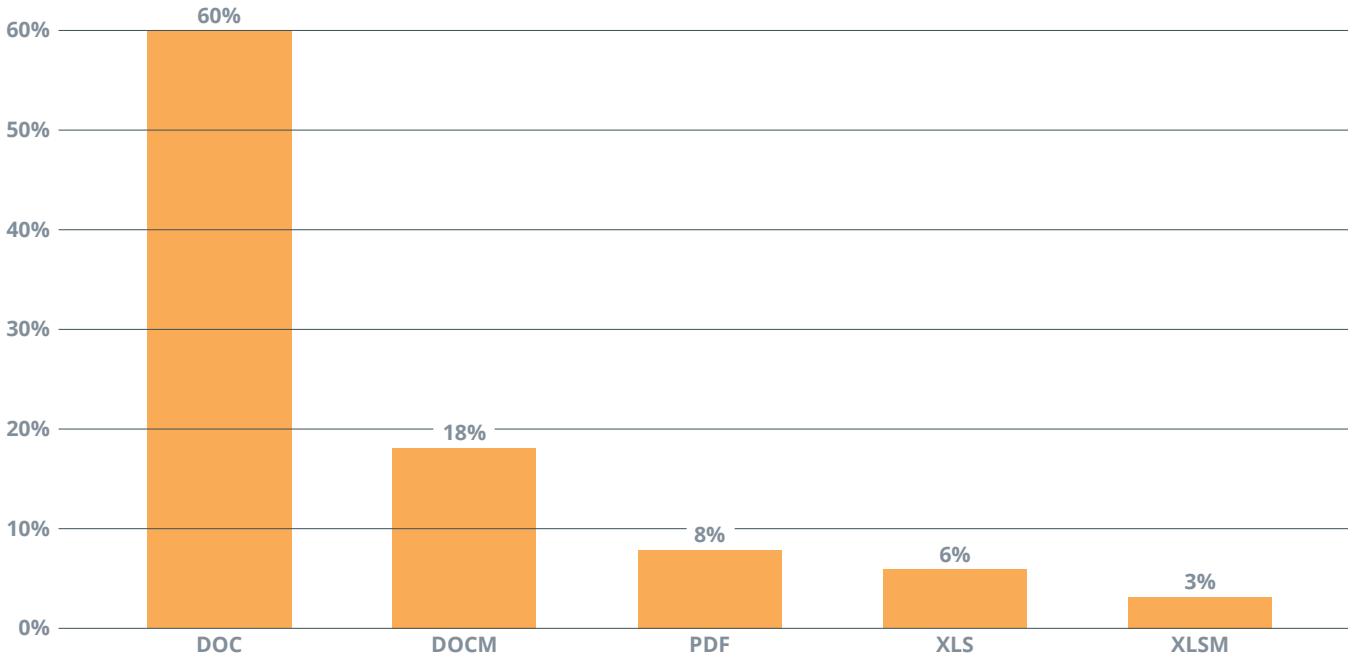
Social engineering and phishing continues to prove valuable to attackers

Attackers continued to exploit known vulnerabilities in conjunction with social engineering, convincing users to click on links in phishing emails as well as open malicious attachments. Malicious Microsoft Word documents accounted for 78 percent of phishing campaign attachments in the Americas, using scripts, macros and embedded objects. Finance felt the most impact

Changes in Targeted Sectors: Americas



Americas – Phishing Attachments



with 59 percent of phishing attacks, followed by the education sector at 28 percent.

The most popular malware associated with phishing campaigns in the Americas was Lokibot at 19 percent, followed by Trickbot and Locky.

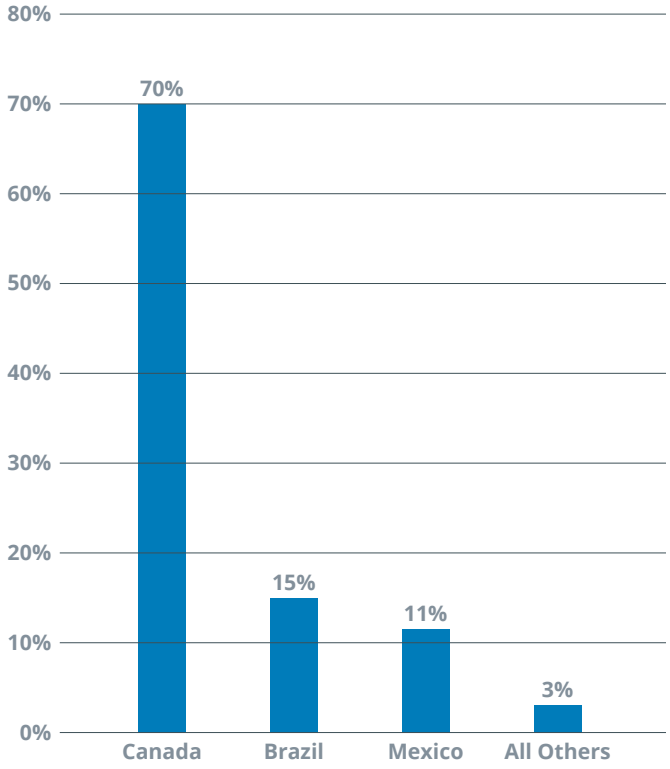
The United States was the biggest source of hostile activity from the Americas, but not the only source

Globally, the United States accounted for 27 percent of hostile activity. Twenty-eight percent of attacks from the Americas focused on application attacks, but like most regions, attacks from the Americas were varied.

The United States was not the only hostile source within the Americas. Canadian sources accounted for 70 percent of attacks from the Americas which were not attributed to the U.S. While only 18 percent of attacks from Canada were web application attacks, those attacks included an impressive variety of SQL injection techniques against a variety of technologies in a variety of sectors.

Brazilian sources continued a high level of malicious cyberactivity, with over 15 percent of attacks from sources in the Americas other than the United States. Over 94 percent of

Americas Attack Sources Other than U.S.



application-specific attacks from Brazil focused on remote code execution attacks. Much of this activity targeted vulnerabilities in ASUS and Netcore routers, along with TVT Digital and Linksys router exploitation.

As the fourth largest source of attacks within the Americas, attacks from Mexican sources emphasized reconnaissance activity and brute force attacks (91 percent SSH) more than other countries in the Americas.

It's usually not the newest vulnerability

While new vulnerabilities are identified every day, previously discovered vulnerabilities often are the root cause for system or network compromise. A prime example was a large U.S.-based credit rating company, whose breach exposed credit data for over 150 million U.S., U.K. and Canadian citizens. The attack took advantage of a vulnerability in the Apache Struts framework (CVE-2017-5638[3]) with an available but unapplied patch. A large-scale breach like this highlights how a relatively simple breakdown in the process can underscore the need for better patch management. Patching remains a top priority as a primary, baseline defensive measure, but is not implemented consistently enough that it will cease being an issue.

Industry Highlights: Technology Sector

The technology sector is composed of companies focused on computer hardware and software, semiconductors, communications equipment, office equipment, and information technology services and consulting. The sector includes technology design and manufacturing organizations, as well as their supply chains.

Technology expands into other sectors via the Internet of Things (IoT), operational technology (OT), autonomous vehicles, ride sharing, manufacturing, online travel and hospitality, and automated financial investing algorithms as a few examples. In all the amazement of technology advancements, security often remains an afterthought well past the prototype, design and testing phases.

Across all regions, technology ranked in the top five attacked sectors

In the Americas, technology was the second most attacked industry sector, with 27 percent of attacks. Beyond the Americas, technology was the only sector ranked among the top five most attacked industry sectors in all regions. The percentage of attacks targeting the technology sector has at least doubled in every region since the previous year. Reconnaissance, service-specific attacks and activity from known bad sources as lead hostile activities. Within APAC and Japan, technology ranked third for both regions at 16 and 17 percent respectively. The United States, Australia and China represented 54 percent of attack source countries globally while the United States ranked first or second within all regions as the attack source. Additionally, Australia was the leading attack source country for targets in Australia.

Consistent attack types target the technology sector in all five top source countries

Regional data for the technology sector shows specific attack characteristics, focusing on reconnaissance, unpatched vulnerabilities and activity from known bad sources.

Detection of the same hostile activities across multiple geographic regions suggests the targeting of technology organizations in a consistent manner.

Why is reconnaissance important in the Americas?

Like other regions, the Americas experienced significant amounts of reconnaissance activity. For cybersecurity, reconnaissance is typically a preliminary step toward exploiting a target system or environment, using port scanning and looking for vulnerabilities on open ports, fingerprinting applications, and in general, identifying potential weaknesses. This, in the physical world, can be similar to a burglar casing a potential victim before he actually commits the act of burglary. Attackers use reconnaissance activities to identify viable targets, and to identify potentially attackable systems within a specific target. Firewalls and intrusion prevention systems (IPS) are common defenses to protect ports and block common reconnaissance activities.

Automation is key for reconnaissance to quickly find possible targets. Reconnaissance activities may be hosted at a static IP address for an extended period of time and managed by an attacker. In some cases, scanning activities occur from systems which were previously compromised by the attacker and the malicious activity may appear to originate from a legitimate business or web presence. The IP source addresses of these hosts become "known bad sources" based on this hostile activity. Investing in IP-based reputation services, plus whitelisting known good sites and monitoring network activity for hostile addresses, can limit the effectiveness of reconnaissance from known bad sources.

Technology as a sector often accepts more risk

Technology organizations tend to build aggressive business plans, and may result in taking more business risks, such as being early adopters of new technology both in their processes and products. Technology companies frequently have open campuses and policies to stimulate creativity and encourage collaboration, which may make them more difficult to defend. These variables may contribute to a larger threat surface.

[3] https://nvd.nist.gov/vuln/detail/CVE-2017-5638

Targets in Americas – Known Bad Sources	Targets in EMEA – Reconnaissance Sources
Netherlands – 84%	China – 88%
France – 83%	Russian Federation – 87%
China – 78%	United States – 81%
Russian Federation – 76%	Sweden – 40%
United States – 64%	United Kingdom – 32%

Regional Impact: Highlighting the National Institute of Standards and Technology Framework

After extensive coordination with the public and private sectors, the National Institute of Standards and Technology (NIST) released Draft 2 of its Framework for Improving Critical Infrastructure Cybersecurity,[4] version 1.1 in December 2017.

Several key shifts and changes are highlighted in the newest version of the NIST cybersecurity framework.

The draft document covers several essential changes to existing guidelines, especially concerning organizations' self-assessment of cybersecurity risk. Version 1.1 introduces some new changes affecting authorization, authentication, identity proofing, and disclosure of vulnerabilities. NIST also released a proposed update to its Roadmap for Improving Critical Infrastructure Security which describes planned future activities and topics to focus on for upcoming versions of the framework.

As NIST explains, the newest framework is simply guidance for critical infrastructure organizations – to be voluntarily implemented. The framework is based on existing standards, guidelines, and best practices, to reduce cybersecurity risk. In addition, version 1.1 clarifies, refines, and builds upon version 1.0 of the framework, allowing for simpler employment of new guidance. In fact, NIST states, "This draft is intended to provide a flexible, voluntary, and effective tool to help organizations better manage their cybersecurity risks. Like the earlier proposed update, this draft is fully compatible with Version 1.0 and can be used as the basis for communication between organizations."

Making it even easier, the newest strategies are quite broad, providing baseline guidance, allowing organizations to tailor solutions applicable to their industry, budget, business functions, and operational infrastructure.

As a stand-alone reference, the framework offers a common and understandable lexicon for cybersecurity risk management. In its simplest form, that lexicon is: Identify, Protect, Detect, Respond, and Recover. This simple yet effective lexicon allows organizations which are not experts in cybersecurity to contribute to – and understand – the cybersecurity dialog.

One of the highlighted priorities of the new framework emphasizes the potential weak links in supply chains. In fact, NIST is hoping that version 1.1 will facilitate greater consideration of supply chain risk within a cybersecurity strategy.

Other significant changes and key updates to the framework are as follows:

1. Cybersecurity measurements: The new framework revises NIST's segment regarding implementing cybersecurity measurements. As mentioned above, the discussion is simplified, allowing for those not well-versed in cybersecurity to better understand the policies and implications, allowing for better tailoring of the guidelines to each individual organization.

2. Relevance to Internet of Things devices: NIST has updated the new framework to "reflect security implications of a broadening use of technology." Draft 2 of version 1.1 notes that each industry leverages a wide breadth of technologies, "including information technology (IT), industrial control

[4] https://www.nist.gov/sites/default/files/documents/2017/12/05/draft_roadmap-version-1-1.pdf

systems (ICS), cyber-physical systems (CPS), and connected devices more generally, including the Internet of Things (IoT)."

3. Coordinated vulnerability disclosures: The newest framework includes a subcategory considering both internal and external vulnerability disclosure programs, including references.

4. Authorization, authentication, and identity proofing: The newest framework also adds an authentication subsection, providing numerous references.

It is worth noting that this framework IS voluntary, however, best practices and cybersecurity standards have been observed to thwart those vulnerabilities which are most easily compromised by attackers. These guidelines, while broad, will allow you to tailor solutions for your infrastructure.

NIST anticipates finalizing the Cybersecurity Framework version 1.1 in the Spring of 2018.

Recommendations based on trends in the Americas

1. **Protect against compromises designed to persist.** Spyware/keyloggers, especially in the financial sector, were highly used during 2017. Design and implement a network architecture which isolates different functions and key information into protected subnetworks. Protect those internal networks with elevated controls such as internal firewalls.

2. **Protect against phishing attacks.** Implement spam and anti-phishing tools and capabilities. Consider restricting inbound attachments if that is within your risk tolerance. Enforce good endpoint security practices, and reinforce user training to reduce the probability that users will click through malicious emails.

3. **Filter or block sources.** Blacklists and other tools can help identify known bad sources and reduce your attack profile. Build whitelists of organizations and locations with which you do business. This will better enable you to clearly identify hostile sources. Monitor for sources of activity, benign and hostile, to more readily react if observed actions become more malevolent.

Focus on Asia-Pacific (APAC)

For data analysis of the APAC region, note that Japan was analyzed independently and is not included in the APAC regional results of the report. This is due to our special focus on the upcoming 2020 Olympic Games to be hosted in Japan and resulted in separate data analysis focusing on threats affecting the country.

Activities related to breach notification laws are new this year in Australia and Singapore, increasing visibility and transparency. However, many countries in the region are not required to follow or do not enforce them.

The Australian Privacy Amendment (Notifiable Data Breaches) Act 2017 was passed in February 2017, and went into effect 22 February 2018. The act targets notifiable data breaches and requires affected organizations to notify regulators and affected individuals if the organization has reason to believe a privacy breach has taken place. Like other more recent privacy acts, the Notifiable Data Breach act includes significant penalties, up to AUD1.8 million, for failure to comply.

Like any region, breaches were all too common in APAC. WannaCry, NotPetya and BadRabbit are sophisticated examples of ransomware and destructive malware with widespread damage. Malware authors are likely to utilize the same password harvesting and propagation techniques used in NotPetya to create their own malware.

The APAC region tends to have strong representation in the manufacturing sector, with China as the leading global manufacturing country, and South Korea ranked fifth globally. Even with these leading manufacturing countries, the manufacturing sector did not make the top five most targeted sectors this year in APAC after ranking second in last year's report at 32 percent. In comparison, APAC was the only region in which manufacturing was not in the top four targets.

In 2016, NTT Security detected that 60 percent of traffic related to the Mirai Internet of Things (IoT) botnet showed source IP addresses in Asia. Operational technology (OT) and IoT attacks continued in 2017 both originating from and focused on resources within APAC. NTT Security includes an overview of OT/IoT later in this section.

Focus on Asia-Pacific (APAC)

APAC Key Findings

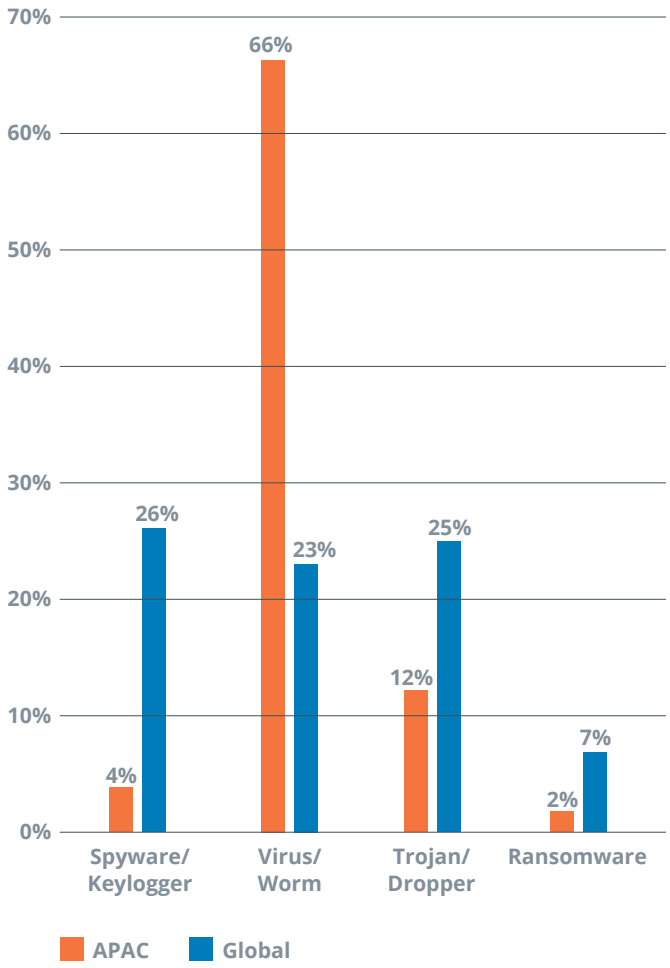
APAC Top Malware

- Virus/worms accounted for 66 percent of malware in APAC compared to 23 percent of global malware.
- Spyware/keyloggers were low at four percent for APAC compared to 26 percent globally.
- While ransomware measured at only two percent for APAC, globally it showed at seven percent.

APAC Industry Sector Attacks

- A 46 percent decrease in attack volume resulted in the finance sector dropping to 26 percent of attacks within APAC, from 46 percent of attacks in the previous year.
- Australia was the attack source country for 66 percent of the attacks against the finance sector, likely due to compromised resources.
- Manufacturing decreased from 32 percent of attacks the previous year to seven percent, falling out of the top five attacked industries in APAC.
- Education doubled to 18 percent of attacks.
- The top attack type within the APAC region for all industry sectors was brute forcing at 26 percent.

Malware Comparison: APAC vs Global



APAC Industry Attack Rankings

Finance 26%
Top Attack Type – Service-Specific Attacks

Education 18%
Top Attack Type – Brute Forcing

New Top 5 — **Technology 16%**
Top Attack Type – Service-Specific Attacks

New Top 5 — **Retail 15%**
Top Attack Type – Brute Forcing

New Top 5 — **Government 13%**
Top Attack Type – Network Manipulation

Manufacturing dropped to 7% from a previous year of 32%
Top Attack Type – Network Manipulation

Focus on Asia-Pacific (APAC)

2018

NTT Security

APAC Industry by Attack Source Country and Attack Type

Finance 26%

Australia	66%	Service-Specific Attacks	56%
		Web Application Attacks	15%
		Application-Specific Attacks	12%
United States	23%	Brute Forcing	53%
		Service-Specific Attacks	31%
		Web Application Attacks	7%
China	3%	Reconnaissance	43%
		Application-Specific Attacks	26%
		Known Bad Source	18%
Netherlands	1%	Service-Specific Attacks	39%
		Network Manipulation	37%
		Reconnaissance	8%
Russian Federation	1%	Reconnaissance	33%
		Application-Specific Attacks	31%
		Web Application Attacks	23%

Service-specific attacks were 46 percent of hostile activity for the finance sector. 89 percent of these attacks were sourced from Australia and the United States.

As we have identified, the finance sector was highly targeted in APAC. This report includes additional observations and provides guidance that may aid in defending against evolving threats.

Education 18%

China	18%	Service-Specific Attacks	63%
		Application-Specific Attacks	20%
		Brute Forcing	16%
France	16%	Brute Forcing	81%
		Denial of Service Attacks	16%
		Web Application Attacks	2%
Romania	15%	Brute Forcing	98%
		Web Application Attacks	2%
		Application-Specific Attacks	<1%
United States	12%	Brute Forcing	63%
		Denial of Service Attacks	11%
		Application-Specific Attacks	10%
Germany	8%	Brute Forcing	98%
		Web Application Attacks	<2%
		Denial of Service Attacks	<1%

Brute force attacks represented 64 percent of attacks against the education sector within APAC.

Technology 16%

Australia	35%	Service-Specific Attacks	43%
		Web Application Attacks	30%
		Network Manipulation	12%
United States	22%	Service Specific Attacks	39%
		Evasion Attempts	34%
		Reconnaissance	7%
China	8%	Application-Specific Attacks	53%
		Evasion Attempts	36%
		Reconnaissance	10%
India	7%	Evasion Attempts	100%
Netherlands	5%	Service-Specific Attacks	41%
		Network Manipulation	40%
		Evasion Attempts	18%

The sector most targeted by ransomware in APAC was technology, which experienced 29 percent of all ransomware in APAC.

Retail 15%

United States	47%	Brute Forcing	99%
		Application-Specific Attacks	<.5%
		Service Specific Attacks	<.5%
Australia	46%	Brute Forcing	60%
		Application-Specific Attacks	26%
		Service Specific Attacks	12%
Netherlands	3%	Brute Forcing	99%
		Web Application Attacks	1%
		Application-Specific Attacks	<.05%
China	2%	Brute Forcing	94%
		Application-Specific Attacks	5%
		Known Bad Source	1%
Czech Republic	1%	Brute Forcing	100%

Brute force attacks represented 80 percent of hostile activity within the retail sector. The United States and Australia combined to represent 93 percent of the attack source countries, likely due to compromised resources.

Government 13%

Australia	84%	Network Manipulation	26%
		Application-Specific Attacks	16%
		Denial of Service Attacks	15%
United States	5%	Web Application Attacks	39%
		OS Specific Exploits	25%
		Denial of Service Attacks	13%
Belgium	3%	Denial of Service Attacks	48%
		Service-Specific Attacks	26%
		Network Manipulation	26%
France	2%	Denial of Service Attacks	48%
		Service-Specific Attacks	25%
		Network Manipulation	25%
Netherlands	1%	Denial of Service Attacks	85%
		Service-Specific Attacks	8%
		Network Manipulation	6%

In APAC, 84 percent of attacks against government targets originated from IP addresses in Australia. While attack sources tend to be located within the same region as the victim, the next six sources were all outside of APAC.

APAC Threat Highlights

Attacks on finance nearly doubled globally and stayed at the top in APAC

Finance ranked as the most attacked sector within APAC with 26 percent of attacks. This is even more interesting when you consider that NTT Security observed a 46 percent decrease in attack volume targeting these same organizations. Finance was also the most attacked sector in the Americas with 43 percent, and globally with 26 percent. Over two-thirds of attacks on the finance sector came from the United States and Australia, likely from compromised sources.

The leading type of attack in the region for the finance sector was application-specific attacks.

Attacks are dispersed across multiple industry sectors for APAC

APAC attacks by industry sector were evenly dispersed compared to the previous year. Finance and education remained in the top three, but sectors targeted within APAC were much more distributed. For instance, in attacks against targets in the Americas, the top two sectors accounted for 70 percent of all attacks – in APAC, the top five industries combined to include 88 percent of all attacks. This suggests attackers spread out attacks more evenly across a focused set of industries within APAC (finance, education, technology, retail and government) – and potentially indicates a trend of more targeted attacks against those sectors in the APAC region.

Attacks against education (three percent in 2016 and 18 percent in 2017) and technology (five percent in 2016 and 16 percent in 2017) jumped dramatically. Though most regions saw a decrease in attacks against government targets, APAC actually increased from six to 13 percent.

Malware and brute force attacks dominate

In APAC, viruses and worms spiked with 66 percent of malware, nearly triple their 23 percent share of global malware. While ransomware rose in every region, it stayed at two percent of malware for APAC targets. Brute force attacks accounted for 26 percent of all attacks in the region, but were ranked the twelfth most common attack type in both the Americas and EMEA.

Brute force attacks spiked to 64 percent for the retail and education sectors in APAC, and was the leading attack type at 26 percent in the region. A brute force attack usually uses automated software to perform many consecutive guesses to identify usernames and passwords. Simple passwords can be broken in seconds or minutes depending on password complexity.

Regional sources dominate attacks

IP addresses in Australia, the United States and China were responsible for 53 percent of attacks targeting APAC resources. Sixty-six percent of attacks against the finance sector, the most targeted sector in APAC, were from Australia. Australia or China were the top two attack sources for all the top five targeted industry sectors and were the most common attack sources in every industry except retail (where the U.S. was first, Australia was second and China was fourth). This continues previously observed trends where attack sources tend to be located in the same region as the target, but this trend is more pronounced in APAC than some other regions.

Industry Highlights: Finance Sector

While the finance sector leads the world in earnings and equity market capitalization, it is very fragmented. This sector is made up of a broad range of businesses including accounting, banks and credit unions, credit card companies, consumer finance, insurance, investment funds, individual fund managers, stock brokerages, venture capital firms, and some government-sponsored enterprises. Finance also frequently intersects with other industries regarding attacks, such as point-of-sale (POS) attacks within the retail sector.

Brick and mortar infrastructure continues its digital transformation within the finance sector, where some financial companies now consider themselves software houses. The future of digital transformation in financial services includes increased customer connectivity through multiple channels, increased use of algorithms for automated trading, use of cloud computing and data storage, potential outsourcing to third parties including across borders, and the potential use of virtual and digital currencies. While the recent past has seen financial market growth with low volatility, history – with added insight into cyber risks – reminds us of what to expect.

Finance sector is the most highly attacked, despite a decrease in attack volume in APAC

Specific to APAC, finance remained the leading attack sector even after decreasing to 26 percent from 46 percent the previous year. The finance sector in APAC actually experienced a 46 percent decrease in attack volume from the previous year.

Australia was the leading attack source country in APAC, accounting for 66 percent of attacks on the finance sector, while the leading attack type was service-specific attacks. Attacks from the United States were the second most common. Combined, sources in Australia and the United States accounted for nearly 89 percent of attacks against finance in APAC. Outside of APAC, the finance sector was the most attacked sector globally, as well as in the Americas, and the second most attacked sector in EMEA.

This continues trends from previous years. In 2016, for example, the finance sector was the second most attacked sector globally, only a fraction of a percent from the number one spot.

How does reconnaissance factor into attacks on the finance sector?

Financial companies have moved services to mobile applications to keep up with the demands of customers and in an attempt to differentiate themselves from competition. Online and mobile banking are now commonplace. Changes in customer requirements, changes in regulatory requirements, and changes in technology create an environment where financial companies must evolve their available applications in a dynamic and robust manner. In this fast-moving environment, attackers have the potential to uncover greater numbers of vulnerabilities within those greater numbers of applications and releases. Automated scanning for exploitable vulnerabilities makes sense for attackers. In such environments, automated scanning for exploitable vulnerabilities increases the potential for attackers to uncover and exploit those vulnerabilities in a timely manner.

Regional Impact: Highlights of Internet of Things and Operational Technology

The Shifting Landscape

Connected devices are rapidly transforming the internet landscape as we know it. Devices such as Wi-Fi connected light bulbs, connected cars, apps which allow you to set your home heating system remotely, or even a chip monitoring a medical condition in a person's body are all part of the Internet of Things (IoT) ecosystem[5].

As with most technology innovations, the IoT creates tremendous opportunity. But with this opportunity comes new risk. The data, devices and systems users count on for new and innovative services are being compromised in ways which are increasingly difficult to detect or defend against.

The NTT Security 2017 Risk:Value report included results of a survey of about 1,350 companies, and unsurprisingly, nearly 60 percent of respondents said they see IoT as a potential security threat to their organization, but the IoT is only part of the equation.

Automation and control systems such as Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS) are also on the spectrum of connected devices, with devices in these environments referred to as Operational Technology (OT[6]). These systems (and the devices running on them) are often used to control critical infrastructures such as power, pipelines, water distribution, sewage systems and production control.

The Challenge

What was traditionally the information technology (IT) ecosystem is now a confluence of PCs, mobile devices, consumer-friendly IoT devices and OT systems and devices. What this convergence means is that the risks which have existed in the IT space for years now directly impact IoT and OT systems as well, creating exploit opportunities for would-be attackers.

Ecosystem	Priority	Cybercriminal Motivation
IT	Confidentiality Integrity Availability	Monetization
OT	Availability Integrity Confidentiality	Disruption
IoT	Availability Confidentiality Integrity	Control, Monetization

The security challenge with this convergence is unmistakable, with the three ecosystems (IT, OT, IoT) all having different – arguably, competing – priorities.

Each aspect of this converged system is plagued by its own threat landscape, as threat actors continually adapt their tactics, techniques and procedures (TTPs) to increase their exploitation capabilities.

Security practitioners have been working for decades to defend against threat actors targeting IT infrastructure, and this wealth of experience has led to the implementation of risk management strategies, patch management policies and incident response plans.

Compounding the challenge for security professionals is that the proliferation of IoT devices shows no signs of slowing, with the number of IoT devices in homes and commercial environments alike increasing by the day.

Out of the three (IT, OT, IoT), IoT is historically the most insecure, with IoT devices battling with vulnerabilities such as unsecured web interfaces, insufficient authentication/authorization, unsecured network services, lack of transport encryption and many more. OT though cannot be ignored, as there have been multiple reported successful attacks targeting critical infrastructure around the globe.

[5] https://www.nttsecurity.com/docs/librariesprovider3/resources/gbl_thought_leadership_iot_uea_v2.pdf
[6] https://www.nttsecurity.com/docs/librariesprovider3/resources/gbl_thought_leadership_operational_technology_uea_v1.pdf

Four Pillars of OT Security

1. Detecting
Detecting anomalies, threats or incidents and knowing how quickly you can respond.

2. Securing
Controlling and securing the data flow between defined networks.

3. Managing
Protecting the growing array of network endpoints, beyond PCs and mobile devices to include OT.

4. Protecting
Controlling and managing user access to systems, and how systems can access one another.

Over the past two decades, threat actors have successfully attacked organizations in multiple industries, to include power, steel, water, nuclear and oil – and this is only the disclosed attacks. There have likely been countless others which organizations did not disclose or discover.

What can be done about it?

While there is no single solution to addressing these security challenges, there are steps which can be taken in addressing the new challenges the IoT and OT present to an organization's risk profile.

Internet of Things (IoT)

Beyond the obvious items such as password management, multifactor authentication, permissions via access control lists, enabling port security on network switches, etc., there are additional steps organizations can (and should) take to secure the IoT devices in their environment.

1. Map out all interconnectivities, identifying attack paths in the system to identify appropriate protections.

2. Re-examine existing firewalls, and configure those firewalls to eliminate any vulnerabilities.

3. Use the firewall's DMZ as applicable.

Whatever approach an organization takes to IoT deployment, a robust, secure wireless network is an essential component, as is wireless connectivity management, controllers to manage traffic and a secure system to integrate wireless and wired networks.

Operational Technology (OT)

The first step in controlling risk is to understand your exposure across all areas of the business and prioritize those deemed critical. OT security can be broken down into four basic pillars to establish your level of capability in key areas.

The IoT and OT are transforming[7] not only the internet landscape, but also the threat landscape as we know it – and this transformation is happening with each new device connected to the internet.

Organizations must safeguard their networks and now more than ever, must ensure their network environment employs a defense-in-depth strategy to reduce risk across the entire converged ecosystem.

Recommendations based on trends in APAC

1. **Maintain an active patch management program.**
   Update operating systems, applications, tools and other resources with patches and updates as they become available. Beside monitoring and applying patches, an effective patch management program includes asset inventory management, including the identification of critical systems which are prioritized for patches and updates. The EternalBlue exploit became public 31 days after the MS-17-010 patch, was exploited 59 days later in WannaCry, and 105 days later in NotPetya. Unfortunately, all these attacks had some success, yet all of them were against vulnerabilities which had patches available.

[7] https://www.nttsecurity.com/docs/librariesprovider3/default-document-library/gbl_trends_predictions_uea_v1.pdf

2. **Maintain an active vulnerability management program.** Scan systems for open vulnerabilities. Scanning can identify vulnerabilities in a controlled manner. Once a scan identifies vulnerabilities, patches can be applied on a priority basis. The process helps to actively close vulnerabilities in a proactive manner, before attackers have an opportunity to exploit them.

3. **Secure your profile and access methods.** Each website has specific purposes and its profile should be customized and secure. For access, implement multi-factor authentication (MFA) when possible. In some cases, risk-based authentication is reducing the impact of MFA. High levels of brute force attacks can potentially provide a signal to verify your organization is using strong passwords.

EternalBlue is an exploit developed by the U.S. National Security Agency (NSA) which took advantage of a vulnerability in Microsoft's implementation of the Server Message Block protocol. Microsoft released a patch for the underlying vulnerability in March 2017. EternalBlue was stolen from the NSA by the Shadow Brokers and released to the public in April, and in May (two months after a patch was available), WannaCry used EternalBlue to spread within organizations.

Focus on Japan

The Olympic games is a significant event in the worldview and draws thousands of competitors, millions of attendees, and billions of viewers. An event of this magnitude attracts both positive and negative attention. The Olympic games are targets of activists and cybercriminals, just like any large event, but on a larger scale. This was evident as recently as the 2018 Winter Olympics in Pyeongchang which had its opening ceremonies disrupted by a cyberattack.

With this elevated level of visibility, NTT Security included analysis of attack activity specifically for Japan, as well as for the APAC region. In many cases, the attacks and activity which affected APAC in general also affected Japan in the same way. Several countries continue to have a significant impact on cybersecurity within APAC and in Japan. China, Australia and Japan are all key contributors in the Japan region. Oddly enough, despite discussions about North Korean cyberattacks, North Korean IP addresses ranked as the 130th most active attack source against Japanese targets. This suggests that North Korea is taking additional actions to hide the source of their attacks so that attacks from the Democratic People's Republic of Korea (DPRK) will appear as originating from other sources.

2017 saw Japan taking a more proactive defense position in its efforts to become a major cyber power. This is highlighted with initiatives taken while hosting the 2016 G7 Summit, and with steps taken to validate confidence in cybersecurity ahead of the 2020 Olympic games.

Activity in Japan made manufacturing the most attacked industry sector in the region for the second year in a row. Japan has been a top manufacturing country for many years, consistently ranking in the top five manufacturers in the world. Japan businesses are well-known for market-leading automation and innovation. Such market leadership helps increase the value of targeting manufacturing companies in Japan.

Japan Key Findings

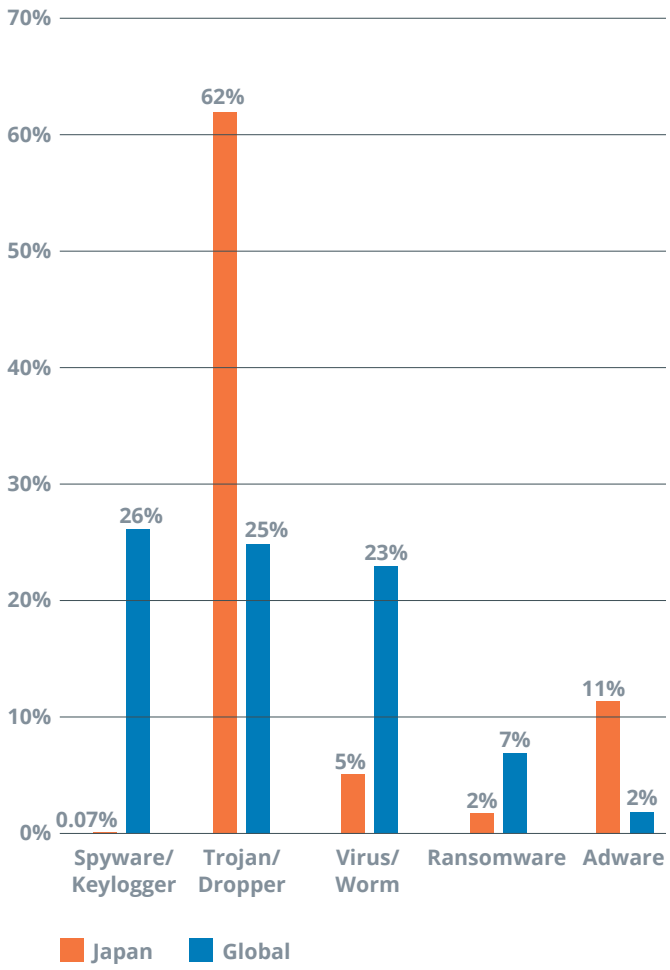
Japan Top Malware

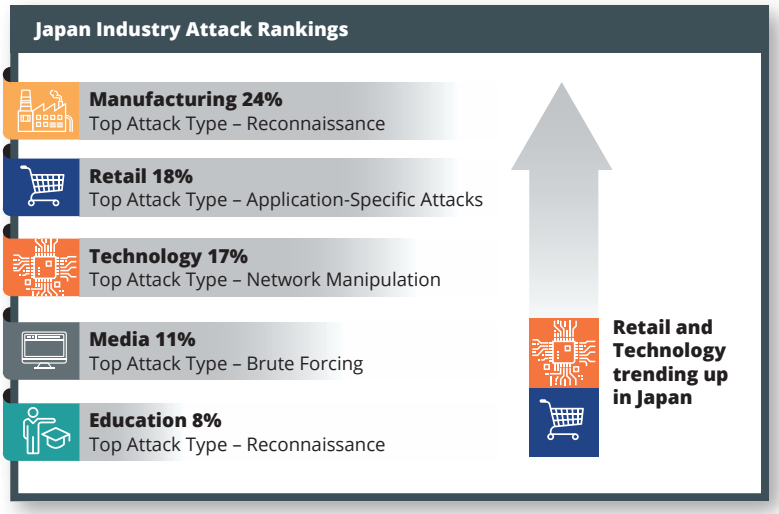
- Trojans/droppers accounted for 62 percent of malware in Japan compared to 25 percent globally, more than double the global percentage and five times the percentage for the APAC region.
- Adware ranked third at 11 percent of malware.
- Spyware/keyloggers for Japan were low at under one percent, compared to 26 percent globally.
- Ransomware accounted for about two percent of malware in Japan (a number similar to that of APAC) and seven percent globally.

Japan Industry Sector Attacks

- Manufacturing was the most attacked industry sector in Japan with 24 percent of global attacks.
- In manufacturing, reconnaissance was the most prolific activity at 47 percent.
- Retail was the second most targeted at 18 percent, with application-specific attacks accounting for 58 percent of attacks.
- Both the retail sector at 18 percent and the technology sector at 17 percent are trending up in Japan since 2016.
- Media made the top five attacked industries in Japan at 11 percent. Brute force attacks accounted for 41 percent of this activity.
- Education at eight percent rounds out the top five most attacked sectors for Japan. The only other top five ranking for this sector was in APAC, where attacks on education came in at 18 percent.
- 26 percent of attacks were from Japanese sources, 21 percent from the United States and 11 percent from China.

Malware Comparison: Japan vs Global





Focus on Japan

2018

NTT Security

Japan Industry by Attack Source Country and Attack Type

Manufacturing 24%

Japan	55%	Reconnaissance	79%
		Denial of Service Attacks	6%
		Brute Forcing	6%
United States	10%	Brute Forcing	55%
		Known Bad Source	22%
		Web Application Attacks	11%
China	5%	Known Bad Source	75%
		Brute Forcing	15%
		Application-Specific Attacks	6%
France	5%	Brute Forcing	92%
		Known Bad Source	6%
		Application-Specific Attacks	1%
Thailand	4%	Reconnaissance	95%
		Known Bad Source	3%
		Brute Forcing	1%

Top activities against the manufacturing industry in Japan were reconnaissance at 47 percent and brute force attacks at 22 percent. A total of 55 percent of these attacks were from Japanese sources.

The manufacturing sector was highly targeted in Japan. This report includes additional observations and provides guidance that may aid in defense against evolving threats.

Retail 18%

Japan	45%	Application-Specific Attacks	83%
		Web Application Attacks	4%
		DoS/DDoS	3%
United States	21%	Reconnaissance	45%
		Application-Specific Attacks	40%
		Web Application Attacks	10%
China	7%	Web Application Attacks	74%
		Application-Specific Attacks	15%
		Brute Forcing	6%
Netherlands	5%	Network Manipulation	79%
		Application-Specific Attacks	12%
		Reconnaissance	7%
Canada	3%	Application-Specific Attacks	85%
		Web Application Attacks	14%
		Reconnaissance	1%

Application-specific attacks were responsible for 58 percent of hostile activity for the retail sector in Japan.

Technology 17%

Japan	34%	Network Manipulation	64%
		Reconnaissance	19%
		Brute Forcing	12%
United States	19%	Service-Specific Attacks	75%
		Reconnaissance	12%
		Application-Specific Attacks	6%
United Kingdom	10%	Denial of Service Attacks	91%
		Reconnaissance	4%
		Web Application Attacks	3%
China	7%	Reconnaissance	26%
		Application-Specific Attacks	23%
		Denial of Service Attacks	21%
Seychelles	6%	Service Specific Attacks	98%
		Network Manipulation	<1%
		Reconnaissance	<1%

The most common attacks targeting technology in Japan included network manipulation at 24 percent, service-specific attacks at 22 percent and denial of service attacks at 19 percent.

Media 11%

Japan	57%	Brute Forcing	41%
		Web Application Attacks	29%
		Application-Specific Attacks	18%
United States	18%	Denial of Service Attacks	52%
		Brute Forcing	28%
		Application-Specific Attacks	10%
China	7%	Brute Forcing	52%
		Web Application Attacks	24%
		Application-Specific Attacks	18%
Chile	3%	Application-Specific Attacks	60%
		Brute Forcing	40%
Germany	2%	Brute Forcing	58%
		Reconnaissance	27%
		Denial of Service Attacks	6%

Japan and the United States represented 75 percent of all attacks against the media sector, while brute force attacks accounted for 41 percent of all attacks against Japanese media.

Education 8%

Japan	37%	Reconnaissance	89%
		Application-Specific Attacks	9%
		Web Application Attacks	1%
Iran	19%	Web Application Attacks	96%
		Application-Specific Attacks	2%
		Network Manipulation	2%
China	13%	Brute Forcing	69%
		Denial of Service Attacks	15%
		Application-Specific Attacks	13%
United States	6%	Application-Specific Attacks	43%
		Web Application Attacks	19%
		Brute Forcing	11%
Russian Federation	5%	Application-Specific Attacks	65%
		Denial of Service Attacks	17%
		Network Manipulation	12%

For all attacks against education in Japan, reconnaissance was the leading observed hostile activity at 34 percent, followed by web application attacks at 23 percent.

Japan Threat Highlights

Manufacturing sector leads attacks while media experiences brute force attacks

In Japan, manufacturing was the most attacked sector at 24 percent, followed by retail at 18 percent and technology at 17 percent. Interestingly, media organizations (e.g., cable television providers, production studios, social media companies) in Japan were the fourth most attacked, suffering 11 percent of attacks. 41 percent of the attacks targeting Japanese media organizations were related to brute force attacks.

Japan was the top attack source country for all top five sectors, indicating attackers used local resources to launch attacks.

Droppers in Japan spike to more than five times the rate for APAC

The significant trend for malware in Japan was that Trojans and droppers accounted for 62 percent of all detected malware, more than five times the amount for the APAC region and more than double the global rate. Droppers are technically not malware, but help to download malware and then often delete themselves. Adware ranked third for malware in Japan at 11 percent whereas globally it was only two percent. Other forms of malware, such as spyware, keyloggers and ransomware were significant globally, but were not regularly detected within Japan.

Japanese financial and government institutions become popular targets

Japan saw a wide array of attack types throughout 2017 with financial institutions, cryptocurrency exchanges and government offices being popular targets. These industries accounted for significant hostile traffic for short durations during focused campaigns, but such attacks were not lengthy enough to push them into the "most attacked" sectors. Multiple financial institutions in Japan, including some foreign exchange firms, suffered DDoS attacks throughout the year.

Apache Struts vulnerabilities S2-045 and S2-046 proved problematic for Japanese organizations, including one attack against a government agency which resulted in the leak of nearly 677,000 credit card numbers and over 614,000 email addresses. NTT Security Japan first began seeing attacks against clients as early as 7 March 2017, with the number of attacks spiking on 8 March and continuing at varying levels throughout the year.

Brute force attacks were the number one attack type

Attacks against Japanese targets differed from the types of attacks observed in most other regions. At 19 percent, brute force attacks were the number one type of attack against targets within Japan. In other regions, brute force attacks never ranked higher than ninth, and with the exception of a couple sectors in APAC, did not account for more than one percent of total attacks. Brute force attacks were significant for both manufacturing and media, at 22 percent and 41 percent respectively. For comparison in the manufacturing sector, no other region showed more than two percent brute force attacks.

Brute force attacks attempt to perform remote logins, suggesting attackers are trying to take advantage of weak password practices. Given that the second most common attack type against Japanese targets was application-specific attacks (17 percent), it appears likely that hostile actors targeted available systems and public-facing applications, attempting to gain access through those applications.

Japan was also targeted by the second highest rate of denial of service (DoS/DDoS) attacks of any region. In most sectors, these attacks did not outnumber other attack types, but they were consistent enough that the aggregate impact was measurable across multiple industries. There were also spikes in DoS/DDoS attacks against technology, media and education.

Why are application-specific attacks important in Japan?

Application-specific attacks were detected against almost every sector in every region, but Japan experienced higher volumes of application-specific attacks against the industry sectors which were most targeted in Japan. Beyond popular web application attacks using SQL injection and cross-site scripting are application-specific attacks targeting vulnerabilities and weaknesses within applications, including broken authentication and session management, security misconfigurations, exposed secrets and credentials, insecure direct object references, lack of encryption for data at rest and in transit, escalation of privilege (sometimes to administrator levels), and Trojanized or unpatched third-party

Per the NTT Security Risk:Value Report, only 56 percent of global respondents noted that C-level discussions about attack prevention were occurring on a regular basis. Additionally, only 56 percent responded their organization had a formal information security policy in place.

components. Applications are also subject to web redirects, forwarding from trusted sites, and cross-site request forgeries executing undesired actions in authenticated sessions.

Industry Highlights: Manufacturing Sector

Manufacturing organizations are generally categorized as organizations which build things. Manufacturing includes the process of transforming raw materials into finished or component parts using machines, tools and labor. This include organizations such as producers of food, chemicals, textiles, equipment and machines. The truth is that manufacturing organizations are much more than "builders" as they rely heavily on design, inventory management and distribution/ transportation systems to succeed.

As manufacturers experience the benefits of automation and the emergence of interconnected and intelligent production systems, companies of all sizes are realigning their operational models to take advantage of these disruptive technologies. More than 50 percent of manufacturers have adopted Industry 4.0 and Smart Manufacturing, the latest phase in the evolution of manufacturing technology, which began with mechanization and has moved through mass production, computing and automation, and is now focused on developing cyber physical systems (CPS).

The concept behind CPS is based on a "digital twin" of the physical machine which is operating in a cloud platform to simulate its health conditions using integrated knowledge from both data-driven analytical algorithms and other available physical knowledge. CPS benefits include completing a range of tasks which are unsafe, unpleasant or too exhausting for humans. These systems can make decisions on their own to complete tasks as autonomously as possible, plus inform management of required maintenance.

Intellectual property and trade secrets are top data theft targets for manufacturing

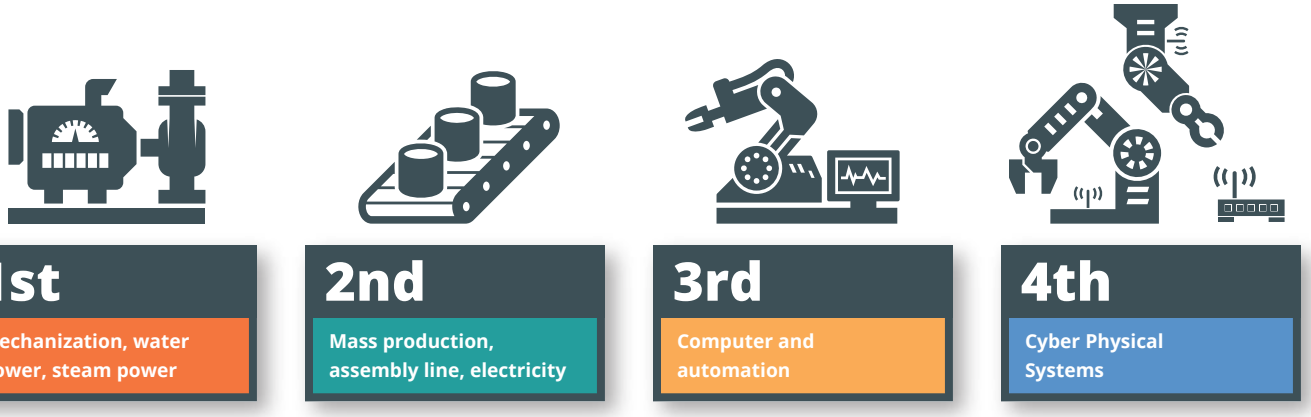
The line between traditional and digital forms of manufacturing has begun to blur, creating a unique landscape where high-value manufacturing and advanced technologies are key for global competitiveness. Manufacturing organizations have become more complex, and operate in a more complicated environment. This makes the manufacturing sector a prime target for the theft of intellectual property (IP) and trade secrets, the sabotage of processes and output, and extortion, as well as disruption of computing resources and networks.

Smart factory cyber physical systems increase manufacturing cyber risks

The first three generations of manufacturing were mainly self-contained and isolated from external access and potential threats. CPS introduces interconnectivity via Operational Technology (OT), cloud computing and data storage, as well as information sharing within communities and supply chains. Experts predict that manufacturing will become increasingly interlinked due to CPS, adding complexity to production and supplier networks. This scenario opens new doors for cyberthreats and risks.

Most industrial controls and manufacturing systems were not designed for defense against cyberattacks

As manufacturing systems move into digital infrastructure with CPS to create smart factories which are more productive, they also increase their attack surface area. In response, cybercriminals and nation-states are using automated tools to continuously scan for exploitable vulnerabilities in these systems. Threat intelligence, automated scanning capabilities, and blocking known bad sources with preventative defenses are excellent baseline defensive measures against such attacks. The scenario can be compared to an automated arms race



between organizations and cybercriminals to find exploitable vulnerabilities in manufacturing systems. The former is searching for these vulnerabilities to patch them and secure the production environment, while the latter is seeking out opportunities to exploit these vulnerabilities.

China and the United States lead in manufacturing, also as attack source countries

The top five leading manufacturing countries are China, United States, Germany, Japan and South Korea. While China benefits from labor rates at less than one-tenth those of the United States and Germany, some experts predict the United States could become the world's leading manufacturing country by 2020. Manufacturing is the leading sector at one-third of gross domestic product (GDP) for China and represents one-third of GDP for South Korea. In contrast, manufacturing represents one-fifth of GDP for Germany and Japan, and one-eighth for the United States. The United States and China are the leading attack source countries against all regions except Japan, where they rank second and third, respectively.

Japan's manufacturing sector ranks first for attacks led by hostile reconnaissance activity

The manufacturing sector in Japan ranked first among attacked industries at 24 percent, with reconnaissance activity leading at 47 percent. Attack sources from within Japan made up 55 percent of attacks on manufacturing, with reconnaissance the main type of activity from these Japanese sources. The United States, China and France followed as sources for the next 20 percent of attacks in Japan, mainly using brute force attacks and hostile activity from known bad sources.

Manufacturing is the third most attacked sector in EMEA with China as the lead attack source

While manufacturing was the most attacked industry in Japan, it was also targeted elsewhere. EMEA's manufacturing sector ranked third for attacks after business and professional services and finance, and the leading activity in EMEA's manufacturing sector came from known bad sources at 73 percent. China was the leading source country for 67 percent of attacks against manufacturing in EMEA. Attacks from the United States and Germany combined made up 10 percent, with much of the attack traffic originating from previously known bad addresses and reconnaissance activities. Manufacturing ranked fourth for attacked sectors globally, with Australia as the leading attack source country, followed by the United States and China. But, while manufacturing was a top four most attacked industry in EMEA, the Americas, Japan, and globally, it ranked sixth in APAC with only seven percent of regional attacks.

Attacks targeting manufacturing sector decline for APAC and the Americas

Ranking at number six with just under seven percent of attacks, APAC's manufacturing industry did not make the list of the top five most attacked sectors, although it ranked second in the previous year. Manufacturing remained in the top five attacked sectors in the Americas, but its ranking dropped to fourth from first in the previous year. Within the Americas, the leading activity for manufacturing was from known bad sources, while viruses and worms were the leading malware type at 49 percent. The United States at 32 percent and China at 21 percent, accounted for the majority of manufacturing attacks within the Americas.

Given the future of CPS for enabling smart factories, the manufacturing sector is one to watch for hostile activities and new cyberattacks. Analysis shows that for Japan, now is the time to address cyberthreats and cyberattacks within the manufacturing industry. In other regions, such as APAC and the Americas, a decline in attack activity likely signals a combination of improved defenses and reprioritization by attackers.

Regional Impact: Highlighting the 2020 Olympic Games

Considering the upcoming Olympic and Paralympic Games in Tokyo in 2020, the continued interest of threat actors targeting the Games, and Nippon Telephone and Telegraph (NTT) being appointed as the first Gold Partner of the 2020 Olympic and Paralympic Games, NTT Security determined a quick glimpse into the possible cyber threats the Games face – along with several mitigation strategies – was warranted.

Please note that, while NTT Security understands Japan is part of the overall Asia-Pacific (APAC) region, NTT Security has included this special section to highlight the potential threats to the upcoming Olympic Games in Tokyo in 2020.

Cyber operations against the Olympic Games in recent years are nothing new. In fact, all previous Olympic Games in recent history – from Rio to London to Pyeongchang — have been targets of cyber operations. Some have been from opportunistic threat actors (e.g., those seeking financial gain) or from those actors seeking retaliatory measures from a perceived injustice (e.g., Russian athletes being banned from the Games because of alleged performance enhancing substance misuse).

The Rio Games[8] saw those opportunists profiting from counterfeit ticket sales. The London Games[9] saw a 40-minute denial of service on the power systems in the Olympic Park on the day of the opening ceremonies.

[8] https://www.fastcompany.com/3062313/rio-olympics-hacking-cybercrime
[9] https://www.computing.co.uk/ctg/news/2252841/how-the-london-olympics-dealt-with-six-major-cyber-attacks

For the 2018 Winter Olympics in Pyeongchang, a cyberattack took out internet and television services. In an additional self-inflicted 'denial of service' of sorts, officials took down their own servers and shut down the official Pyeongchang Olympics website to prevent possible further damage. It is unknown how attackers were able to access the network, but Operation GoldDragon, a targeted campaign aimed at organizations affiliated with the Olympics in December 2017, may have been the initial entry vector, using powerful spear-phishing emails. Officials and researchers believe this operation was carried out by Russian actors, who attempted to make it look like actors from the DPRK.

Additionally, a suspected Russian-linked group dubbed Fancy Bear leaked a set of emails stolen from the United States Olympic Committee. The primary focus of these leaked emails was the correspondence with anti-doping officials investigating the potential use of illegal substances by Russian athletes.

Historically, hacktivism has been one of the major methods of attacking the "perceived adversary." Japan has historically been a target of hacktivist campaigns, including #OpKillingBay, attributed to the Anonymous group. And, the Tokyo Games will be one of a series of events over the next two years that may, in fact, incite a wave of hacktivist campaigns, including the Rugby World Cup and the change of the Emperor of Japan, both in 2019.

Hacktivism, however, appears to have greatly reduced in recent years, as other, more effective means have come to the forefront. Alternatively, threat actors likely have developed the capability to conduct more sophisticated types of attacks, along with a shift in their goals from simply defacing a website to operations which are possibly more destructive or disruptive to operations and infrastructure to get their point across.

As the geopolitical climate continues to change, as technology advances and becomes more pervasive, and as both offensive and defensive cyber operations become more of "the norm," the threat of continued – and likely more advanced – cyber operations against all aspects of the Olympic Games are not likely to end, particularly given that there are few, if any, repercussions.

The Threat to Japanese infrastructure

Looking forward to 2020, Tokyo wants to surpass the technological advancements showcased during the Olympic Games in Pyeongchang, South Korea, and aspires to be the most highly technological Olympics ever. These types of advancements, because they may not be properly secured (as many new technologies are not in their infancies), could provide a significant broadening of the playing field for threat actors seeking a name, disruption of operations, or even destruction of infrastructure.

From a geopolitical perspective, the 2020 Olympics in Tokyo only adds fodder to those wanting to conduct cyber operations against Japan. Meaning, it will provide an excuse – or a cover – for other activity.

The 2020 Games will see an increase in technologies overall, as technology is now applied to almost every facet of the Games – from housing, to medical records, to scoring. And, with this extraordinary increase in connected devices, the playing field is massive. This will provide countless ways attackers could gain access to any number of hosts, potentially allowing attackers to gain a foothold in Olympic or local Japanese infrastructure for use ahead of – or during – the Games.

To further broaden the potential attack surface available to attackers, Tokyo plans to grow its tourism industry from 29 million visitors annually to 40 million ahead of the Games – immeasurably increasing the opportunities for personal data or credential theft over unsecured Wi-Fi networks, spear-phishing, and ransomware, to name a few.

While primary targets may be the Olympic Committee itself, sensitive data pertaining to athletes, Japanese or Olympic infrastructure, corporate sponsors are also likely targets, especially those providing technological or moral support (e.g., from a patriotic perspective), could increase the chances of these organizations becoming targets.

Like the Olympics, sponsoring organizations should carefully consider what risks they can tolerate and which risks are unacceptable under any circumstances. So far, the benefits reaped (from online ticketing sales, for instance) have outweighed the potential risk. That could easily change.

Current Security Posture and NTT Security Support

Japan is already on the offense – conducting cyber security drills – currently about six times a year – which could rise to about 10 times per year leading up to the 2020 games. These drills include local government organizations.

Organizations, individuals and sponsors involved in the Games should also ensure best practices are met, at a minimum, such as knowing the network structure, including devices, software installed and the like. Verify patches are updated as soon as possible; attackers typically look for the path of least resistance – sadly, this is often a well-known, yet unpatched, flaw. Keep up-to-date with any major breaches, as attackers also quickly leverage new flaws.

As events in the Pyeongchang Games have shown, the Olympic Games have adversaries, likely at the nation-state level, with

both the intent and capability to interfere. To date, threat actors targeting the Olympic Games haven't sought to threaten injury or the actual integrity of the Games, but that may not always be the case.

Recommendations based on trends in Japan

- **Use strong passwords for user and administrator accounts.** To the extent feasible, consider using strong authentication or multi-factor authentication. The use of brute force attacks indicates attackers are concentrating on identifying weak passwords. The best way to defeat such attacks is to use strong passwords on systems which must remain exposed. If systems or applications do not need to be exposed, removing or restricting access to systems would ultimately be more effective.

- **Add DoS/DDoS protections to your external environment.** Include your internet service provider (ISP) in your DDoS solution planning, and consider commercial DDoS protection or mitigation services.

- **Enhance malware protection against Trojans and droppers.** Implement an anti-malware solution and maintain current signatures. Consider additional protection such as file integrity monitoring. Benchmark network and system traffic, and monitor ongoing traffic against that benchmark to help identify aberrant events, including unauthorized outbound traffic. This can identify infections and external attackers exerting control over organizational systems.

Report Conclusion

Business is about flexibility, but it is also very much dependent on balance: the balance between being first, and *being first with security as a priority.*

The threat landscape is dominated by email phishing threats, exploitable vulnerabilities, and insider actions. Attackers are using macros, scripts, and social engineering methods, finding unpatched vulnerabilities, and compromising access credentials. They are also using newer methods, such as compromising trusted supply chains, shared code, and applications, thereby increasing the need for software component analysis. Although their methods continue to evolve, attackers still favor the path of least resistance.

This report dived into individual industry sectors to help identify differences between who is attacking sectors and how they are being attacked. While NTT Security analyzed data across 18 sectors, some of those sectors clearly received more attention from attackers than others. As such, we presented details about the impacts and concerns in the sectors which consistently appeared in our analysis.

- The finance sector became the most attacked sector globally, despite a 46 percent drop in attack volume in APAC. Attacks against finance were characterized by extensive use of spyware and keyloggers, as well as application-based attacks.

- The technology sector experienced a 25 percent increase in attack volume, resulting in the biggest jump in any sector evaluated. Technology was the second most sector attacked globally, and the only sector to appear in the most attacked sector in every region. Hostile activity against technology was highly characterized by reconnaissance and continual attacks from sources which were previously known to be hostile.

- The business and professional services sector was the most attacked sector in EMEA, and third overall. Business and professional services attacks were dominated by application-based attacks, and experienced the second highest rate of ransomware infection.

- The manufacturing sector was the most targeted sector in Japan, but it dropped in attack ranking in nearly every region. China was responsible for 67 percent of attacks against manufacturing in EMEA. The manufacturing sector experienced high amounts of reconnaissance activity; manufacturing companies were 11 times more likely to experience brute force attacks in Japan than in any other region.

Attack sources curated in this report often represent compromised resources within those countries, and serve as a starting point in tracing an attack. However, attackers often hide behind anonymous systems and compromised identities, making attribution difficult. The use of highly visible smoke screen attacks is common to hide smaller and more targeted attacks, and to distract security staff, who have limited resources. Even without full attribution, this report's analysis points to methods used by attackers in specific industries and regions, and helps indicate where to focus limited security resources.

Defending your organization is no small task, but focusing on key areas can really help. Fundamental practices discussed in this report include:

- Develop incident response plans and test your capabilities against the most common threat scenarios for your industry and region.

- Require multi-factor and strong authentication. Many of the threats we observe today can be mitigated by implementing proper detective and preventative controls, including the use of enhanced authentication.

- Focus on ensuring operating system and application patching processes are comprehensive and reliable. Prioritize patching efforts based on your exposure and highest risk vulnerabilities.

- Security must be usable to be effective. Implement controls which have less complexity but a higher adoption rate, rather than unrealistic controls which cripple the business or fail to be adopted. Carefully identify the best policies your organization can implement with its security goals in mind.

NTT Resource Information

Global Threat Intelligence Center (GTIC)

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

- Threat research
- Vulnerability research
- Detective technologies development
- Threat intelligence management
- Communication to NTT Group clients

The GTIC goes above and beyond the traditional pure research organization, by taking its threat and vulnerability research and combining it with its detective technologies development to produce applied threat intelligence. Its mission is to protect and provide NTT Security clients with the services and tools to prevent and provide early warning notifications of risks and threats 24/7.

Threat intelligence management is where it all comes together. The GTIC continuously monitors the global threat landscape for new and emerging threats using NTT's global internet infrastructure, clouds, and datacenters along with 3rd-party intelligence feeds. NTT Security works to understand, analyze, curate, and enrich threat data using advanced analysis techniques and proprietary tools; and publishes and curates them using the Global Threat Intelligence Platform (GTIP) for the benefit of NTT Security clients.

NTT Group Resources

NTT Security

NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies (Dimension Data, NTT Communications and NTT DATA) to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit nttsecurity.com to learn more about NTT Security or visit www.ntt.co.jp/index_e.html to learn more about NTT Group.

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

Partnering for Global Security

NTT Communications

NTT Communications provides consultancy, architecture, security and cloud services to optimize the information and communications technology (ICT) environments of enterprises. These offerings are backed by the company's worldwide infrastructure, including the leading global tier-1 IP network, the Arcstar Universal One™ VPN network reaching over 190 countries/regions, and over 140 secure data centers worldwide. NTT Communications' solutions leverage the global resources of NTT Group companies including Dimension Data, NTT DOCOMO and NTT DATA. Visit www.ntt.com to learn more.

NTT DATA

NTT DATA partners with clients to navigate the modern complexities of business and technology, delivering the insights, solutions and outcomes that matter most. We're a top 10 global IT services and consulting provider that wraps deep industry expertise around a comprehensive portfolio of infrastructure, applications and business process services.
Visit www.nttdataservices.com to learn more.

Dimension Data

Dimension Data's security business supports organisations in creating an adaptable and predictive security posture across their network, data assets, cloud, applications, and the digital workplace. With our end-to-end portfolio of security capabilities including consulting, a suite of technical, support and managed security services, we help our clients through the full security lifecycle.

Founded in 1983, Dimension Data is a USD 8 billion global leader in designing, optimising, and managing today's evolving technology environments. This enables its clients to leverage data in a digital age, turn it into information, and extract insights.

Headquartered in Johannesburg, Dimension Data employs 28,000 people across 46 countries. The company brings together the world's best technology provided by market leaders and niche innovators with the service support that clients need for their businesses – from consulting, technical, and support services to a fully-managed service.

Dimension Data is a proud member of the NTT Group. Visit us at www2.dimensiondata.com

NTT Security Global Data Analysis Methodology

The NTT Security 2018 Global Threat Intelligence Report contains global attack and incident response data gathered from NTT Security and supported operating companies from October 1, 2016, to September 31, 2017. The analysis is based on log, event, attack, incident and vulnerability data from clients. It also includes details from NTT Security research sources, including global honeypots and sandboxes located in over 100 different countries in environments independent from institutional infrastructures.

With visibility into 40 percent of the world's internet traffic, NTT Security summarizes data from over 6.1 trillion logs and 150 million attacks for the 2018 GTIR. NTT Security gathers security log, alert, event and attack information, enriches it to provide context, and analyzes the 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 Security with a set of 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 Security provides a highly accurate representation of the ever-evolving global threat landscape.