2018

GLOBAL THREAT INTELLIGENCE REPORT

NTT Security

PARTNERING FOR GLOBAL SECURITY

NTT Communications

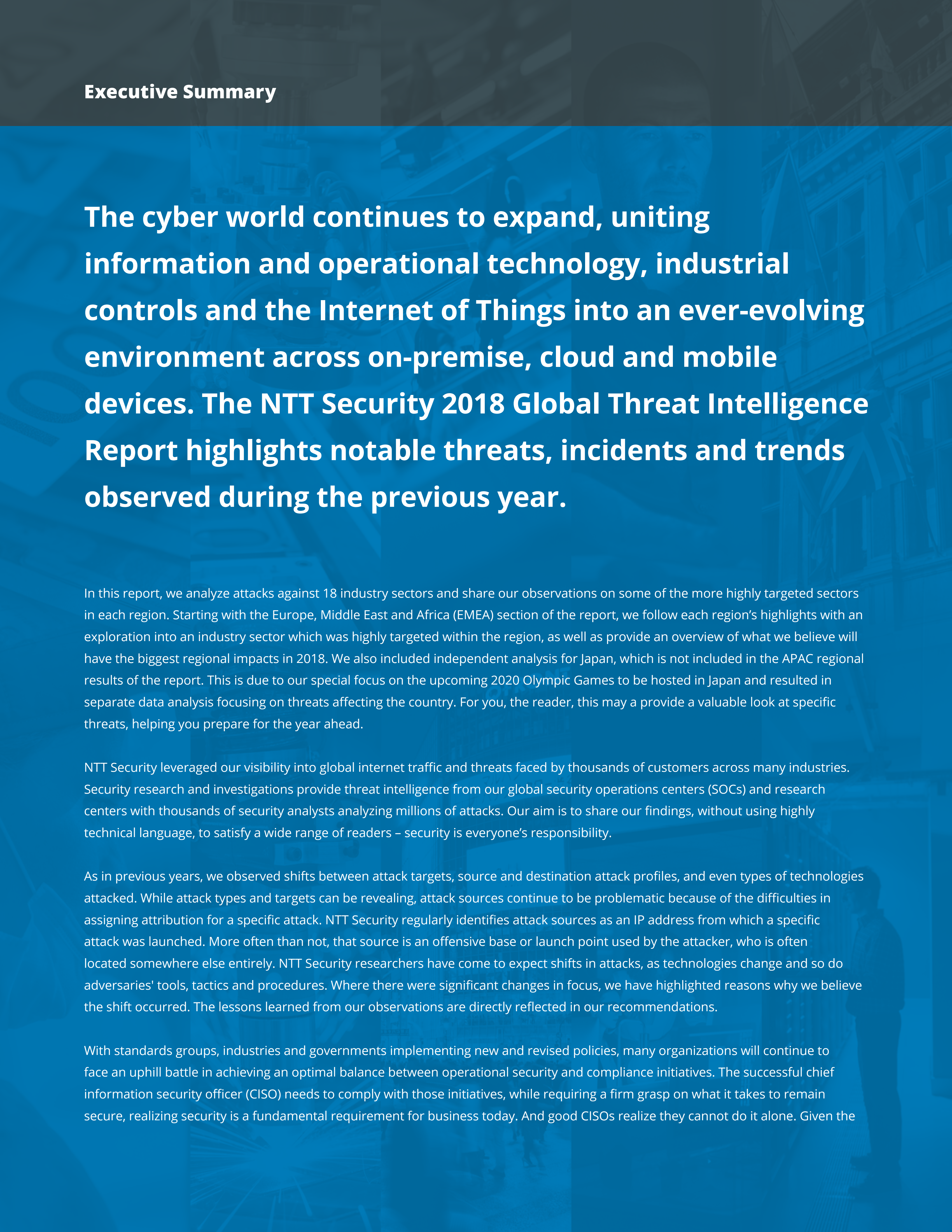
www.ntt.com

NTT DATA

www.nttdataservices.com

dimension data

www2.dimensiondata.com



Executive Summary

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 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.

Key Findings

NTT Security

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.

Key Findings

- 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.

Conclusion

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 sector. 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.