



2017 Global Threat Intelligence Report



Table of Contents

Executive Summary	3
Key Findings	5
Global Findings	5
EMEA Findings	5
Americas Findings	6
Asia Findings	6
Australia Findings	6
Japan Findings	6
Incident Response Findings	6
Focus on the Global View	7
Focus on Europe, Middle East and Africa (EMEA)	9
2016 at a glance	11
Business Challenge: Phishing, Social Engineering, and Ransomware	12
How Can Phishing Affect You and Your Organization?	12
How Does This Happen?	14
What Can You Do About This?	14
Focus on Americas	16
2016 at a glance	16
Business Challenge: Business Email Compromise/CEO Fraud	18
How Can This Affect You and Your Organization?	18
How Does This Happen?	19
What Can You Do About This?	19
Focus on Asia	21
2016 at a glance	21
Business Challenge: The Internet of Things and Distributed Denial of Service Attacks	23
How Can This Affect You and Your Organization?	23
How Does This Happen?	23
What Can You Do About This?	25
Focus on Australia	27
2016 at a glance	27
Business Challenge: Attacks Against End User Technology	29
How Can This Affect You and Your Organization?	29
How Does This Happen?	31
What Can You Do About This?	32

Table of Contents

Focus on Japan.....	33
2016 at a glance	33
Business Challenge: Securing the G7 Summit.....	35
Overview of Ise-Shima Summit.....	35
Cyber Threat Landscape in Japan.....	35
How We Prepared.....	36
Coordinated Structure	36
Incident Handling Rehearsal.....	36
Sharing Vulnerability Information	36
Collecting and Analyzing Open Source and Dark/Deep Web Intelligence	36
Supporting Around the Clock Operations.....	37
Lessons Learned	37
Conclusion	38
NTT Security Resource Information.....	39
NTT Security Global Data Analysis Methodology	39
About Us.....	39
NTT Security.....	39
Dimension Data.....	39
NTT Communications	39
NTT-CERT	40
NTT Innovation Institute	40

Executive Summary

The goal of this report is not only to demonstrate the impact of today's threats against every kind of organization around the world, but also to make cybersecurity personal, interesting, and relevant to the people being targeted by these threats. This report explains what the most important threats are and how they work, for readers interested in those topics. However, the key focus of this report is to emphasize actions management, technical staff, and users can take to improve security.

Most cybersecurity reports are meant for security professionals. They're not intended for use by anyone without significant security knowledge and experience. NTT Security has taken a different approach for this year's Global Threat Intelligence Report (GTIR). We want to provide a resource for educating everyone with security responsibilities, from security and IT professionals to executives, management, and end users. In today's environment, everyone has an important role to play in cybersecurity. Effectively communicating the importance of security to all groups, from decision makers at the executive level to the users who are exposed to attacks on a daily basis, is an ongoing challenge at nearly every organization.

At NTT Security, we have identified the top threats, analyzed their activities, and determined how they should be handled by organizations. This is based on our analysis of trillions of security relevant logs over the past year. On our clients' networks across six continents, we identified over six billion attempted attacks. We monitored threat actors using nearly every type of attack imaginable. We assisted organizations with data breach investigations, collected and analyzed global threat intelligence, and performed our own security research. The lessons learned from all these efforts are directly reflected in recommendations throughout this report.



Executive Summary








For leadership, we have defined three overarching principles to adopt:

- 1. Security is a business problem.** Security strategy and practice are needed so your organization can conduct business while safeguarding its sensitive information and ensuring its services are available whenever needed. Security is not performed just for the sake of “doing security things,” but rather to support the needs of the business. Security should be considered a basic business requirement.
- 2. Security is much more than technology.** Security is technology, processes, and people working together. Throwing more technology at a security problem without taking processes and people into consideration may do more harm than good. Also, with threats changing and evolving so quickly, most organizations can’t possibly add new security technologies at a pace which can keep up with evolving threats. This means organizations must often rely on people and processes to compensate for the use of older security technologies.
- 3. Security practices need to be more helpful to users.** Attackers are targeting users more than ever, but it’s unrealistic to think exposing users to a few hours of security awareness training, conducted at best once a year, will be effective at stopping attacks. Users need help from technologies which prevent attacks from reaching them. Users also need security support which helps users differentiate the malicious from the benign. Users must be empowered to do their jobs while protecting sensitive data. Leaving it all in users’ hands is unfair and unrealistic.


Users face a significant set of problems, not the least of which is managing their own security expectations and maximizing their ability to protect both personal and organizational data. The good part of this equation is that the interests of users and those of the organization are usually in alignment. Controls designed to protect the user also protect the organization – and the reverse is true as well.

This report contains recommendations for management, technical staff, and users. It also presents interesting findings from NTT Security analysis of real-world security event data from the past year. These findings will assist you to in understanding just how pervasive certain types of attacks are so you see how they affect all organizations, including yours. Our hope is this report will enable you to improve your own daily security practices, and perhaps the practices of others as well.




Global Findings





-  Phishing attacks were responsible for as much as 73 percent of malware being delivered to organizations.
-  Nearly 30 percent of attacks detected worldwide targeted end-user technology like Adobe products, Java and Microsoft Internet Explorer.
-  The three technologies found on end-user computers which were targeted most throughout the year were Adobe Flash Player, Microsoft Internet Explorer, and Microsoft Silverlight.
-  Only 13 percent of exploit kit activity detected throughout the year occurred during the third quarter of 2016, showing a steady decline in exploit kit activity throughout the year.
-  77 percent of all detected ransomware was in four industries – business and professional services (28 percent), government (19 percent), health care (15 percent), and retail (15 percent).
-  The finance industry was the only industry to appear in the “top three most attacked industries” in all six geographic regions analyzed. The next most commonly attacked industry was manufacturing, appearing in the “top three” in five of the six regions. No other industry appeared in the top three more than twice.
-  25 passwords accounted for nearly 33 percent of all authentication attempts against NTT Security Honeypots.
-  Over 76 percent of authentication attempts included a password known to be implemented in the Mirai IoT botnet.
-  Globally, distributed denial of service (DDoS) attacks accounted for less than 6 percent of all attacks, but DDoS attacks accounted for over 16 percent of all attacks from Asia, and 23 percent of all attacks from Australia.

EMEA Findings

-  Source IP addresses in EMEA accounted for 53 percent of the world's phishing attacks. The Netherlands alone accounted for over 38 percent of all phishing detections.

Legend

-  Focus on impact of the user
-  Focus on impact of technology
-  Focus on general impact


-  In EMEA, three industries were targeted in 54 percent of all attacks – finance (20 percent), manufacturing (17 percent), and retail (17 percent).
-  Of attacks targeting EMEA, the United States (26 percent), France (11 percent), and the United Kingdom (10 percent) accounted for the most attacks.
-  45 percent of brute force attacks targeting EMEA also originated within EMEA.
-  NTT Security detected more brute force attacks originating from EMEA (45 percent) than from the Americas (20 percent) and Asia (7 percent) combined.

Honeypots are systems built as lures, specifically built to attract attackers, and gather information from cyberattacks directed against the honeypots.





Mirai is a specific botnet composed of Internet of Things devices. A botnet is a network of remotely controlled systems. Mirai was used to conduct what was, at the time, the largest ever denial of service attacks – a flood of communications designed to make the target system unusable.

P2P – Peer-to-peer traffic is communications directly between computers, without going through a central server or hub. It is often used for file sharing.

bash is a command line interpreter used to support computer administration.

-  Over 67 percent of the malware detected within EMEA were some form of Trojan.





Americas Findings

-  Clients in the Americas accounted for nearly 99 percent of outbound P2P traffic. Detections included applications like BitTorrent, Hola VPN, and Groove Virtual Office.
-  After the United States (54 percent), China (17 percent) was responsible for more attacks against clients in the Americas than any other source country.
-  In the Americas, three industries were targeted in 58 percent of all attacks – manufacturing (23 percent), education (20 percent), and finance (15 percent).
-  At nearly 15 percent of all attacks, malware was the most common form of attack detection within the Americas.


Asia Findings


-  In Asia, two industries were targeted in 78 percent of all attacks – finance (46 percent) and manufacturing (32 percent).
-  Malware was the top attack type with Asia both as a source (29 percent) and as target (12 percent).
-  About 60 percent of all global Mirai detections showed source IP addresses in Asia.



Australia Findings

-  In Australia, three industries were targeted in 81 percent of all attacks – finance (34 percent), and retail (27 percent), along with business and professional services (20 percent).
-  Over 93 percent of the malware detected within Australia was some form of Trojan.
-  Over 70 percent of application attacks against Australian targets attempted remote code execution.
-  Over 50 percent of application attacks in Australia targeted bash.







Japan Findings

-  In Japan, three industries were targeted in 83 percent of all attacks – manufacturing (41 percent), media (26 percent), and finance (16 percent).

-  Japan was the largest single source of botnet activity, accounting for nearly 48 percent of all such activity.

-  Nearly 44 percent of the malware detected within Japan were some form of spyware or key logger.
-  Malware cases accounted for 82 percent of critical incidents in Japan.

Incident Response Findings

-  Over 60 percent of incident response engagements were related to phishing attacks.
-  Incident engagements related to ransomware were the single most common (22 percent).
-  50 percent of all incidents in health care organizations were related to ransomware incidents.
-  59 percent of all incident response engagements were in four industries – health care (17 percent), finance (16 percent), business and professional services (14 percent), and retail (12 percent).
-  Globally, 32 percent of organizations had a formal incident response plan. This is up from an average of 23 percent in previous years.
-  56 percent of all incidents in finance organizations were related to malware.

Focus On **The Global View**



Top attack source countries

- United States (63%)
- United Kingdom (4%)
- China (3%)
- Other (30%)



Top targeted sectors

- Government (14%)
- Finance (14%)
- Manufacturing (13%)
- Other (59%)



Top attack categories

- Website application attack (16%)
- Service specific (8%)
- Application specific (6%)
- DoS/DDoS (6%)
- Other (64%)



Cyber threats are now having an impact to the bottom line of most organizations. Awareness in the boardroom and at the C-level is becoming essential as these evolutions take shape:

- 1. Explosive growth of endpoint devices, such as mobile-optimized applications, along with internet of things (IoT), operational technology (OT) and cloud services adoption increase complexity and potentially additional risks.*
- 2. Adversaries are well financed and continue to evolve the sophistication of their attack techniques.*
- 3. New data protection laws and regulations are reaching across geopolitical boundaries.*

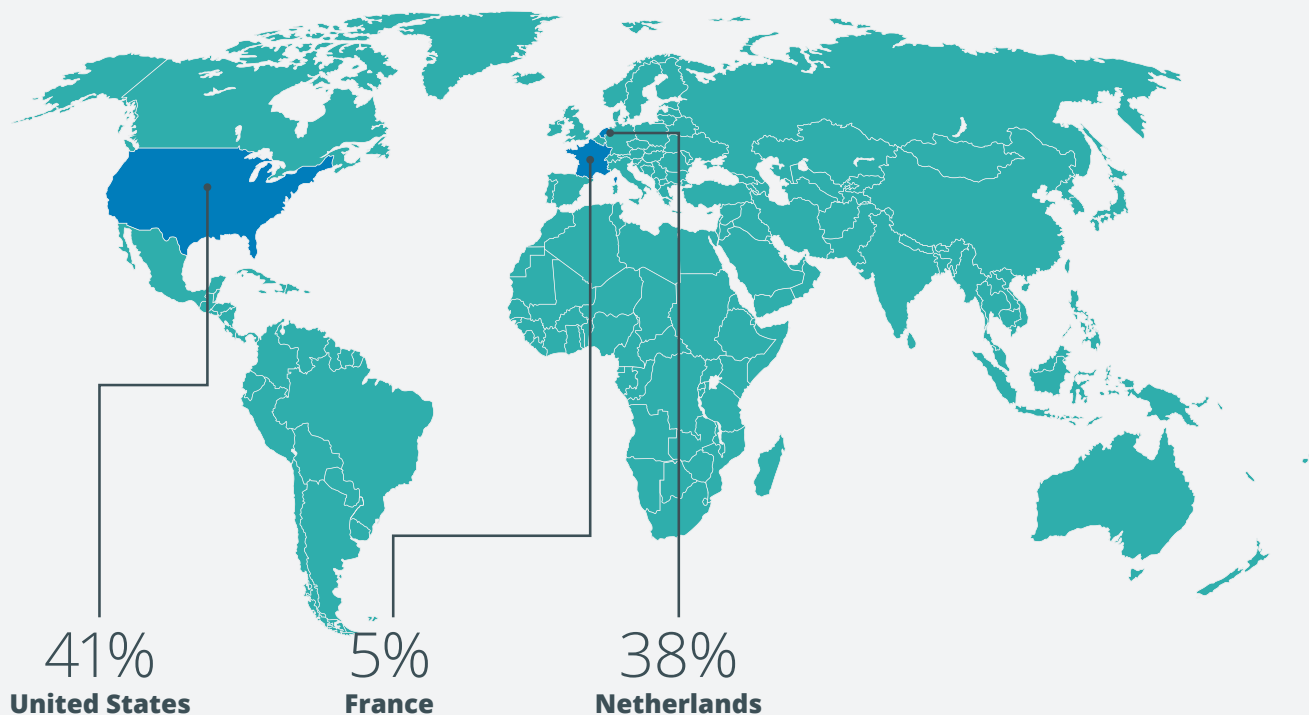
NTT Security is seeing executives become more proactive, allocating resources based on specific business risks. Organizations are establishing a frontline defense, investing in threat intelligence and expanding their cyber response capabilities. Executives are taking notice that a breach into their enterprise system is a possibility, and they are now preparing for it. CEOs are starting to realize that you must have a plan in place. Being prepared and having a tested response plan, coupled with actionable threat intelligence, can limit the impact of a breach, while also supporting clear business justification for that plan. Any investment in threat intelligence must produce relevant, accurate, timely, transparent, and actionable information in order to be truly impactful. Executives must ask themselves the question – how does implementing this plan strengthen the security posture of my company?

Jun Sawada, CEO, NTT Security

Focus On **The Global View**



Top phishing sources:



Top phishing attack targets:

1	Government (65%)
2	Business & Professional Services (25%)

Top incident response engagement types:

1	Ransomware (22%)
2	Breach Investigation (22%)
3	Malware (18%)

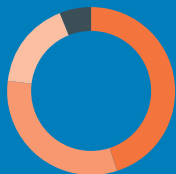
Top sectors supported for incident response:

1	Health Care (17%)
2	Finance (16%)
3	Business Services (14%)
4	Retail (12%)

Percentage of organizations having an incident response plan:

32%

Focus On **Europe, Middle East and Africa (EMEA)**



Top services used in attacks against EMEA

- File shares (45%)
- Websites (32%)
- Remote administration (17%)
- Other (6%)



Top attack categories from EMEA

- Website application attack (22%)
- Application specific attack (17%)
- Brute force (11%)
- Other (50%)



Top attack categories targeting EMEA

- Website application attack (19%)
- Application specific attack (15%)
- DoS/DDoS (9%)
- Other (57%)



In order to make specific and strategically sound business decisions, clients are finding ways to measure their security posture by making cybersecurity more visible, measurable, and accountable. We all know that no security plan is guaranteed, and there will always be some level of exposure, but defining your acceptable level of risk is important. Clients are starting to understand that by default every employee is part of their organization's security team, and businesses are now seeing the value in security awareness training, knowing that educating the end user is directly connected to the mission of securing their enterprise. Expanding cyber education and ensuring employees adhere to a common methodology, set of practices, and mindset are key elements. Clients see that assisting and coaching their employees (end users) on the proper usage of technology will only enhance the organization's overall security presence.

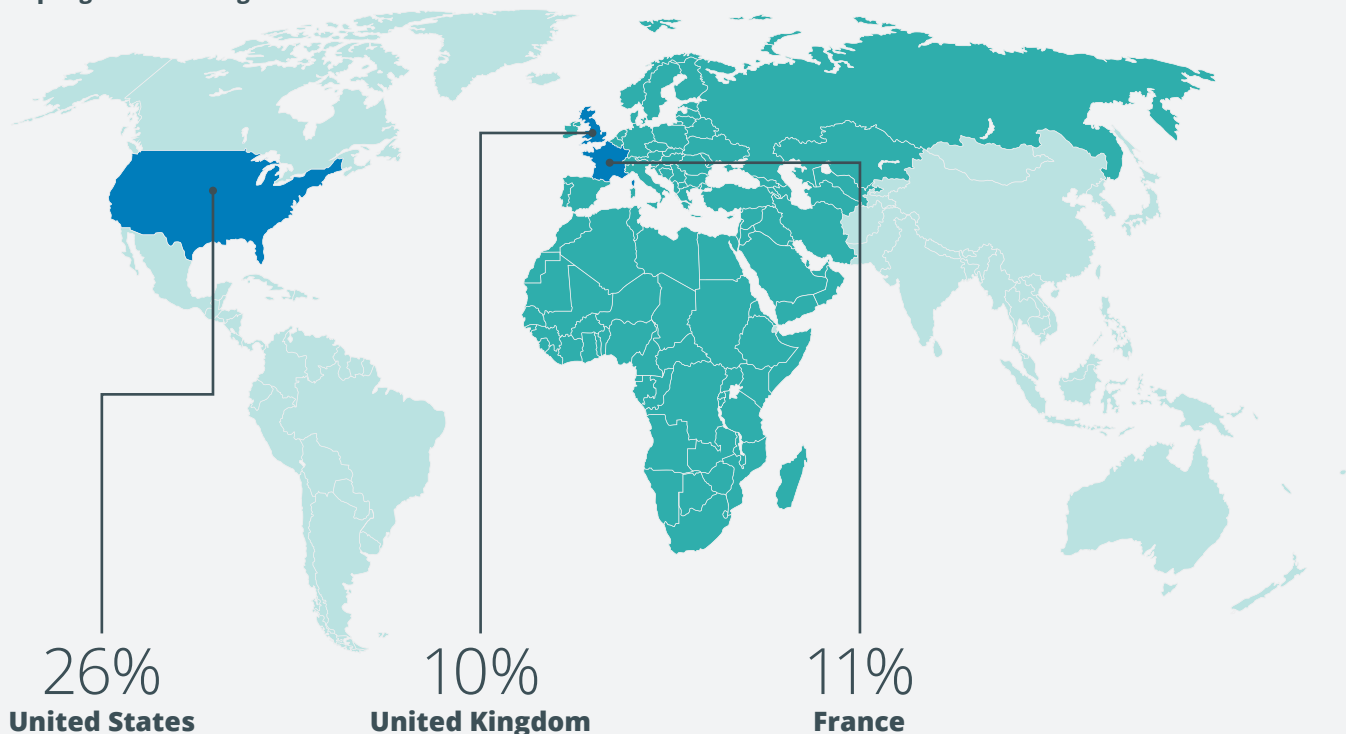
With mobile use, remote access, cloud services, virtualization, and other technological advances, access to most organizations' enterprise perimeters have expanded. The dynamics of allowing users to access networks through a wide variety of types of devices and applications has forced companies to adjust their current cybersecurity practices. Organizations must know who the end user is, what role they have and what they should have access to. Organizations must now invest in strong authentication, role-based access, and subsequently, harden the authorization processes.

Frank Brandenburg, COO and Regional CEO, NTT Security

Focus On **Europe, Middle East and Africa (EMEA)**



Top regions attacking EMEA:



Top services used in attacks against EMEA:

1	File Shares (45%)
2	Websites (32%)
3	Remote Administration (17%)

Top malware types from EMEA:

1	Trojan/Dropper (67%)
2	Virus/Worm (15%)



38%

of worldwide phishing attacks come from the Netherlands.

53%

of worldwide phishing attacks come from EMEA.

Focus On **Europe, Middle East and Africa (EMEA)**



2016 at a Glance

With the European Union (EU) General Data Protection Regulation (GDPR) around the corner, adopted April 27, 2016 and entering into application May 25, 2018, any organization processing data belonging to EU citizens will need to be able to demonstrate that their processing is lawful and that their information security measures are robust. With heavy fines and grave reputational impacts in the balance, organizations must address their risks in this space without delay.

This includes restrictions imposed by customers on “data residency” – the principle that data must be stored and maintained where it is gathered and used. This has continued to push the envelope with service providers. The flexibility of cloud computing and globally-resourced managed service providers, coupled with customers' need to contain data storage and processing within their national boundaries means that development of innovative security solutions is critical to stop data leakage – both accidental and malicious – across geographic borders.

Compliance and certification with internationally respected bodies such as the International Organization for Standardization's ISO 27001 standard and other national security management benchmarking agencies (such as the UK Government's Cyber Essentials scheme) have also proven to remain a critical focus area in EMEA during 2016.

These efforts have helped elevate attention to cybersecurity to the point organizations are taking significant actions. In December 2016, Europol, the U.S. Federal Bureau of Investigation (FBI), and German police worked alongside many other law enforcement agencies to disrupt activities related to the “Avalanche” campaign. The joint effort resulted in the coordinated takedown of over 800,000 malicious websites and domains, and prevented attacker access to the malicious systems. This type of active collaboration is critical if we want measures to have a long-lasting impact on global cybersecurity.

The need for this type of collaboration is no more evident than it is for preventing and managing phishing attacks. While phishing attacks affected clients in every region, EMEA had the unfortunate distinction of showing as the source of 53 percent of the world's phishing attack, with IP addresses in the Netherlands accounting for 38 percent of those attacks. The challenges of phishing attacks are discussed in the next section.

Anyone who uses email, texting, or other forms of messaging is probably all too familiar with phishing. Phishing is when attackers create messages and websites mimicking their legitimate counterparts in order to trick people into taking some action as requested by the attacker. Examples include typing passwords into a phishing website or following instructions in a phishing email. Phishing is a form of social engineering, a broad term for attackers conning people into doing things they shouldn't do, all for the benefit of the attacker.

Over the last few years, phishing has become widely used as a mechanism for distributing ransomware. Ransomware is a form of malware which essentially holds information or entire devices, such as desktops, laptops, or servers, hostage. In most cases, the person or organization must pay ransom to the attacker in order to regain access to the information or devices. Ransomware commonly works by encrypting files and safeguarding the key needed to decrypt those files. When the ransom is paid, the attacker often, but not always, provides the key or decrypts the files. If the attacker doesn't provide the key, the information or devices remain inaccessible, or in some cases, the information may be released to the public.

How Can Phishing Affect You and Your Organization?

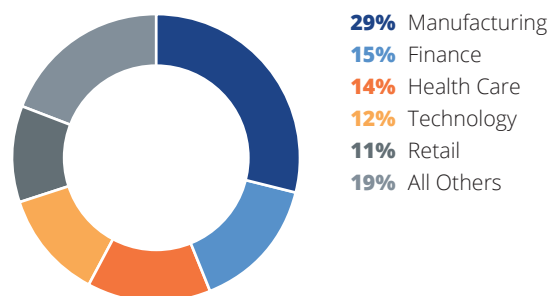
Attackers perform phishing attacks with many motives, but here are some of the most common reasons and their potential consequences:

- **Infesting an employee's computer with malware.** An attacker could do this as a first step in a larger attack, such as a data breach. However, this is often done to install ransomware and coerce organizations into paying ransom. Based on analysis of NTT Security detections, phishing attacks were responsible for as much as 73 percent of malware being delivered to organizations.
- **Obtaining personal information for one or more employees.** This enables the attacker to commit identity theft, such as opening a credit line in the employee's name or making purchases using the employee's existing credit cards, or to sell the stolen information to other attackers.
- **Getting an employee's username and passwords.** An attacker can use these to access the organization's systems, applications, and data. The ultimate result of this could be anything from preventing the organization from doing business to causing a major data breach.

Enterprise clients face a wide array of threats. While advanced malware may be a significant issue, attackers do not limit themselves, and complex security breaches and intellectual property theft from organized groups and potential state sponsored attacks require more advanced strategies.

Kazuhiro Gomi, President & CEO, NTT America

Phishing by Industry



Ransomware by Industry

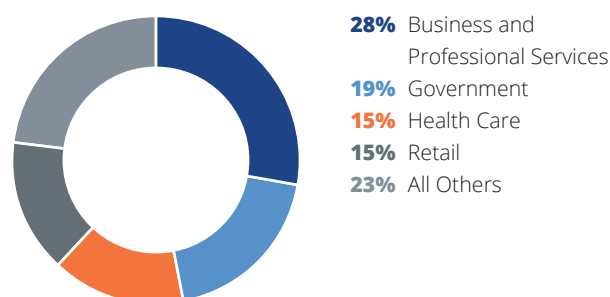


Figure 1: Phishing and Ransomware by Industry

Business Challenge: Phishing, Social Engineering, and Ransomware



- **Convincing an employee to perform wire transfers.** This can cause an organization to lose millions of dollars in a matter of minutes. See the “[Business Email Compromise](#)” section in this report for more information on this highly focused form of phishing.

Phishing attacks are constantly being launched at every organization and employee. Over 60 percent of recent NTT Security incident response engagements were initiated to help organizations manage phishing attacks. Figure 1 identifies the sectors most often impacted by phishing attacks from October 2015 through September 2016, along with the sectors impacted by ransomware attacks during the same timeframe. Health care and retail appear in the top five industries targeted by both phishing and ransomware. This does make some sense that attackers targeting these industries with phishing attacks are also targeting them with ransomware, as these are two of the industries which have the strongest drive to maintain continual operations. The strong correlation between phishing and ransomware attacks in health care and retail is likely no accident,

and highlights the impact phishing campaigns can have. The difference between phishing attacks and ransomware attacks in other industries primarily indicates that phishing was being used to deliver other attacks besides ransomware, such as other forms of malware.

Figure 2 looks at some of the more obvious quarterly trends in phishing volumes for selected industries. While some industries, like retail, were exposed to consistent levels of phishing attacks throughout the year, other industries saw definite spikes in attacks, some of which were related to specific campaigns. For instance, government clients recorded 90 percent of their annual phishing attacks during the second quarter of 2016 alone. Much of the higher volume in this timeframe has been attributed to a group known as APT28, also known as Sofacy or Fancy Bear. There are many indicators that this well-run and organized hacking group has ties to espionage activities for the Russian government. During the second quarter of 2016, APT28 conducted a large phishing campaign against government agencies in the United States and other countries, as well as the North Atlantic Treaty Organization (NATO).¹

Industry Phishing Volumes

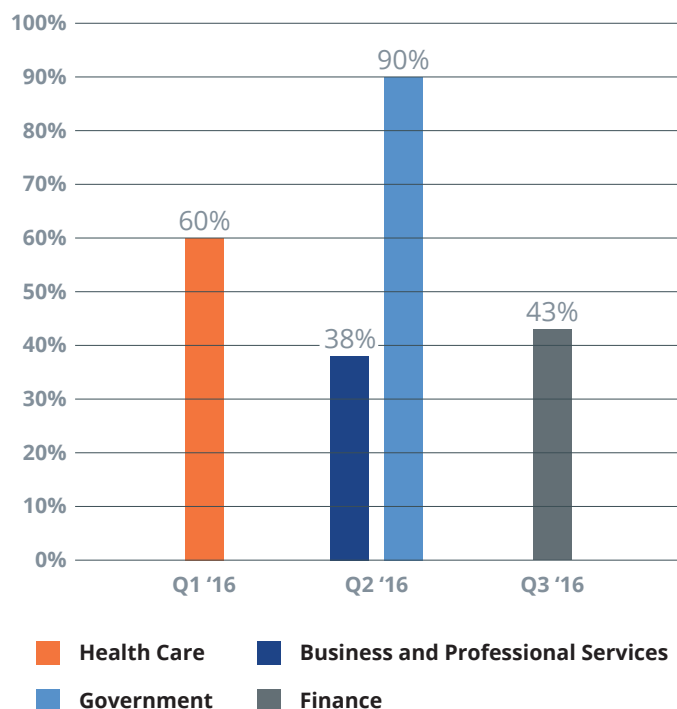


Figure 2: Industry Phishing Volumes

The health care industry also showed significant spikes, and received 60 percent of their phishing attacks of the past year in the first quarter of 2016. The health care sector has been particularly hard-hit by ransomware, with half of NTT's 2016 incident response engagements for health care institutions involving ransomware. Health care organizations were also the most likely industry to obtain incident response support, and about 50 percent of their incidents related to ransomware attacks. This may indicate that attackers have identified health care institutions as a vulnerable target more willing to pay ransom than other sectors.

The typical impact of ransomware is not what you might expect. Ransoms are usually relatively low, and organizations can easily afford them—although there are exceptions. In the best cases, organizations can safely restore from an uninfected backup. In the worst cases, organizations can pay ransoms over \$50,000 USD and not get their data restored, since there is no guarantee paying a ransom will result in decryption. The vast majority of costs to organizations involve the inability to provide service to their customers while the ransomware is in place and embarrassment to the organization if the ransomware attack becomes publicly known.

¹ <http://www.federaltimes.com/story/government/cybersecurity/2016/06/14/apt28-sofacy-us-officials/85866698/>

Business Challenge: Phishing, Social Engineering, and Ransomware



How Does This Happen?

Most of today's phishing attacks are highly sophisticated and thus can be difficult for people to distinguish from legitimate messages. Because it's human nature to be trusting, people see something which looks like messages or websites they've seen before, so they don't question it. When someone calls a person and says they're from the help desk, that person is likely to believe them. Even if a person thought to question the caller's identity, as well as the source of each received message, it takes time, knowledge, and experience to be able to investigate each case and decide what to do.

Phishing attacks are essentially a form of social engineering attack. The attacker takes advantage of human nature to manipulate people into doing what the attacker wants. The most elaborate social engineering attacks may be preceded by extensive research so that the attacker can pose as an employee, contractor, or vendor with authorized access to sensitive facilities. It may sound like the stuff of movies, but it really does happen.

As for ransomware, it usually gets delivered to users' computers through phishing or other forms of social engineering. A user may be tricked into downloading and executing a rogue application, or a user's computer may have vulnerabilities that the ransomware can exploit simply by the user visiting a malicious website.

What Can You Do About This?

Here are some recommendations you and your coworkers can follow to reduce your organization's chances of being victimized by phishing attacks in general and ransomware attacks in particular.



Everyone:

1. Check emails, texts, and other messages for any signs of phishing before clicking on links or attachments. Whenever possible, visit the official website directly (by typing in the URL or using a bookmarked URL) instead of clicking on a link. For file attachments, avoid opening them until you can verify they are legitimate. There is nothing wrong with calling the sender to ask if they emailed you an attachment.
2. If you receive requests which seem unusual in any way, verify their legitimacy before following the instructions. For example, if someone says they are calling from the help desk and they need your password to resolve a problem, get their name and tell them you'll call them back at your organization's main help desk number.
3. Don't give out any information the person contacting you should already have. For example, if someone calls claiming to be from your credit card company, don't give them your credit card number.
4. Don't download and install new software onto your corporate desktop or laptop unless specifically authorized to do so.



Management:

1. Require regular security awareness training for all users so they are up to speed on phishing, social engineering, and ransomware, especially how to identify attacks, what to do if they need help, and how to report possible attacks.
2. Strengthen the organization's business continuity capabilities to help ensure quick restoration of operations if a ransomware incident happens. This includes a comprehensive backup strategy, including secure storage of offline backups, as well as confirming the organization's ability to rebuild systems and restore data.
3. Schedule and perform regular assessments in the form of phishing attack simulations emulating real world threats. This is a great way to determine if your training and awareness programs are effective and allow for opportunities to further enrich defensive capabilities.
4. Develop a policy for handling ransomware incidents. Decide under which conditions a ransom payment is authorized, if any.



Technical Staff:

1. Use anti-phishing and anti-malware technologies to stop phishing emails, links to phishing sites, ransomware files, and other phishing attack components from reaching users. These technologies should be kept up-to-date at all times. Any anti-phishing or anti-malware technologies installed on end user devices should be set up so users can't reconfigure or disable them.
2. Ensure valid data backups are occurring at the predetermined frequency. This includes monitoring the status of backup systems and software, and regularly testing restoration capabilities. The data backups need to be well secured, especially if they are kept online, so they cannot be encrypted by ransomware.

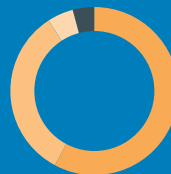
3. Ensure systems can be rebuilt quickly. For example, you may keep standard images or baselines for building new systems. If so, these images and baselines should be kept up-to-date at all times.
4. Minimize opportunities for ransomware to be installed by giving users the least privileges possible (especially restricting access to administrator-level privileges), and keeping systems fully patched. Use software configuration settings to prevent ransomware installation and minimize the impact if ransomware is installed.
5. Follow the principle of least privilege for file access on servers and other systems available through file shares. This reduces the impact of ransomware encrypting files on these systems.
6. Limit administrator-level privileges as much as possible. Require people to use administrator accounts only when necessary and to use regular user accounts for all other tasks. This reduces the chances attackers will be able to gain immediate access to administrator privileges through a single attack.
7. If feasible, use application whitelisting on servers, desktops, and laptops so ransomware and other unauthorized executables can't be run.
8. Use firewalls, routers, and other network security devices to implement and enforce network segregation. This means restricting the flow of network traffic between network segments with different security profiles.

Focus On **Americas**



Top attack categories from Americas

- Evasion attempts (13%)
- Website application attacks (12%)
- DoS/DDoS (6%)
- Other (69%)



Top services used in attacks against Americas

- Websites (58%)
- File shares (33%)
- Remote administration (5%)
- Other (4%)



Top attack categories targeting Americas

- Malware (15%)
- Evasion attempts (13%)
- Web application attacks (11%)
- Other (61%)



In today's environment the cyber threat to our world is real. Our adversaries are well financed, patient and have a wide range of skills. The sophistication of their attack techniques continues to rapidly evolve. We have more data than ever before as the number of connected devices increases daily. Organizations and end users benefit from innovation in IoT, OT, cloud, automation, mobile, and other forms of modernization. These innovations only increase challenges to secure this interconnected and expanding attack surface. This clarifies the need for detection policies and procedures along with an orchestrated defense which includes advanced response capabilities in order to ensure that these innovative technologies are properly protected from evolving threats.

Developing a mature and proactive security approach is essential to protecting and defending agile and dynamic environments against increasingly opportunistic and targeted threats.

Mike Hrabik, CTO and Regional CEO, U.S., NTT Security

2016 at a Glance

Ransomware played a very large part in the most prevalent types of attacks observed in the Americas during 2016. Many organizations found themselves asking, "Do I pay ransom in the form of Bitcoin to get my data back?" On a positive note, NTT Security also observed many organizations that were prepared to combat this threat, but there is a long way to go until organizations are truly resilient.

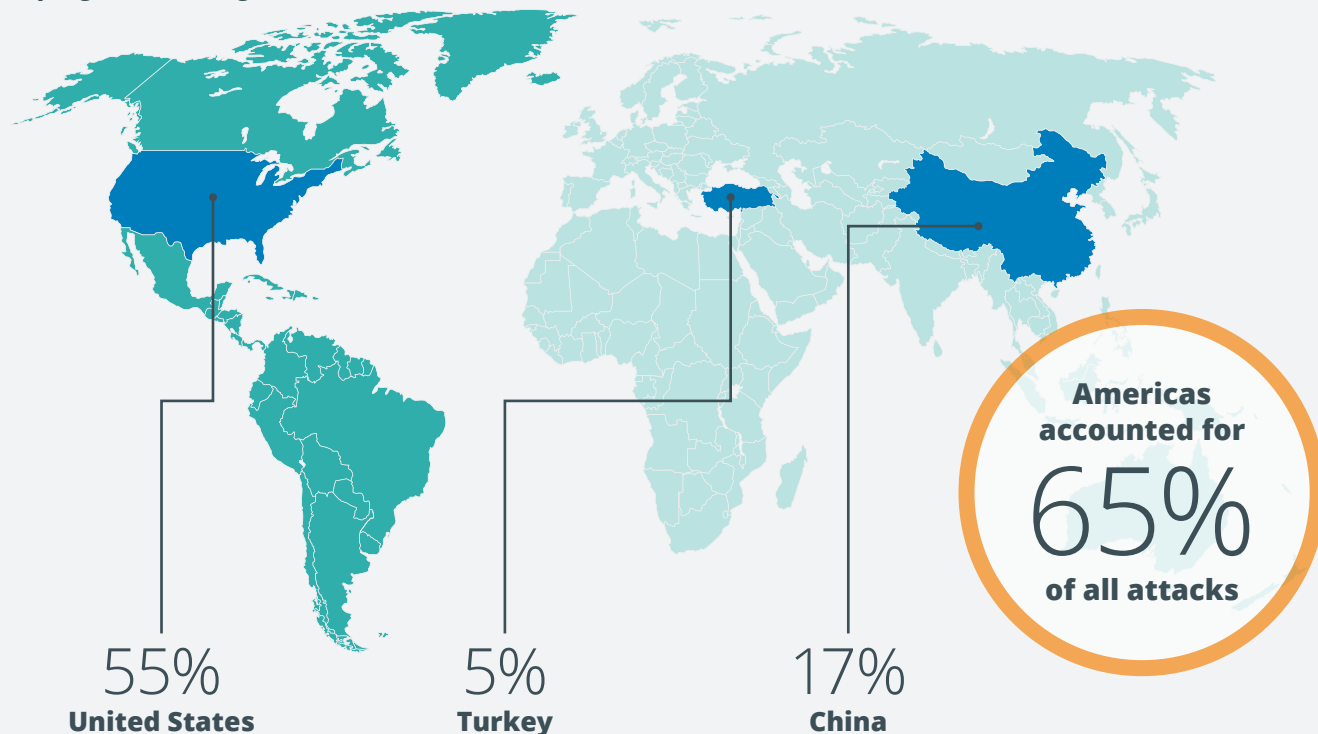
Data breaches continued to take center stage on the evening news. Although organizations are working hard to make their environments more secure and protect their clients' data, the adversary still has the upper hand with time and motivation to persist.

Effective internal communications are one of the most significant challenges NTT Security sees in our large clients. We continue to see breakdowns in communications between IT, business, and security teams. Blind spots may also contribute to security threats in project scope (too big, too small, or not involving security soon enough), misunderstandings of compliance requirements, or missed opportunities to be prepared for a rapid change in business direction.

Nation-state attacks are attacks conducted by or at the behest of a foreign government. Nation-state attacks are usually motivated, skilled, and well financed. As such, these attacks were a key focus of the media in 2016. There was no shortage of reports of tampering of the 2016 US presidential elections.



Top regions attacking the Americas



Top targeted sectors:

1	Manufacturing (23%)
2	Education (20%)
3	Finance (15%)

Top malware types from Americas:

1	Virus/Worm (50%)
2	Spyware/Keylogger (26%)
3	Trojan/Dropper (17%)

Top attack sources from Americas:

1	US (63%)
2	Canada (1%)
3	Brazil (1%)

Although many people point the finger at foreign countries for conducting nation-state attacks, there is also a need to realize the rest of the world is not sitting idle, and many other countries have invested in a strong presence on the cyber battlefield.

IoT and OT technology are advancing at an explosive rate. There is much discussion today about the complexity of managing security for these types of technologies. NTT Security believes this newer breed of technology will taunt security practitioners for many years to come.

While IoT challenges loom, the Americas have received a significant amount of attention from Business Email Compromise (BEC) attacks; sometimes called CEO fraud. BEC attacks were the second most common type of phishing attack which NTT Security supported with incident response engagements both globally, and in the Americas specifically. The challenges of BEC attacks are discussed in the next section.

Business Challenge: Business Email Compromise/CEO Fraud

Imagine you're sitting at your desk when you receive an email similar to the one below, and this email is from your organization's CEO. He needs you to take care of something today. It's a task you routinely perform, so you when you receive the information from him you make sure it's done within the hour. Unfortunately, this email wasn't really from your CEO. It was from an attacker impersonating your CEO to deceive you into doing what the attacker wants—in this example, transferring a large sum of money to the attacker. This type of attack is known as business email compromise (BEC) or CEO fraud.

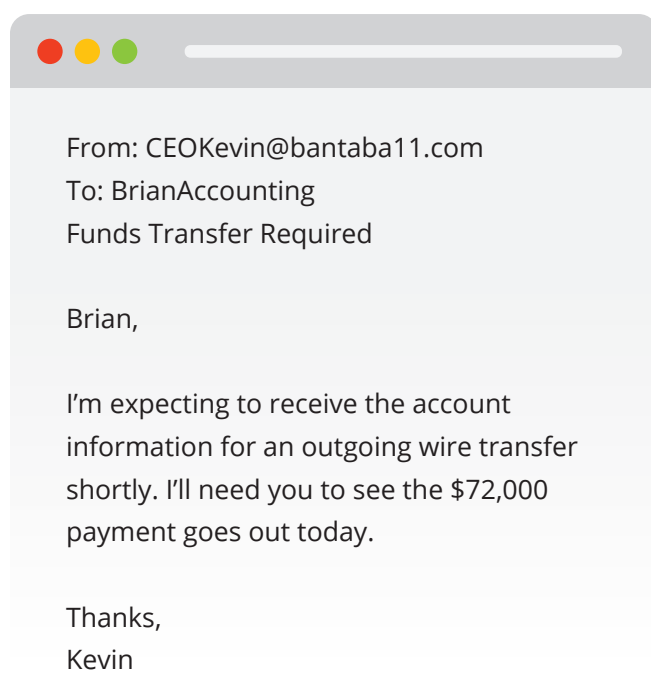


Figure 3: Sample BEC Email

How Can This Affect You and Your Organization?

BEC attacks are a form of phishing, targeting a particular person within an organization. The most common form of BEC attack is the attacker posing as an organization executive, directing an authorized employee, like a specific person in accounting or finance, to perform a wire transfer to an account owned by the attacker. NTT Security has also observed attackers emailing people in human resources to obtain access to employees' tax withholding forms. The goal of BEC attacks is to steal money, either by getting it directly from the organization or by using employees' personal information to commit identity theft.

BEC attacks are directed at just about every organization, regardless of its size, sector, or geographic region. These attacks have become so common law enforcement agencies around the world have issued warnings in the past two years about their impact on business. Phishing attacks accounted for over 60 percent of all NTT Security incident response engagements in 2016, and BEC attacks are the second most common form of phishing attacks, behind serving as the delivery mechanism for ransomware. However, even though the news is full of stories about ransomware, BEC attacks are typically much more financially damaging to companies. The average cost of a ransomware incident is only \$700 USD, while the average BEC incident involves a loss of about \$67,000 USD. NTT Security has performed several incident response engagements where the loss due to BEC was in excess of \$100,000.

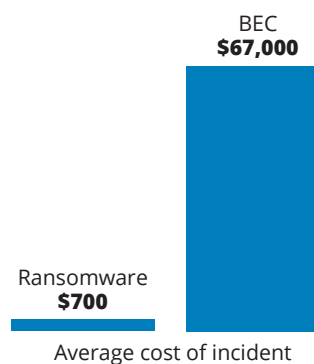


Figure 4: Ransomware vs. BEC Cost

If a BEC attack involving a wire transfer or other transfer of funds succeeds, chances are the funds will be moved elsewhere quickly and become unrecoverable before anyone at the organization realizes what has happened. An organization which acts immediately might be able to recover some of the transferred money, but in most cases attempts to recover any distributed funds will prove unsuccessful. The attacker has the desired funds in an account he controls, ready for immediate use. As a result, the attacker can effectively steal cash.

If a variant of a BEC attack succeeds in acquiring copies of tax withholding forms or other personnel records, there is not much the organization can do other than offer credit monitoring services to its employees. The information has been routed outside the organization and is freely available to the attackers to use to commit identity theft. Attackers may also choose to sell the personal information. Some of this information may have value for years in the underground, so identity theft may occur long after the BEC attack.

To make matters worse, if a BEC attack succeeds and the organization does not address it quickly, the attacker may contact the targeted individual again to ask for additional wire transfers, employee tax withholding forms, etc. This could turn a

single incident into a series of compromises, seriously damaging the organization's financial status and reputation.

Ultimately a BEC attack is low risk and high return for attackers. An attacker can acquire millions in stolen funds with relatively little effort. Every indication is that attackers will increasingly use BEC attacks to steal cash from any type of organization.



Figure 5: BEC Attack Flow

How Does This Happen?

What makes BEC attacks so successful is they are based on tricking employees into what amounts to "doing their job." The emails do not ask for anything out of the ordinary. The person who receives the BEC email, for instance, is the person who would perform wire transfers as part of their normal duties. The attacker figures that out before sending the first email. The attacker usually identifies the person to target through social media, as well as who in the management chain would be making requests of that person.

Based on this research, the attacker crafts an email which appears to be from the CEO or other executive, asking the targeted person to transfer the funds. Over 90 percent of the time, the email includes a fake "history" involving a series of emails between the executive and other members of the organization, such as legal counsel and contracting staff. The email may also include an official-looking document or PDF as a file attachment. This complex email is likely to appear legitimate to the recipient.

While BEC emails come in several different forms, NTT Security has most often observed them taking advantage of copycat domain names, which resemble the victim organization's domain name. If, for instance, the organization's domain was bantaball.com, the attacker could register the copycat domain of "bantaba11.com" by substituting ones for the L's. The attacker can then email the targeted person from the copycat domain, expecting the subtle change in domain name to go unnoticed.

Figure 5 illustrates the flow of a BEC attack using a copycat domain. If the target replies to the "hook" email from the attacker, the attacker has tricked the target and can now direct the target to do wire transfers to accounts of the attacker's choosing.

When BEC attacks first became popular, funds were most often transferred to a bank in China or another Asian country, but this is no longer the case. Funds are now regularly transferred to local banks, where professional money mules move the money elsewhere. This makes it extremely difficult to recover the money.

What Can You Do About This?



Everyone:

1. Avoid posting excessive information to social media about your job responsibilities, the names of your managers, teammates, and employees, etc. An attacker could harvest this information and use it against you or your coworkers to conduct a BEC attack.

2. Before fulfilling any sensitive requests in emails, look for signs of a BEC attack, such as the use of a copycat domain name or email content which is not expected for the sender.
3. Immediately communicate with security management and coworkers if you detect an attempted BEC attack.



Management:

1. Require out-of-band verification of sensitive requests made by email, such as wire transfers. For example, require employees receiving wire transfer requests to confirm them by phone calls or face-to-face interaction with the requesters. This may include verifying all transactions over a specific dollar amount or having two people approve each high-dollar transaction request.
2. Minimize the number of people authorized to process sensitive requests made by email.
3. Require regular security awareness training for all staff who have responsibilities which could be exploited by BEC attacks, such as fulfilling wire transfer requests and providing information on personnel. Make sure this training specifically includes BEC training for such staff.



Technical Staff:

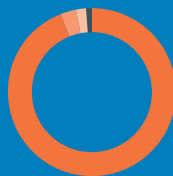
1. Identify and register domains which are copycats of your organization's domain. Your organization can usually register copycat domains for very little cost. This can make it harder for an attacker to identify an available copycat domain from which they can send their fake emails. A copycat domain name with several changes from the original domain's spelling can be much easier for BEC attack targets to spot.
2. Implement brand or reputation monitoring services which leverage threat intelligence to identify copycat domains used for fraudulent activities before they become active threats.
3. Enable spoof protection on your organization's email servers. Spoof protection will allow your organization to block invalid emails sent to your organization from external systems, another technique used to attempt to trick users. For example, your organization should not receive email from the internet which uses your organization's domain name in the "from" address. Such an email is an attempt to fake, or spoof, the source of the email, since the server should only see email using your organization's domain name leaving the organization's network.

Phishing schemes such as BEC are growing increasingly sophisticated, as cybercriminals use new tools and tactics to create authentic-looking emails and other forms of communication which use deception at their core. The impact is often severe, with initial scams resulting in wire transfers in the hundreds of thousands of dollars. Protecting against these attacks requires enterprises to address not only the technical tools, but supporting processes, and corporate culture to ensure employees can determine if a communication is authentic.

Matthew Gyde, Group Executive – Security, Dimension Data

4. Tightly restrict any remote access that could be used to perform wire transfers and other large transfers of money. Closely audit all such activity, and immediately investigate anything unusual.
5. Require sensitive requests made by email to be digitally signed by the sender, and require the recipient to verify those digital signatures. Any requests failing verification should be halted and immediately reported to security.

Focus On Asia



Top services used in attacks against Asia

- Remote administration (94%)
- File shares (3%)
- Databases (2%)
- Other (1%)



Top attack categories from Asia

- Malware (29%)
- DoS/DDoS (16%)
- Web application attack (6%)
- Other (49%)



Top attack categories targeting Asia

- Malware (12%)
- Service specific (11%)
- Website application attack (5%)
- Other (72%)



Information security is everybody's problem – make it culturally part of the way you run your business. Put dependable people in roles accountable for cybersecurity programs and ensure the people are good leaders. After all, people buy into the leader before they buy into the vision. Incorporate information security mantra into all aspects of your organization like you would any business process. Seek automation for cybersecurity activities, but be aware not to let governance rule innovation and progress.

Successful business in the post-information age needs to be agile, collaborative, and responsive to market changes, and building a level of resilience into all facets of the business is critical.

Martin Schlatter, CIO and Regional CEO, APAC, NTT Security

2016 at a Glance

In 2016, phishing was still by far the number one initial attack vector used to solicit information for future malicious activity. Asia saw much more interest in anti-phishing campaigns and security awareness initiatives in general. Malware targeting the end user device and client side applications via phishing campaigns or drive-by internet attacks were some of the biggest security threats impacting NTT Security customers.

Effective patch management remains a challenge for many clients. With 21 percent of exposed vulnerabilities more than three years old and 12 percent more than five years old, exploitation is elementary for an experienced hacker and automated for the cybercriminal. An effective vulnerability management program with a coordinated patch management program would increase the difficulty of exploitation for such low-hanging fruit.

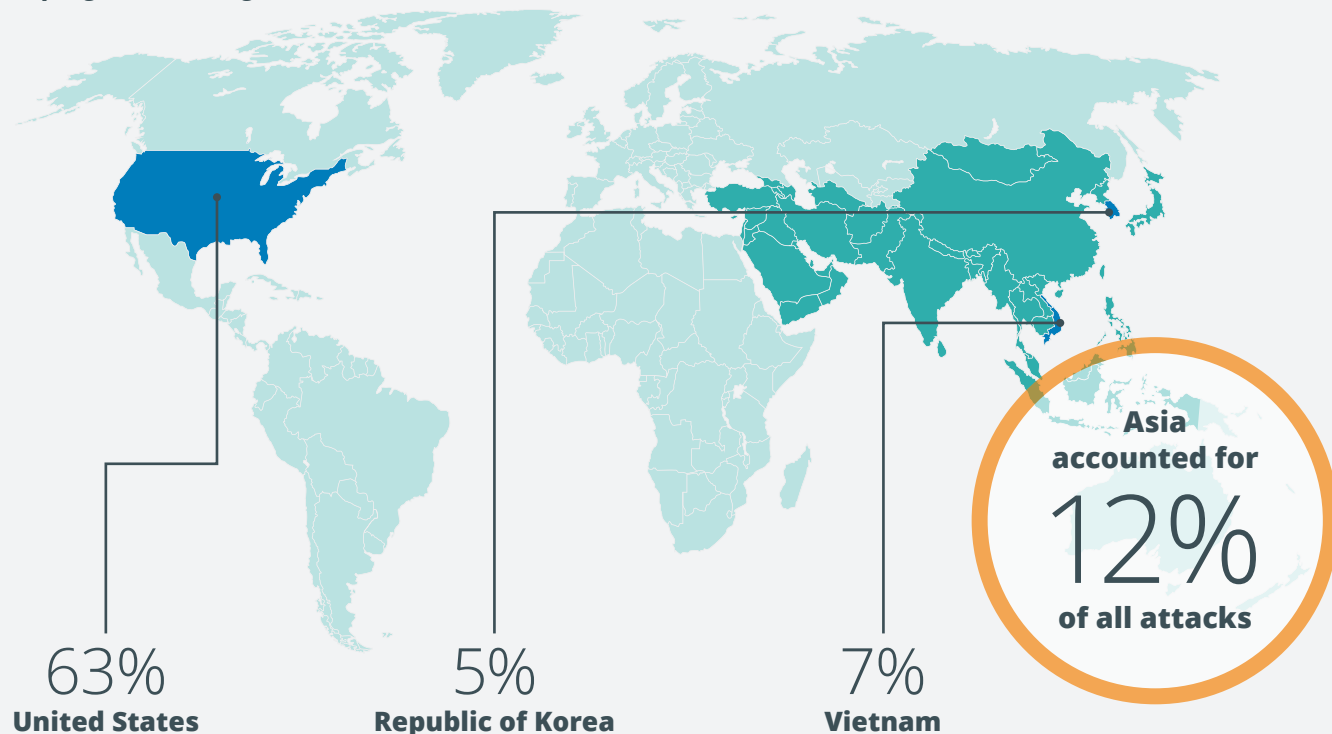
NTT Security saw increases in technology budgets again in 2016, up from 2015. Telecommunications companies again invested more funds into niche security companies in 2016. There is a definite cyclic trend through various cybersecurity disciplines as organizations battle to define what's right for them.

Organizations that assigned a dedicated cybersecurity budget rather than incorporating security into the IT budget tended to have a more mature understanding of the threat landscape and had a CISO as an equal stakeholder of the C-Level staff, rather than reporting to the CIO.

Clients continued to struggle with relentless targeted reconnaissance and the post-attack challenge of timely incident response (IR), as well as accurate diagnosis of the effects of an attack. It was less about the requisite controls and more about prevention, and what the fallout would be if those controls failed. IR is high on the agenda, and clients seemed to be most



Top regions attacking Asia:



Top attack sources from Asia:

1	China (6%)
2	Turkey (2%)
3	India (1%)

Top malware types from Asia:

1	Virus/Worm (78%)
2	Trojan/Dropper (15%)
3	Spyware/Keylogger (5%)

concerned about how they would react if breached and if they have processes to deal with a breach. Additionally, clients spent time evaluating whether they have a mechanism to do any post incident review, attempting to determine if they could contain said breach. Overall, IR has become an important topic of discussion within many organizations.

The need for IR is not dependent on the type of attack. Asia was challenged with being a primary source and target of a variety of malware. However, one of the most telling observations when reviewing data related to Asia was the contribution to attacks related to the Internet of Things. 60 percent of NTT Security's detections of Mirai, the IoT botnet, showed source IP addresses in Asia. Challenges of IoT are discussed in the next section.

The term *Internet of Things (IoT)* is becoming widely used, but its meaning is not always clear. It refers to the billions of devices (things) other than standard computers, smartphones, and tablets that can use computer networks (the internet). Many people already have IoT devices in their homes, such as routers, DVRs, thermostats, video cameras, security systems, coffeemakers, refrigerators, and voice-activated assistants (e.g., Amazon Echo). IoT devices also include wearables such as smartwatches, fitness bands, and medical devices. Even many cars have become IoT devices.

In addition to all these consumer uses, organizations are increasingly deploying IoT-like devices called *operational technology (OT)* to improve their operations. Many of these devices are sensors used to monitor people, processes, or objects. For example, building sensors can collect information on temperature and other environmental conditions, reporting measurements in real time so any deviations from acceptable bounds generate alerts. This could lead to faster detection of fires, floods, heating or cooling failures, and other adverse conditions. Other sensors are invaluable for improving manufacturing processes by providing highly detailed performance information so problems can be addressed much more quickly.

The number of ways in which IoT devices can help people and organizations is boundless. Unfortunately, IoT devices are susceptible to many of the same types of attacks which affect standard IT devices. This was confirmed around the world in September 2016, when attackers used the Mirai botnet to harness hundreds of thousands of compromised IoT devices from consumer and corporate environments to disrupt the operations of other devices and networks. These massive attacks are known as *distributed denial of service (DDoS)* attacks.

By 2020, the number of connected devices will grow from the current 7 billion to more than 20 billion devices. This convergence of IT and non-IT devices will lead to enormous amounts of vulnerabilities to manage.

Khirodra Mishra, Managing Director,
Security Services, NTT Data Services LLC

How Can This Affect You and Your Organization?

DDoS attacks using IoT devices can directly and indirectly endanger an organization in several ways, including:

- ▶ Attacks can prevent customers, partners, and others from accessing your organization's internet-facing resources, impacting sales and other daily operations.
- ▶ Attacks can prevent employees and internal systems from accessing the internet, seriously disrupting many facets of operations.
- ▶ Attacks may knock one or more organizations off the internet which provide services to your organization, causing your organization's supply chain to be broken.
- ▶ Attacks can damage your organization's reputation, and potentially result in blacklisting some or all of your organization's internet presence by having compromised IoT and OT devices within your organization participate in DDoS attacks against other organizations.

But while DDoS attacks via IoT devices may be the most recognized, they are not the only threats. Cybercriminals can use IoT and OT devices for other nefarious purposes including:

- ▶ Attackers may access IoT cameras and other devices to spy on people.
- ▶ Attackers may access IoT and OT devices to obtain personal information.
- ▶ Attackers may manipulate OT devices to cause damage. One example is turning off temperature monitoring for a server rack, and turning up the data center thermostat, which could result in undetected failure of devices due to extreme heat.
- ▶ Attackers may compromise IoT or OT devices to serve as a launch point for other internal and external attacks.

How Does This Happen?

Let's first look at how the IoT devices are compromised, then how the compromised devices are used together to perform DDoS attacks.

IoT devices include many potential security weaknesses attackers can exploit to compromise the devices. In the worst cases, an

While DDoS attacks are the most recognized threat, they are not the only potential outcome of your organization's IoT and OT devices being compromised. Attackers can directly harm your organization by breaching the confidentiality, integrity, or availability of one or more of your IoT and OT devices. The potential outcomes include anything from feeding false data into a building generator to cause it to malfunction and perhaps catch fire, to taking control of a vehicle and causing a serious accident. An IoT or OT device breach could even be the starting point of a much larger attack against your organization.

IoT device doesn't have basic security features or the security features aren't being used, which makes it extremely susceptible to compromise. In other cases, security features are being used but they're not set up correctly. For example, an IoT device may require a person to provide a password before accessing it, but the user never changed the device's password from the default value. Anyone who knows the default password can access the device.

Other potential security issues with IoT devices include the following:

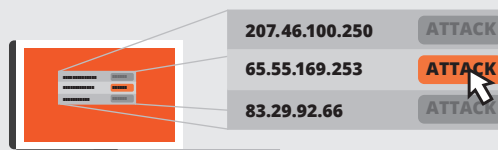
- ▶ A device might be missing patches to fix security issues.
- ▶ A device's vendor might have gone out of business or stopped supporting the device, which means patches are no longer available to fix security issues.
- ▶ A device might not use encryption to protect its network communications from eavesdropping.
- ▶ A Wi-Fi network used by a device might not be secured properly, allowing attackers within the network's range to eavesdrop on the device's Wi-Fi communications.

These security issues are nothing new. They've been present in standard IT devices over the years, and some are still found in many legacy IT deployments. To a large extent, many IoT devices

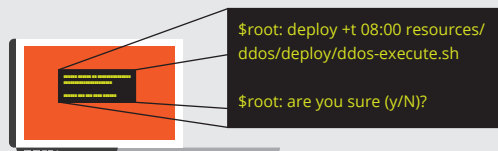
Once an attacker has compromised an IoT or OT device, he can prepare it to participate in DDoS attacks. There are three basic steps to this:



- 1 The attacker installs malware** and tools on the device, usually through an automated process requiring little or no effort by the attacker. The malware and tools give the attacker remote control over the device, and they join the device to a global group of compromised devices called a botnet.



- 2 When the attacker wants to prepare a DDoS attack, he selects a target and a type of DDoS attack to launch against the target.** In the past year, NTT Security has observed over 10 categories of DDoS attacks in use, with some categories being more effective in particular situations.



- 3 The attacker sends a single command** to direct the devices to perform the DDoS attack at the desired time.

are decades behind modern IT devices in terms of security capabilities, and the limited security features available are often difficult or nearly impossible for non-experts to use.

Business Challenge: The Internet of Things and Distributed Denial of Service Attacks

For a six-month period in 2016, NTT Security used honeypots to closely monitor and analyze IoT based attacks. The results of analyzing what the attacks were targeting, based on the credentials they were using, are as follows:

- ▶ 66 percent were looking for specific IoT devices, such as a particular model of video camera.
- ▶ Three percent were seeking a web server or other type of server.
- ▶ Two percent were trying to attack a database.
- ▶ The remaining 29 percent covered a variety of other targets.

Based on NTT Security analysis of honeypot traffic, the 66 percent of attacks targeting IoT devices appeared to be from compromised IoT devices attempting to find and compromise more such devices. This would be consistent with an attacker acquiring a large number of devices to use in DDoS and other forms of attack. As for the other 34 percent of the analyzed attacks, it is likely these are also attempting to grow the attacker's arsenal by targeting other types of devices. There is nothing about a DDoS attack which requires use of IoT devices only, so attackers may look for as many devices as possible regardless of type.

Another part of NTT Security's analysis of the honeypot data was to look at the passwords used by attacks trying to authenticate to the honeypot. The honeypot recorded over 20,000 unique passwords, but a small subset of those passwords was used over and over. The following 25 passwords used most often comprised almost 33 percent of all authentication attempts. NTT Security analysts compared the passwords from these authentication

<none>	root	raspberrypi	changeme	qwe123
!@	1234	12345	oracle	1234567890
123456	support	user	default	nagios
password	ubnt	123	guest	postgres
admin	test	qwerty	123qwe	1

attempts with two well-known lists of passwords. One is a list of passwords most commonly used by people during 2016.² The other list is the passwords used by compromised devices in the Mirai botnet, which was the botnet used to perform many high-profile IoT related DDoS attacks during 2016.²

The results of the password comparisons were illuminating. Only 10 percent of authentication attempts used a password from the list of most commonly used passwords. But an overwhelming 76 percent of the authentication attempts included a password implemented by the Mirai botnet. This indicates a large percentage of the attacks against the honeypot most likely came from the Mirai botnet and other automated attack sources. NTT Security also looked at the geographic source of each IoT-based attack. As Figure 6 shows, 60 percent of all IoT attacks came from IP addresses within Asia, with 21 percent from EMEA and another 19 percent from the Americas. The most likely reason for the high volume of attacks coming from devices in Asia is that the products in Asian markets have historically been shown to be vulnerable to compromise and subsequent reuse in attacks.

IoT/OT Attack Sources

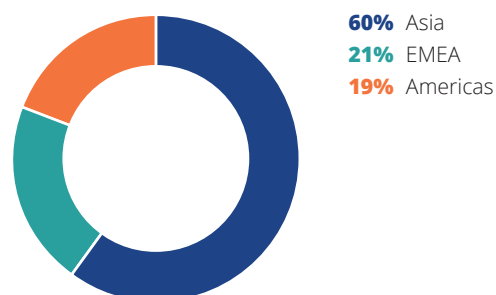


Figure 6: Geographic Sources of IoT and OT-Based Attacks

What Can You Do About This?

Here are some recommendations to reduce your organization's chances of having its IoT and OT devices used to perform DDoS attacks.

Everyone:

1. If a consumer IoT device doesn't need internet access, don't configure it to use the internet.
2. Keep all consumer IoT devices updated. Whenever possible, configure them to automatically download and install updates as soon as they are available.

² <https://blog.keepersecurity.com/2017/01/13/most-common-passwords-of-2016-research-study/>

3. Before putting it online, change the default password for all IoT devices to something only you know.
4. Choose strong passwords for accessing consumer IoT devices. Avoid passwords from the list of the most commonly used ones because attackers know to try those. It's also important to use a unique password for each IoT device—a password you don't use for anything else.
5. Take advantage of available security features in consumer IoT devices. Spend just a few minutes looking at the documentation for each of your devices to find the security options. Do what you can to use those options, and ask someone with more security expertise for help if necessary. This minor effort may save you many headaches in the future.



Management:

1. Make security a primary consideration for all IoT and OT device purchases. Favor devices with robust security capabilities built in. If none are available, look at traditional technologies that may be easier to secure.
2. Expand business continuity and incident response capabilities to include DDoS attacks. For business continuity, this should not only address DDoS attacks against the organization, but also DDoS attacks against suppliers.
3. Authorize funding as needed to replace older IoT and OT devices no longer supported by their vendors.



Technical Staff:

1. Extend existing patch management and software configuration management processes and technologies to include IoT and OT devices. Monitor the patches and configuration settings for the IoT and OT devices as often as possible (ideally continuously).
2. Manage all credentials for accessing IoT and OT devices, such as setting a complex unique password for each device, storing these passwords securely, and changing these passwords if a compromise is suspected.
3. Evaluate and use technologies for monitoring IoT and OT device security and detecting attacks involving IoT and OT devices.
4. Evaluate and use technologies for stopping DDoS traffic (both inbound and outbound).

Focus On **Australia**



Top targeted sectors

- Finance (34%)
- Retail (27%)
- Business and professional services (20%)
- Other (19%)



Top attack categories from Australia

- DoS/DDoS (23%)
- Service specific (19%)
- Website application attacks (19%)
- Other (39%)



Top attack categories targeting Australia

- Service specific (23%)
- DoS/DDoS (22%)
- Website application attacks (20%)
- Other (35%)



Our world is more connected than ever before. With the explosion of the Internet of Things (IoT), new threats will continue to emerge as the market continues its 'race to the bottom', leading to many unsecure devices connected to the internet. IoT access allows users remote access to monitoring a wide range of everyday devices and according to a United Nations report, the number of devices connected to the internet will outnumber the people on earth by 6 to 1 in the year 2020. With a never-ending number of endpoints connected to the internet, our adversaries continue to maintain an advantage because they have an abundant supply of targets. Advanced technology, socioeconomic factors, a constant shifting of consumer attitudes, data protection and legal matters will all play key roles in the ever-changing cyber threat landscape, as businesses continue to expand in this hyper-connected world.

Jordan Del-Grande, Regional CISO, APAC, NTT Security

2016 at a Glance

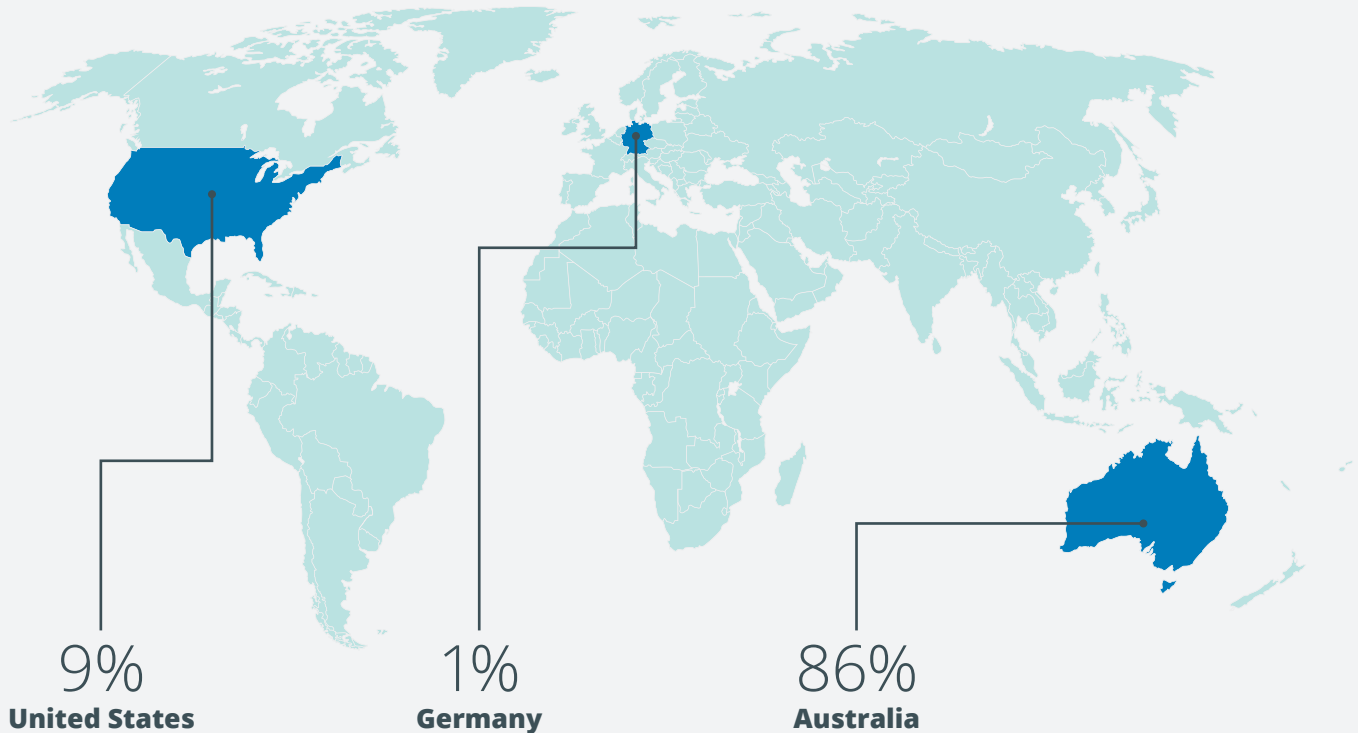
The Notifiable Data Breach Bill was passed by the Australian Federal Parliament in February 2017. The bill will be a mandatory data breach notification law when it becomes an Act, which applies to government agencies and organizations which already must comply with the Privacy Act. Under the bill, organizations that determine they have been breached or have lost data will need to report the incident, and notify customers directly impacted or "at risk." Those who fail to report the incident face a range of penalties, including fines of \$360,000 AUD for individuals and \$1.8 million AUD for organizations.

With legislative penalties in place that not only impact an organization's bottom line, but also the potential to damage the brand, there will likely be more focus and investment on information security in both the public and private sectors. NTT Security expects to see similar legislature across the Asia Pac region in the near future.

The 2016 Cyber Security Strategy published in Australia indicates five key focus areas for its security plan. These areas include a national cyber partnership, strong cyber defenses, global responsibility and influence, growth and innovation, and a cyber smart nation. The report also outlines that the Australian government's investment in achieving this progress is going to



Top regions attacking Australia:



Top services used in attacks against Australia:

1	Remote administration (43%)
2	File shares (40%)
3	Internet phone (VOIP) (7%)

Top malware types from Australia:

1	Trojan/Dropper (93%)
2	Fakeware/dialers (2%)

be approximately \$230 million AUD over the next four years. This all creates an increased focus on legislation, the related attention to breach details, and the role of the end user in their contribution to threats from IoT devices. To successfully navigate these challenges, organizations are going to be required to rely on their users more than ever. Challenges of threats against users are discussed in the next section.

A large number of successful attacks against organizations, everything from ransomware infections to data breaches, start with a compromise of a regular user's desktop or laptop computer. The operating system, applications, and tools make up each user's end user technology. This includes things like the Apple operating system, Microsoft Internet Explorer, and Adobe Reader plug in, along with a variety of others. Many of these attacks come from toolkits known as exploit kits. An exploit kit provides a packaged environment for an attacker to select vulnerabilities, set up websites for distributing malware targeting those vulnerabilities, and manage the malware once it has infected users' computers. What makes exploit kits so dangerous is they're specifically designed to be easy to use, so security expertise is not necessarily required to use and profit from them. More experienced attackers create these exploit kits and sell or rent them.

Exploit kits usually target software which is widely used on desktop and laptop computers and is accessible through a web browser. Examples include Adobe Flash Player, Adobe Reader, Java, JavaScript, Microsoft Internet Explorer, and Microsoft Silverlight. Of the 6.2 billion attacks detected and defended against by NTT Security during the past year, nearly 30 percent targeted these types of end-user products.

How Can This Affect You and Your Organization?

Exploit kit-generated attacks against end user technology can affect you and your organization in several ways. Here are just a few examples:

- ▶ **An attack could compromise your personal desktop or laptop computer.** The attacker could access any information on your computer, from your personal financial and health records to your passwords, to be used to commit identity theft or to be sold to other criminals. If you telecommute from that computer, the attacker could also steal your corporate passwords and install malware to monitor you for months or years to come. He could use your remote access sessions to sneak into your organization's networks and systems and perform a much larger attack.
- ▶ **An attack could target the information on your corporate desktop or laptop computer.** The attacker could steal sensitive information stored on your computer or accessed from your computer. This could constitute a major data breach that costs your organization millions.

The idea that humans are the “weakest link” in security is very popular among security professionals. Of course, it's completely true that many security incidents involve human users making bad decisions, but these sorts of mistakes are evidence that business and technology are failing human users, not the other way around. It is important that we maximise employees' ability to do their jobs safely and efficiently by ensuring that proper training and tools are provided.

Matthew Gyde, Group Executive – Security, Dimension Data

-
- ▶ **An attack could infect your corporate computer with malware.** Malware could enable a remote connection for an attacker, or could allow an attacker to join your computer to a global botnet to participate in attacks against other organizations. Malware could come in the form of ransomware which encrypts the contents of your computer. Malware could also give the attacker a foot in the door to travel throughout your organization's networks and systems to reach more valuable targets.

It is important to understand that a single exploit kit-generated attack against your personal or corporate computer could be the launching point for a much larger attack against your organization, potentially costing your organization millions of dollars.

To better understand how this happens, let's walk through the steps of the attack after the attacker has selected their exploit kit of choice and their target. At this point, the attacker is ready to spread the malware.



1 The attacker needs users to connect their computers to the attacker's malware distribution website. This website may be a benign one the attacker has compromised, or it may be a website owned by the attacker or the exploit kit's creator. The attacker lures victims to the website through any of several methods, including redirecting users from a benign site to the malicious site or sending phishing emails to users. Attackers also make extensive use of malvertising, where a user is shown fake ads which redirect the user to the attacker's exploit kit, instead of connecting to a genuine advertising sponsor.

2 Exploit kits can perform a variety of functions depending on the specific kit and the characteristics of the computer visiting the website. Exploit kits often determine products and version numbers of the visiting computer's browser and operating system, as well as other characteristics, a process referred to as "fingerprinting." The exploit kit then delivers an exploit to take advantage of the identified vulnerabilities. This process normally results in the delivery of malware which is effective on the visiting computer.



3 If successful, the attacker has infected the computer with malware, potentially granting full remote control over the computer. The exploit kit delivers ransomware, keystroke loggers and banking Trojans (among others) to help provide the attacker with additional credentials or access which they can use to extend their reach within the targeted organization.

How Does This Happen?

At any given time, there are multiple exploit kits being widely used by attackers. While many exploit kits target similar vulnerabilities, some kits also target a somewhat different set of vulnerabilities, so the risk to your computer and your organization increases as kits become more diverse. Unfortunately, exploit kits are generally well maintained, adding the ability to exploit the latest vulnerabilities as soon as those vulnerabilities become publicly known, and in some cases even before they are made public (including zero-day vulnerabilities). An exploit kit with the latest vulnerabilities is likely to be more popular, which increases revenue for its developer, so there is a big incentive to keep kits up to date.

Throughout the past year, NTT Security monitored exploit kit usage. Figure 7 shows the trends in this usage for the five most widely used kits: Angler, Magnitude, Neutrino, RIG, and Sundown. Angler was by far the most popular, with 72 percent of all usage, but in June the Angler kit suddenly became unavailable, reportedly after the arrests of a well-known Russian hacking gang. People who had downloaded Angler and the malware

already created by it were still able to use it, which explains the volume from July on. After Angler's withdrawal, Neutrino became more widely used for a few months until its owners shut it down. Since then, there has been a steady rise in the popularity of the RIG exploit kit.

Across all kits, the total volume of usage steadily dropped throughout the year, as shown in Figure 7. It appears that as exploit kits became less readily available, attacker interest in them also declined. However, this trend could easily reverse itself as another exploit kit gains popularity, providing more funding so it can add more features, causing it to gain even more in popularity. NTT Security detected a marked increase in the use of the RIG exploit kit into the fourth quarter of 2016 but exploit kit detections never reached the levels of earlier in the year, with only 13 percent of the year's exploit kit activity being detected in the third quarter of 2016.

In the past year, Adobe Flash Player, Microsoft Internet Explorer, and Microsoft Silverlight were targeted the most often. However, this does not mean other software is not being targeted. Attackers tend to focus on the software which is most widely used and

Total Exploit Kit Detections by Quarter

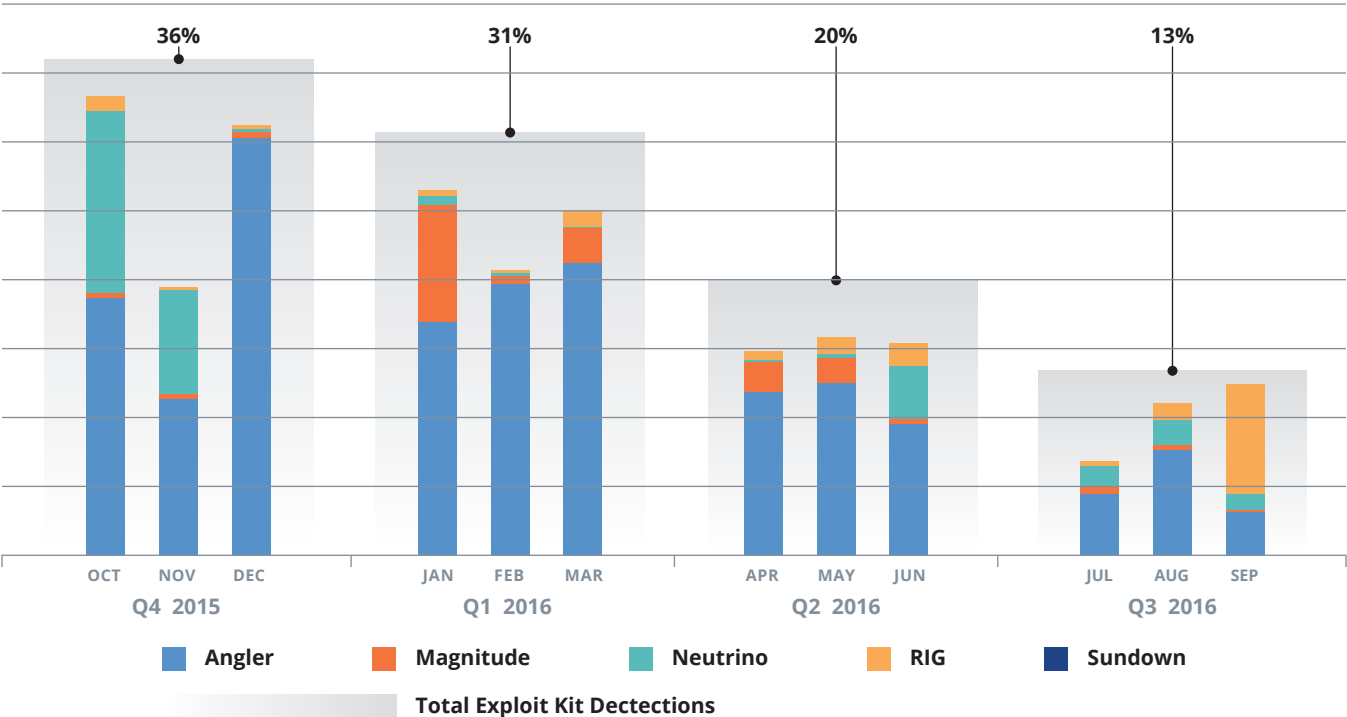


Figure 7: Observed Exploit Kit Usage by Month

Business Challenge: Attacks Against End User Technology



associated with the largest number of new vulnerabilities. As software popularity shifts and the number of vulnerabilities changes, so too will the targets of future exploit kits.

What Can You Do About This?

NTT Security provides the following recommendations to reduce your organization's chances of being victimized by attacks against end user technology. Note that these recommendations are in addition to all the recommendations in the Phishing, Social Engineering, and Ransomware section.



Everyone:

1. Whenever you get a notification from your desktop or laptop computer about downloading and installing patches, comply with it as soon as you can. Ensure it originates from a valid source, otherwise you may be installing malware.
2. Don't use the same passwords for your personal and corporate accounts. Attackers know many people reuse passwords, so if they steal one of your passwords, they're likely to try it in many places you might have an account. You can avoid password reuse by adopting better ways to manage your passwords, such as the use of a password manager utility which securely stores all your passwords and retrieves them for you when you need them.
2. Maintain a current inventory of all desktop and laptop software that might be targeted through web browsers. Review this inventory regularly to identify software no longer on the current version so it can be upgraded before support ends and as security updates are distributed.
3. Evaluate ad blocker technology and consider deploying it to all desktops and laptops to minimize attacks through malicious advertising.
4. Subscribe to threat intelligence feeds for enterprise security controls (firewalls, intrusion prevention systems, security information and event management [SIEM] technologies, etc.) to identify and block exploit kit-associated websites more quickly.
5. Deploy endpoint security solutions to identify and contain never-before-seen malware threats through sandboxing or other advanced techniques.



Management:

1. Allocate sufficient funding so targeted software is upgraded on all desktops and laptops before support for the old (installed) version ends.
2. If any of the targeted software is not currently used for operations, consider uninstalling it throughout the organization and prohibiting its use.
3. If any of the targeted software is not necessary, consider shifting its functions to other software and eliminating the targeted software to the extent possible.



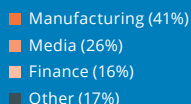
Technical Staff:

1. Develop robust patch management capabilities with heavy reliance on automation. Ensure patches for targeted software are evaluated, deployed, and installed on all affected desktops and laptops as quickly as feasible.

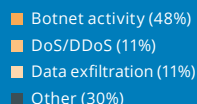
Focus On Japan



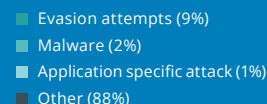
Top targeted sectors



Top attack categories from Japan



Top attack categories targeting Japan



Sophisticated attackers use all possible tools for hacking into Information and Communication Technology (ICT) environments to steal or destroy customers' critical data. In order to protect critical assets, organizations should consider not only making an effort to detect threats, but also responding to incidents immediately to isolate compromised hosts and eradicate threats in a matter of minutes.

Immature organizations tend to solely rely on so-called "highly advanced security appliances" which are expected to protect them from all targeted attacks, but such appliances are often only one piece of a true solution. Highly organized and well-funded attacker groups will always find ways to avoid any expensive protection such as anti-virus, sandbox and artificial intelligence (AI) supported protection technologies. Important points are to utilize available logs and events, and well trained human analysts with sophisticated SIEM solutions to detect previously unknown attacks and threats.

Kazunori Yozawa, CAO/CCO and Regional CEO, NTT Security

2016 at a Glance

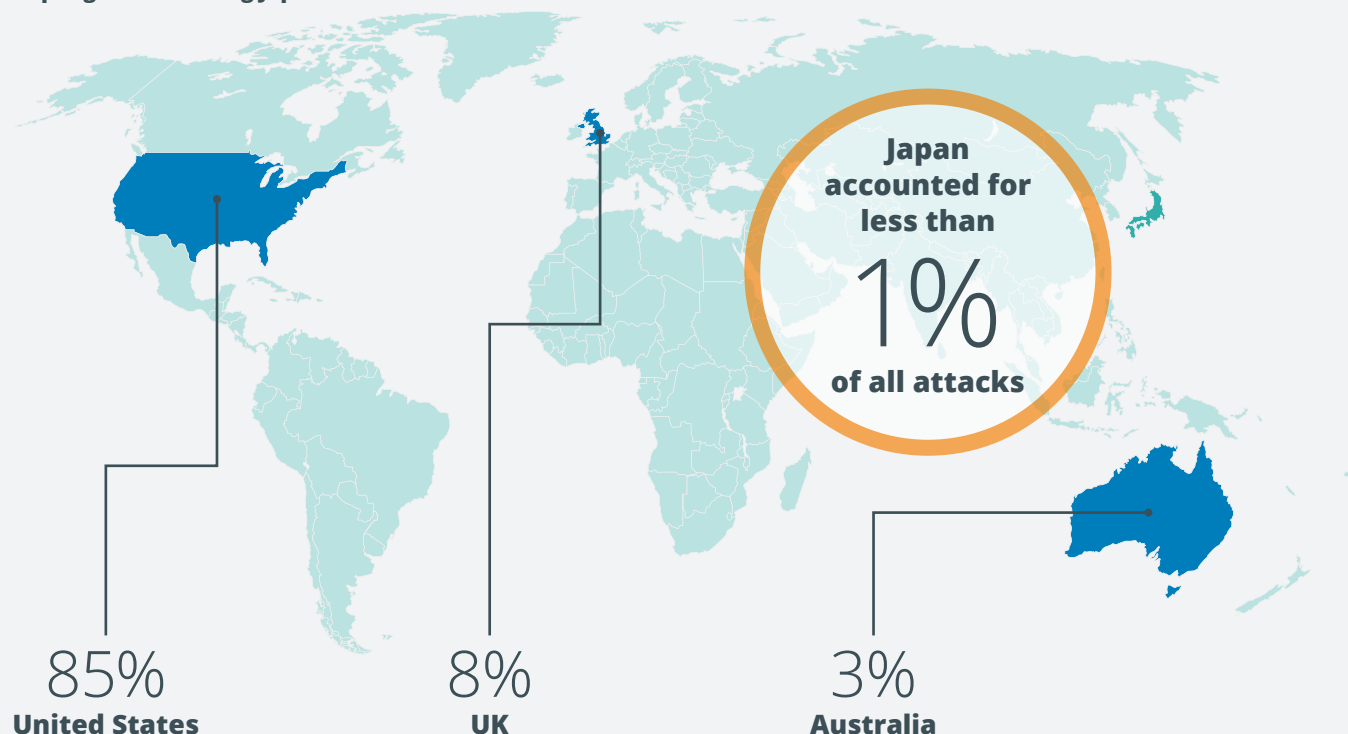
Japanese organizations observed targeted attacks with a deep understanding of Japanese social and business customs in 2016. NTT Security saw a wide range of spam and "drive-by-downloads"– attacks designed to load malware on the targeted device either without the user's knowledge, or with their unknowing consent. This might appear as a pop up which asks the user to update their Adobe Flash or some other plug in. Common exploit kits implemented such attacks to install a large amount of ransomware and banking malware in Japan last year. These attacks were observed specifically targeting Japanese organizations and produced numerous large scale incidents. NTT Security detected very specific malware throughout a series

of campaigns. Targeted attack emails initially employed the Locky Trojan, with primarily English-based payloads. These phishing email attacks became more sophisticated and evolved to using Ursnif, written in the Japanese language, attracting Japanese victims to open malicious emails and hostile attachments. As a result, Ursnif became the most observed malware, followed by Beblon, in successful compromises of ICT systems.

Hackivist activities were observed late in 2016 with a focus on distributed denial of service (DDoS) attacks on public servers within many industries aiming to criticize dolphin-hunting in Taiji, Wakayama Prefecture. The hacker collective Anonymous took credit for the attacks in an operation dubbed "Operation Killing Bay."



Top regions attacking Japan:



Top malware types from Japan:

1	Spyware/Keylogger (44%)
2	Trojan/Dropper (16%)

Percentage of critical incidents in Japan attributed to malware:

82%

The Japanese government's cyber security policy gathered attention following the amendment of the Cyber Security Basic Act and the Act on Promotion of Information Processing. This new amendment provides additional guidance and authority to government organizations to monitor security for special entities and also provides a new credential for "Information Processing Security Supporter," a designation for cyber professionals to consult with businesses for achieving greater cybersecurity.

NTT also participated in "Cross-sector Collaboration for Cybersecurity Workforce Development" consisting of more than 40 companies from major fields of infrastructure. They have

made contributions to define and find methods in producing qualified candidates needed for industries.

We expect that both monetary-motivated attacks and political terrorism threats will continue to expand and affect Japanese organizations in 2017. Japan will continue to face these evolving threats, and will be center stage when they host the 2020 Olympics. Such visibility was also placed on Japan when they hosted the G7 Summit in 2016. Challenges in managing a robust threat environment like the 2016 G7 Summit are discussed in the next section.

As a gold sponsor of the 2020 Olympics and Paralympics hosted in Tokyo, NTT-CERT (Computer Emergency Response Team), an internal security entity within NTT, will play a vital role in securing these games as a critical service provider with NTT Security. NTT-CERT and NTT Security will assist with analyzing potential threats, responding to major events, and sharing information amongst trusted partners to help secure the games together. NTT-CERT provided similar capabilities and functions during the 2016 G7 Summit.

Overview of Ise-Shima Summit

The G7 Summit is a top-level meeting in which the leaders of seven nations (Japan, United States, United Kingdom, France, Germany, Italy, and Canada), the President of the European Council, and the President of the European Commission participate. As the chair country for the 2016 G7 Summit, Japan held this event, with world leaders traveling to Ise-Shima, Mie.

NTT Group was responsible for the cybersecurity of this event as a critical infrastructure provider. The Summit, which included representatives from a variety of countries, presented interesting security challenges in order to meet business needs.

Leaders from around the world gather at the G7 Summit to discuss various political issues including the gaps between developed and developing countries, as well as global issues concerning the environment, energy, and trading. As a result, the Summit gathers attention from around the world. Security experts expected the Summit would be targeted by various interferences, such as terrorism, in both the physical world and the cyber world. While the G7 Summit took place in May 2016, 10 more ministerial meetings were held from April through September.

Cyber Threat Landscape in Japan

When it was determined that NTT would be providing cybersecurity for the G7 Summit, we analyzed previous attack trends to validate our analysis and develop our approach to securing the event. Based on our analysis, we identified the following four cybersecurity threats which shaped our view of protecting the Summit.

- ▶ An increase in the number of domestic targeted email attacks, including ransomware attacks and advanced persistent threats (APT) targeting the Japan Pension Service in May 2016, as well as attacks against the largest travel agency in Japan during our actual support period (May 2016)
- ▶ Hacktivist activity from a group criticizing dolphin hunting; since September 2015, hackers extended their attacks to Japan, progressing from a primary focus on the town of Taiji to DDoS attacks and website defacement, targeting websites of airports, newspaper publishers, and other industries
- ▶ Previous attacks invoked by unstable international relationships (e.g., DDoS attack from far east Asia)
- ▶ Risks to Wi-Fi networks; recent events had shown an uptick in attacks on the Wi-Fi networks of large-scale events, with attacks including communication interception, fraudulent usage, and fake Wi-Fi access points

G7 2016 Summit & Ministerial Meetings



Figure 8: 2016 G7 Summit

How We Prepared

Coordinated Structure

NTT coordinated group-wide measures to protect IT and network systems. NTT-CERT, which is an internal security entity within NTT, directly supported this activity by providing threat information in cooperation with internal and external partners.

Incident Handling Rehearsal

The participating companies within NTT were organized into a special unit for the G7 Summit. They rehearsed incident identification, escalation, and response to clearly identify tasks to maximize cooperation between participating companies, subsequently executing those tasks and evaluating internal unit incident handling procedures in a cohesive, unified manner.

During NTT-CERT's rehearsal and evaluation of cybersecurity measures, NTT-CERT developed scenarios of possible events the units would be confronted with during the G7 Summit.

NTT R&D also developed and implemented an integrated risk management system, which NTT used, both in rehearsal and during the Summit.

This rehearsal enabled NTT to collectively improve communication and coordination in support of the G7 Summit. Rehearsals, or dry runs, such as these were imperative to ensuring NTT's effective operations throughout the Summit.

Sharing Vulnerability Information

Effective security operation in network operations centers (NOCs) and security operations centers (SOCs) requires accurate vulnerability information, but a flood of vulnerability information makes analysis difficult. NTT-CERT collected and analyzed vulnerability information, subsequently disseminating intelligence regarding the vulnerabilities with the greatest potential negative impact. NTT-CERT's analysis resulted in the effective delivery of actionable intelligence and mitigation recommendations for many vulnerabilities during the G7 Summit.

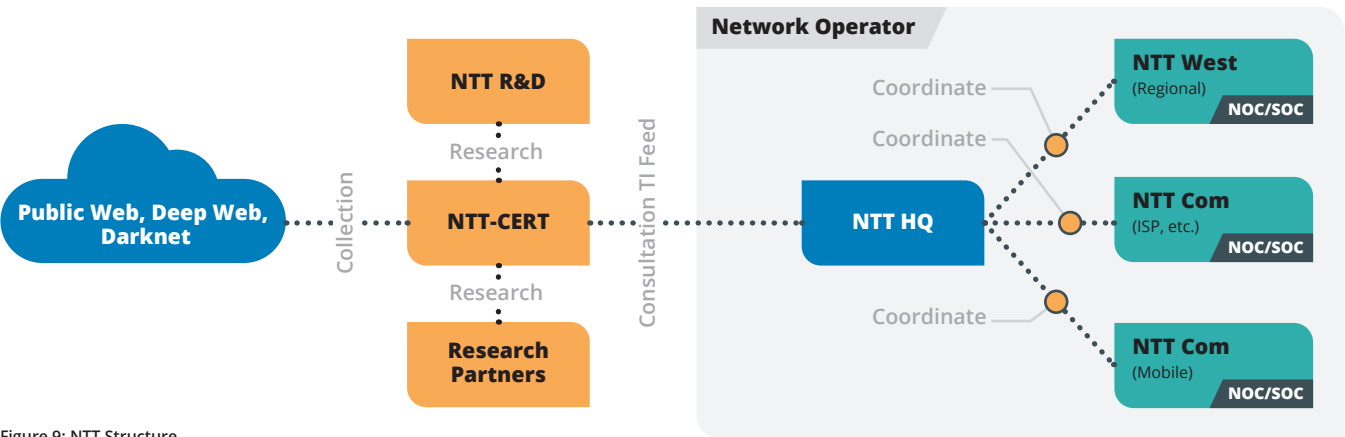


Figure 9: NTT Structure

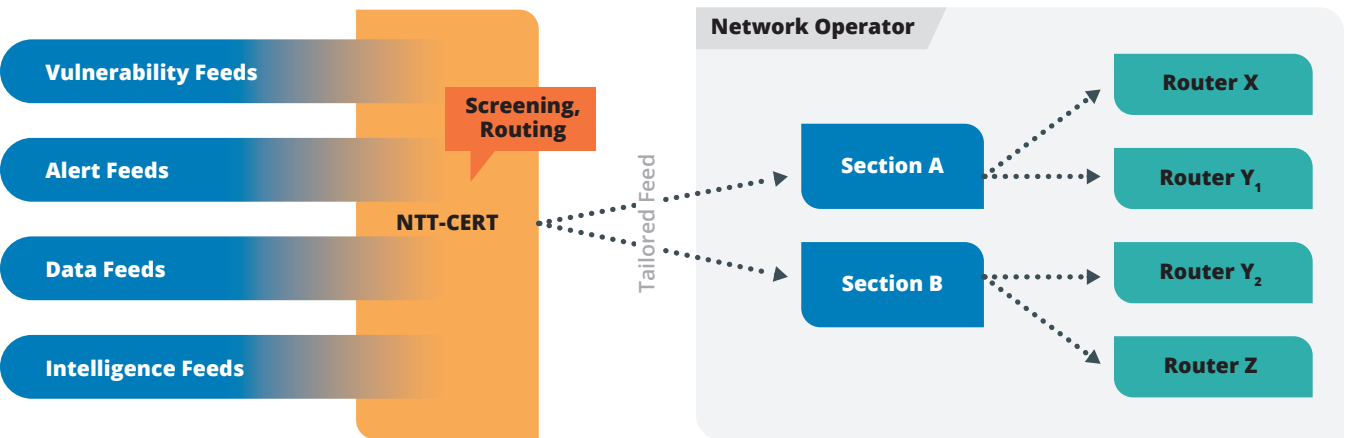


Figure 10: Collecting and Processing for Intelligence Management

Collecting and Analyzing Open Source and Dark/Deep Web Intelligence

NTT-CERT collects many forms of security-related vulnerability, exploit, and threat information. We acquire information by scouring open source intelligence providers and original sources, and by working closely with our research partners to crawl the dark/deep web, analyze and reverse engineer malware samples, identify APT attack cases, etc. Source examples are below:

- ▶ Public sources:
 - Twitter, forums, news sites, blogs
 - Collected and analyzed by NTT-CERT; languages include Japanese, English, Chinese and Korean
 - Native language forums of neighboring countries
 - Anonymous #Oplcarus attack against central banks
- ▶ Partners:
 - Dark webs, deep webs, malware samples, APT attack cases
 - Collected and investigated with research partners

NTT-CERT collected and analyzed the information, examining the data for relationships, in context of understanding the impact on the G7 Summit. Focusing on specific use cases allowed NTT-CERT to further develop findings into manageable and actionable intelligence. Curated intelligence was disseminated in targeted and general reports, including Tactics, Techniques, and Procedures (TTPs) as well as Indicators of Compromise (IOCs), which further assisted in the development of blacklists for threats targeting the G7 Summit as well as additional business requirements.

This entire process included formal analysis of the intelligence set to determine what would be the most useful for dissemination to NOCs or SOCs, as well as evaluation of the entire information gathering and intelligence development process.

By leveraging the vast network of NTT analysts and researchers, NTT-CERT discovered or handled:

- ▶ Specific G7 Summit-themed ransomware,
- ▶ A compromised Wi-Fi router at a hotel near the G7 Summit venue, and
- ▶ Numerous vulnerabilities with the potential to adversely impact G7 Summit cybersecurity.

Supporting Around the Clock Operations

In the most critical period around the G7 Summit, NTT-CERT performed as an intelligence unit by providing 24-hour support from a distributed environment, including regularly sharing information with NTT companies via telephone conference. NTT-CERT collected information through public monitoring as well as

Development and sharing of proactive threat intelligence is one of the highest cybersecurity priorities of clients in 2017.

Khirodra Mishra, Managing Director, Security Services,
NTT Data Services LLC

other methods, and immediately reported relevant information. Additionally, NTT-CERT conducted vulnerability analysis and technical verification on possibly related issues.

Lessons Learned

NTT successfully provided a stable network environment in the host area of the G7 Summit. NTT identified lessons learned from the work leading up to and during the G7 Summit that can be used to support other large-scale events, including the 2020 Olympics in Tokyo.

- ▶ The first lesson learned was the need for native multilingual threat intelligence support. Online forums and exploit code are rarely in a single language. While NTT processed multiple languages for the G7 Summit, for the 2020 Olympics in Tokyo, NTT will integrate greater multilingual threat intelligence support in an effort to enrich data gathering and analysis capabilities, especially important considering the magnitude of the event.
- ▶ NTT identified significant challenges in the area of collaboration and information sharing. NTT actively worked to streamline tool preferences and available communication mediums. This process highlighted the fundamental need to understand the context in which the information and intelligence is being gathered, analyzed, and processed. NTT is continuing efforts to actively manage a truly collaborative environment with enabling tool sets, and targeting such business needs for all future endeavors. This has led to the definition and development of an emergency management support system ("KADAN") to address this problem. NTT will take the lessons learned from the G7 Summit and extend appropriate services and functions into the preparation for and execution of security support for the 2020 Olympics in Tokyo.

The G7 Summit provided NTT a perfect opportunity to validate existing capabilities and scale security and threat intelligence capabilities. In preparing for the 2020 Olympics in Tokyo, NTT will leverage its vast array of global security and threat intelligence resources. NTT is uniquely positioned to not only increase cybersecurity during the event, but also to proactively address and mitigate threats before they impact the event.

In this report, we have made it clear that security affects everyone. Whether it's the aftermath of someone stealing your identity, or mass layoffs because of a million-dollar loss from a data breach, your life can be negatively impacted by poor security practices. Everyone, from management and technical staff to users, has important responsibilities regarding security.

Building an effective enterprise security program is not easy, but it starts with tying your organization's security needs and efforts together. That means identifying those needs and taking advantage of security standards, controls, and technologies which you can integrate into your business. This must include a proven risk management methodology which helps prioritize initiatives and elevates security within your organization to a level that all employees, including executive management, understand. The organization's unique risk needs must always be considered in security decision making.

Organizations must acknowledge that people are a key part of any security program. This includes finding and retaining skilled security professionals, using technology and automation to maximize their effectiveness. This also includes ensuring that all personnel are provided the proper level of security and technical training in the context of the organization's business, so they are best able to apply those skills.

Take advantage of real-time threat intelligence. It should automatically be fed into enterprise security controls so they can proactively defend your organization against both current and developing threats, and prevent incidents. For those cases where prevention isn't sufficient, ensure your organization's incident response capabilities are robust and are prepared to act effectively and efficiently, no matter the location of the incident. This includes complying with all applicable laws and regulations.

Ultimately, it should be the organization's goal to become resilient, to minimize the impact that even severe attacks could have on network and system operations. Resilience is challenging to achieve, but choosing the right security practices can help a great deal. Fundamental practices include:

- 1. Keep all devices updated.** Many attacks succeed because laptops, desktops, smartphones, and other devices don't have the latest updates and patches installed. Without those updates and patches, the devices may have security weaknesses of which attackers can take advantage.
- 2. Be ready for phishing attacks.** Phishing attacks sent through emails, texts, phone calls, and other methods try to trick people into going to phony websites or providing information to attackers impersonating someone else. The

Security can be complex.

Organizations are faced with evolving threats. The biggest security priority for companies which wish to be successful should be providing a comprehensive security management, policy, and governance practice which can help manage these competing challenges. Security is best approached in layers, and an important layer is actively managing security as an ongoing daily practice as part of the business.

Kazuhiro Gomi, President & CEO, NTT America

organization must undergo a cultural change so that everyone knows how to check for signs of phishing before clicking on links or opening attachments.

- 3. Use a strong, unique password for each account.** Using easy-to-guess passwords or using the same password for multiple personal and organizational user accounts makes it much easier for attackers to access those accounts and attack the organization from the inside. Remembering a strong, unique password for each account is impossible, but password manager utilities or other automated aids can securely store those passwords and retrieve them when needed so that memorizing passwords is unnecessary.

Realistically, an effective security program is significantly more complicated than this. But ensuring that the security program starts with these basic elements can help form a foundation for a business-aware, context-driven, enterprise-wide security program.

NTT Security Global Data Analysis Methodology

The NTT Security 2017 Global Threat Intelligence Report contains global attack and incident response data gathered from NTT Security and supported operating companies from October 1, 2015, to September 31, 2016. 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 3.5 trillion logs and 6.2 billion attacks for the 2017 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.

About Us

About NTT Security Global Threat Intelligence Center (GTIC)

The NTT Security GTIC protects and informs NTT Security clients via focused security threat research of the global threat landscape, providing actionable threat intelligence, along with enhanced threat detection and mitigation guidance. During 2016, NTT Security was formed as an entity under the NTT Group family of companies. With this transformation, the GTIC was defined as the next generation of the NTT Security global threat intelligence strategy. Legacy research groups, such as Solutionary SERT, are now included as part of the larger global mission and leadership, and have been incorporated into the GTIC model, to

better address global visibility, analysis, and threat monitoring. As we move into 2017, legacy references to Solutionary SERT, or NTT Group SERT will continue to transition to the Global Threat Intelligence Center.

NTT Group Resources

NTT Security

NTT Security is the specialized security company of NTT Group. With embedded security we enable 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 consulting and managed services 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 information and communications technology companies in the world. Visit nttsecurity.com to learn more.

Dimension Data

Dimension Data is a global IT services and solutions provider that uses its technology expertise, global service delivery capability, and entrepreneurial spirit to accelerate the business ambitions of its clients. With a turnover of USD 7.5 billion, operations in 58 countries, and over 31,000 employees serving more than 6,000 clients, we deliver wherever our clients are at every stage of their technology journey. Our deep understanding of the global business and technology landscape coupled with our commitment to excellence is the key to preparing your business to succeed in the digital era. Visit dimensiondata.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 nttdataservices.com to learn more.

NTT Communications

NTT Communications provides consultancy, architecture, security and cloud services to optimize the information and communications technology 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 196 countries/regions, and 140 secure data centers worldwide.

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.

NTT Innovation Institute

NTT Innovation Institute, Inc., (NTT i3) is the Silicon Valley-based innovation and applied research and development center of NTT Group. The institute works closely with NTT operating companies and their clients around the world to develop market-driven, client-focused solutions and services. NTT i3 builds on the vast intellectual capital base of NTT Group, that invests more than \$2.5 billion a year in R&D. NTT i3 and its world-class scientists and engineers partner with prominent technology companies and start-ups to deliver market-leading solutions that span strategy, business applications, data and infrastructure on a global scale. To learn more about NTT i3, please visit www.ntti3.com.