2017 Global Threat Intelligence Report

Key Findings

NTT Security

Key Findings

NTT Security

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 of hub. It is often used for file sharing.

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

Key Findings

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:

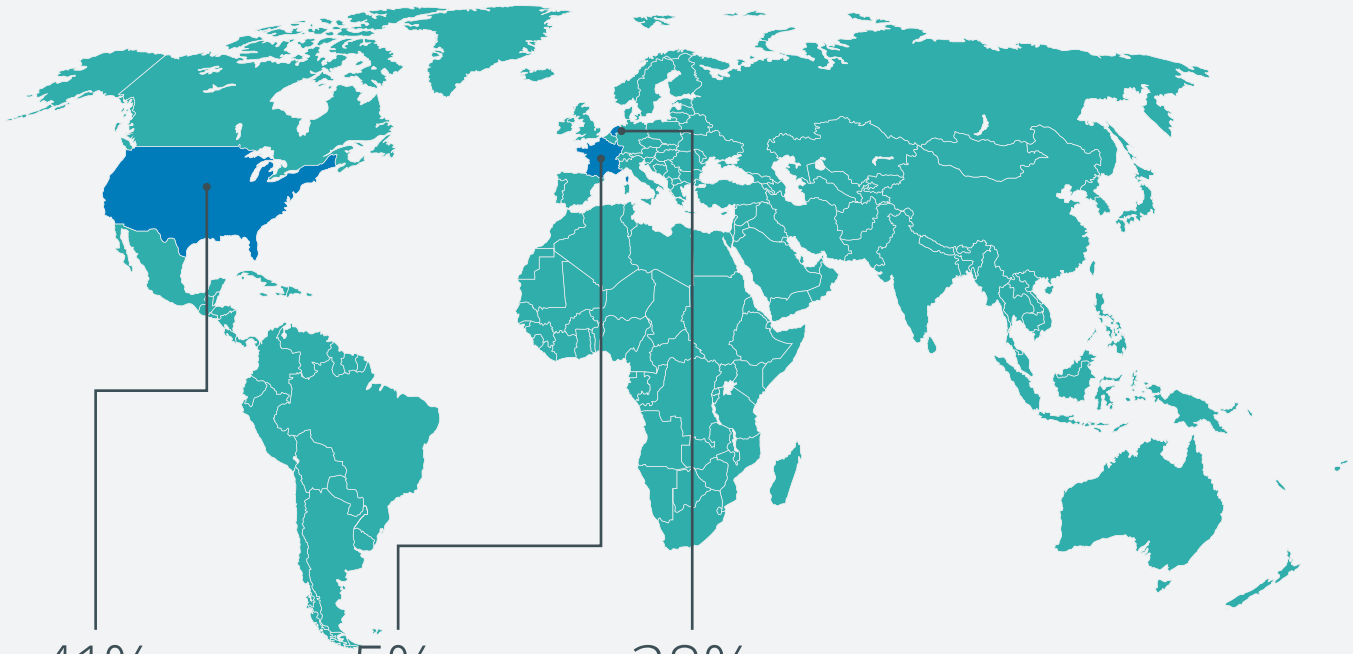
1. *Explosive growth of endpoint devices, such as mobile-optimized applications, along with internet of things (IoT), operational technology (OT) and cloud services adoption increase complexity and potentially additional risks.*
2. *Adversaries are well financed and continue to evolve the sophistication 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%)

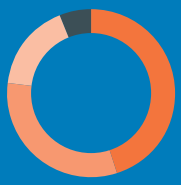
Top sectors supported for incident response:

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%)

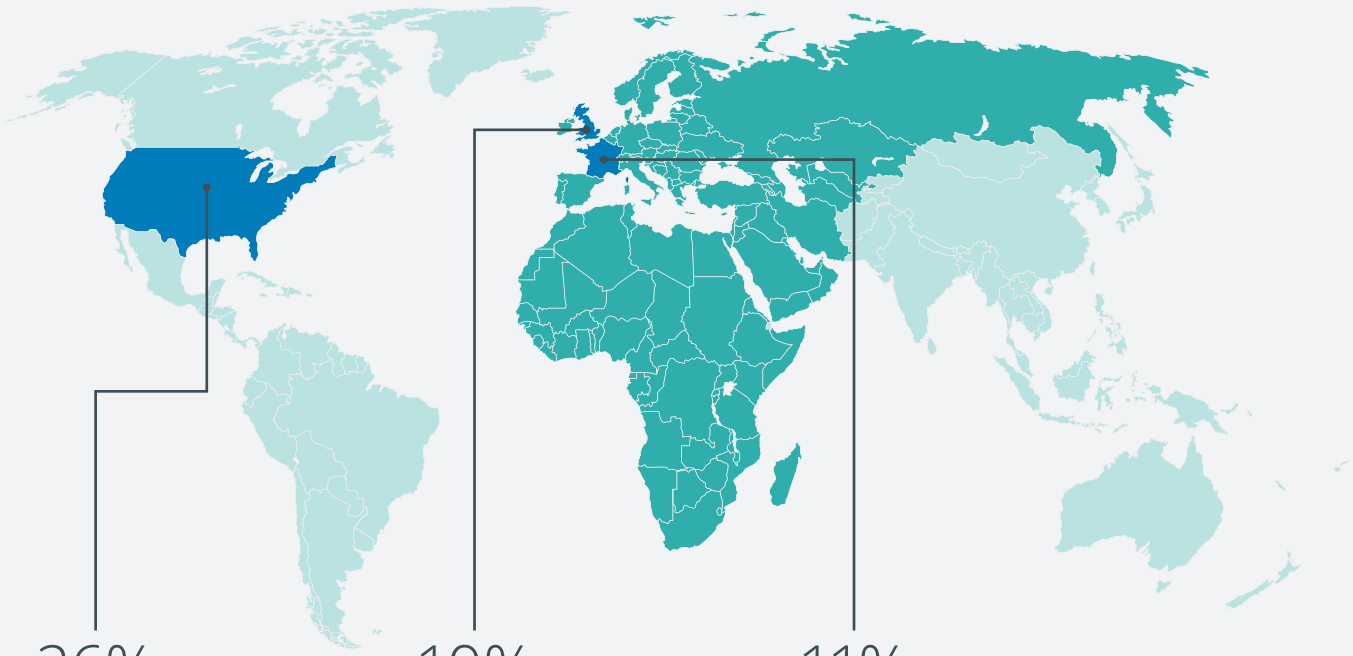
In order to make specific and strategically sound business decisions, clients are finding ways to measure their security posture by making cybersecurity more visible, measurable, and accountable. We all know that no security plan is guaranteed, and there will always be some level of exposure, but defining 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:



26%
United States

10%
United Kingdom

11%
France

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 Netherland.

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.

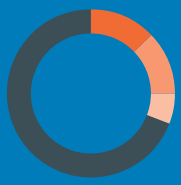
This includes restrictions imposed by customers on "data residency" – the principle that data must be stored and maintained where it is gathered and used. This has continued to push the envelope with service providers. The flexibility of cloud computing and globally-resourced managed service providers, 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.

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.

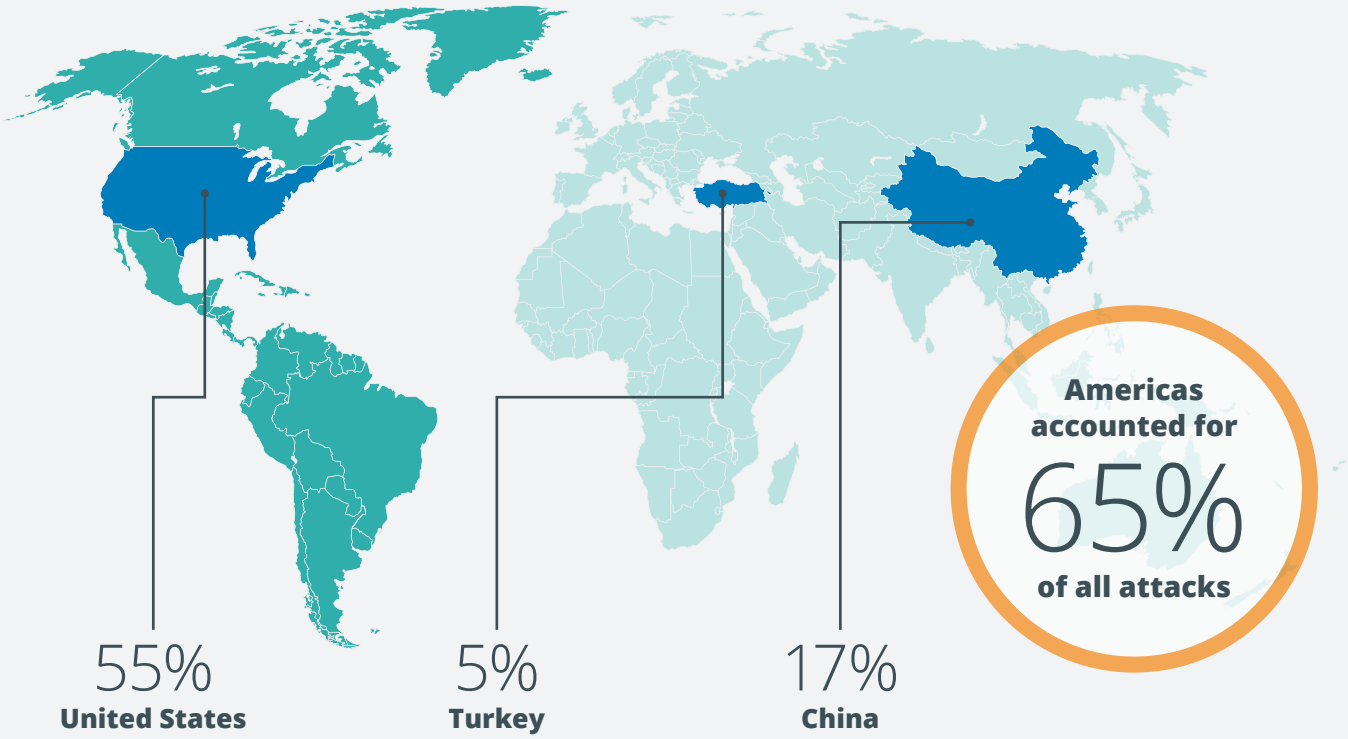
Data breaches continued to take center stage on the evening news. Although organizations are working hard to make their environments more secure and protect their clients' data, the adversary still has the upper hand with time and motivation to persist.

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.

Focus On **Americas**

Top regions attacking the Americas



Top targeted sectors:

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

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.

Top malware types from Americas:

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

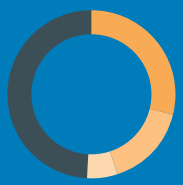
IoT and OT technology are advancing at an explosive rate. There is much discussion today about the complexity of managing security for these types of technologies. NTT Security believes this newer breed of technology will taunt security practitioners for many years to come.

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.

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.

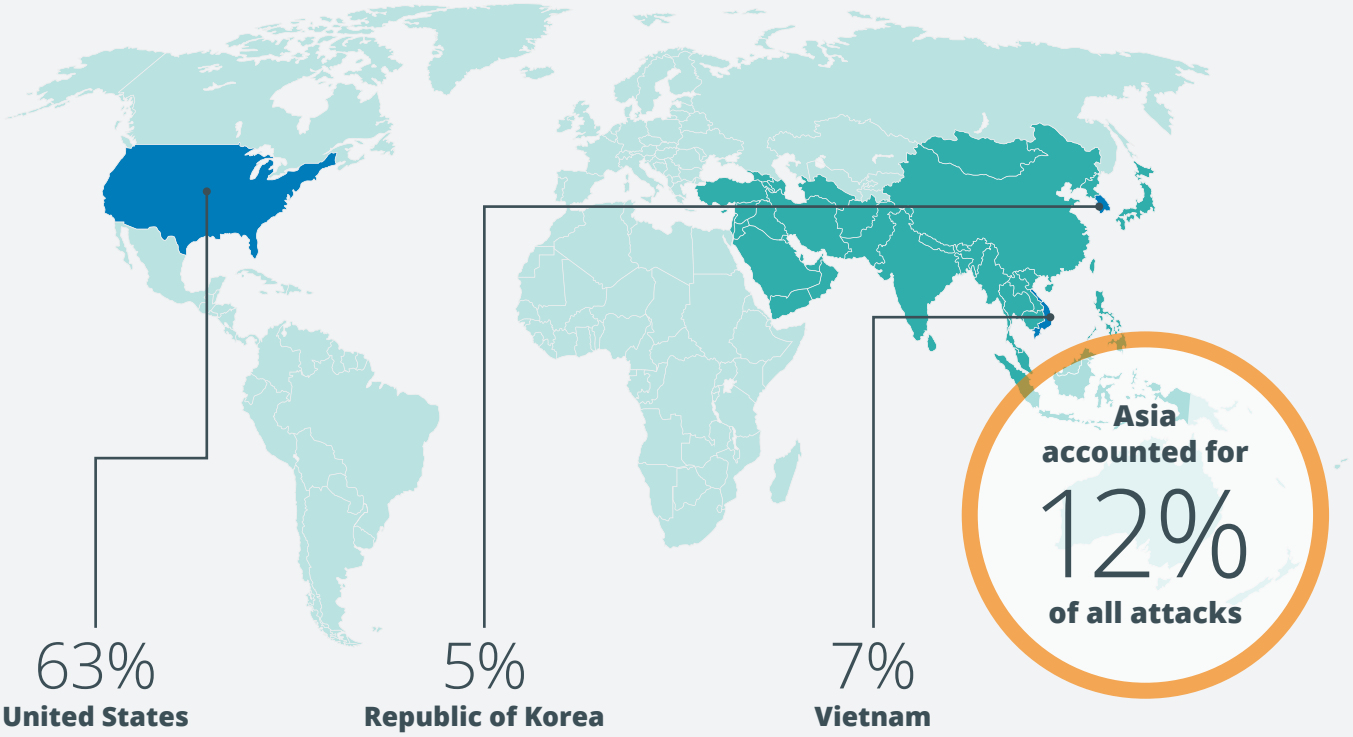
NTT Security saw increases in technology budgets again in 2016, up from 2015. Telecommunications companies again invested more funds into niche security companies in 2016. There is a definite cyclic trend through various cybersecurity disciplines as organizations battle to define what's right for them.

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

Focus On **Asia**

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.

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

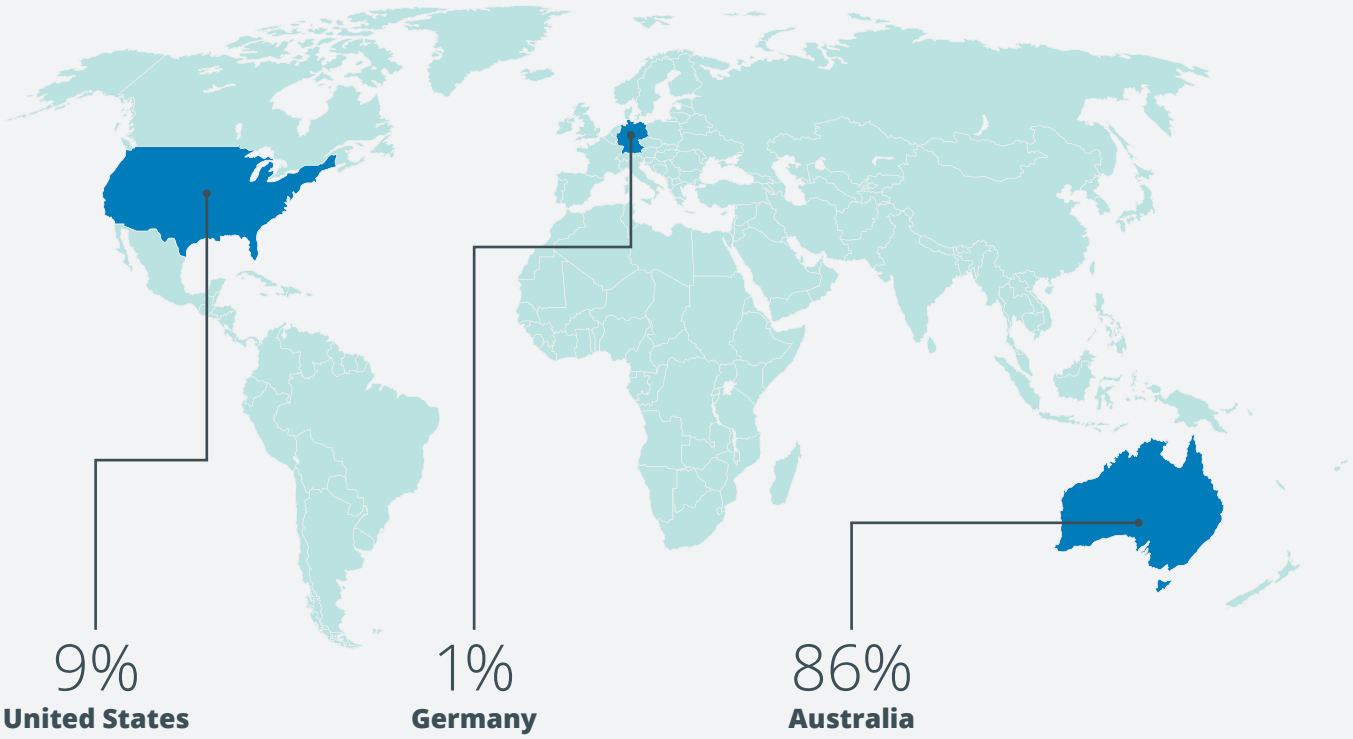
The Notifiable Data Breach Bill was passed by the Australian Federal Parliament in February 2017. The bill will be a mandatory data breach notification law when it becomes an Act, which applies to government agencies and organizations which already must comply with the Privacy Act. Under the bill, organizations 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

Focus On **Australia**

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.

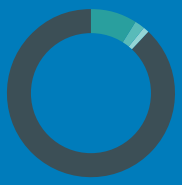
Focus On **Japan**

Top targeted sectors

- Manufacturing (41%)
- Media (26%)
- Finance (16%)
- Other (17%)

Top attack categories from Japan

- Botnet activity (48%)
- DoS/DDoS (11%)
- Data exfiltration (11%)
- Other (30%)



Top attack categories targeting Japan

- Evasion attempts (9%)
- Malware (2%)
- Application specific attack (1%)
- Other (88%)

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

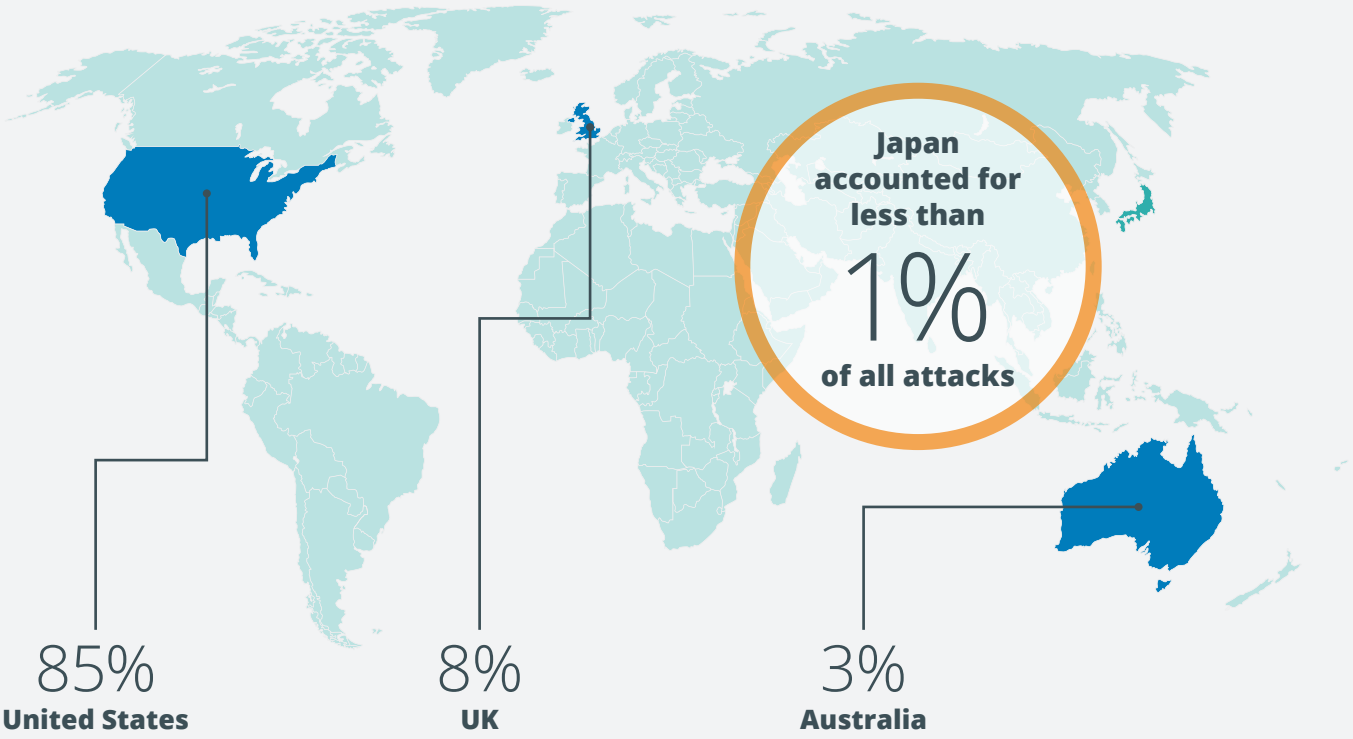
2016 at a glance

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 Bebloh, in successful compromises of ICT systems.

Hacktivist 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."

Focus On **Japan**

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.

About 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 ICT companies in the world. Visit **www.nttsecurity.com** to learn more.