



OVERVIEW AND KEY FINDINGS

# 2017 Global Threat Intelligence Report



## 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.



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 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.

# Key Findings

## 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.*

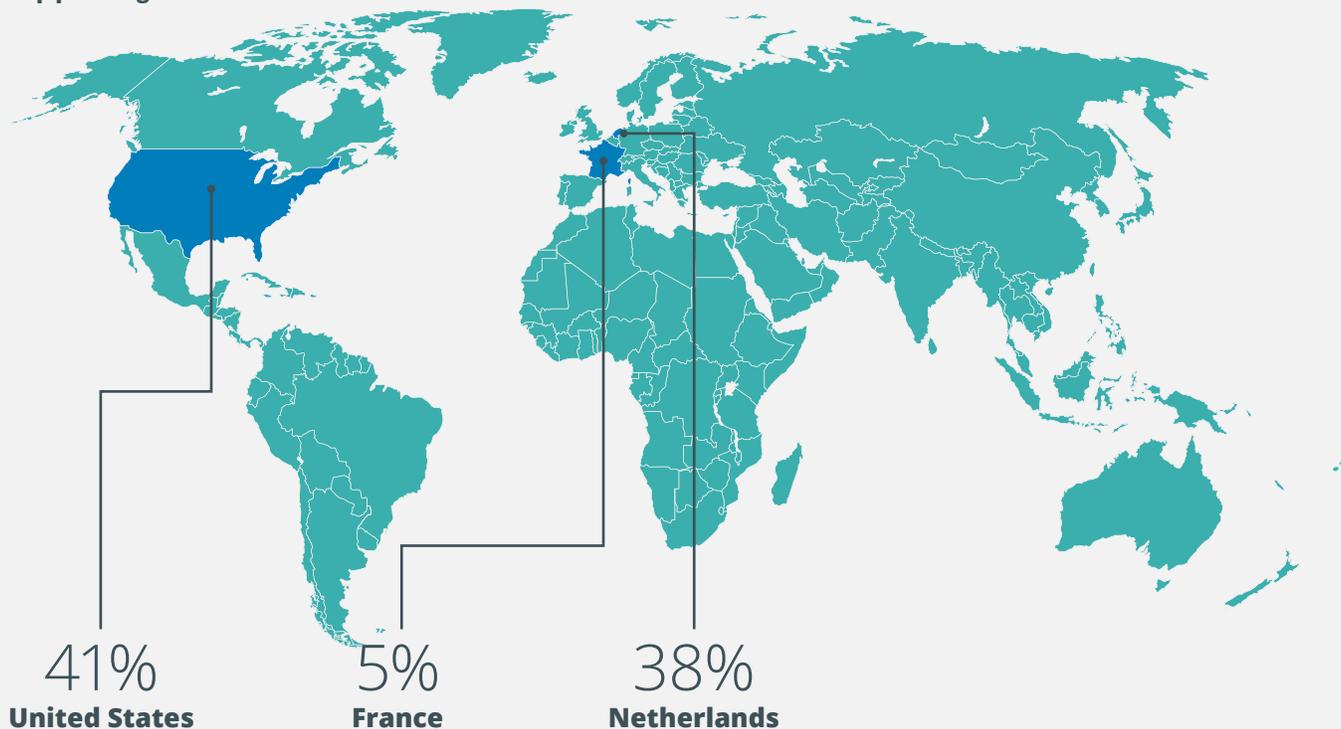
*NTT Security is seeing executives become more proactive, allocating resources based on specific business risks. Organizations are establishing a frontline defense, investing in threat intelligence and expanding their cyber response capabilities. Executives are taking notice that a breach into their 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**



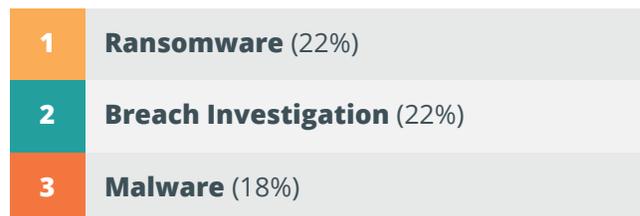
## Top phishing sources:



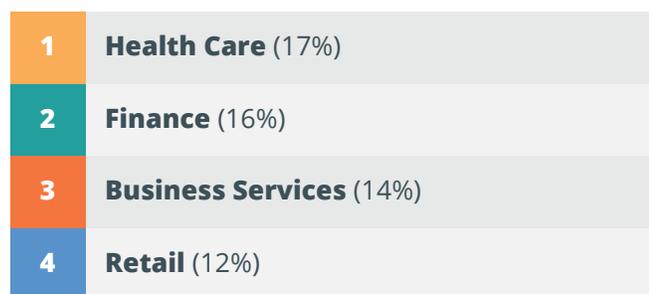
## Top phishing attack targets:



## Top incident response engagement types:



## Top sectors supported for incident response:



## Percentage of organizations having an incident response plan:

**32%**

## 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

Visit [www.nttsecurity.com](http://www.nttsecurity.com) to learn more.

### Dimension Data

Visit [www.dimensiondata.com](http://www.dimensiondata.com) to learn more.

### NTT DATA

Visit [www.nttdataservices.com](http://www.nttdataservices.com) to learn more.

### NTT Communications

Visit [www.ntt.com](http://www.ntt.com) to learn more.

### NTT-CERT

To learn more about NTT-CERT, please visit [www.ntt-cert.org](http://www.ntt-cert.org).

### NTT Innovation Institute

To learn more about NTT i3, please visit [www.ntti3.com](http://www.ntti3.com).

For a copy of the full report visit:

<https://www.nttsecurity.com/us/GTIR2017>