Global Threat Intelligence Center (GTIC) Quarterly Threat Intelligence Report

NTT Security

2017 Q3

Table of Contents

Introduction

NTT Security and its Global Threat Intelligence Center (GTIC) focus on providing timely and actionable information, allowing our clients to gain a better understanding of the threats facing their organizations today. This is accomplished through research and analysis of both current and emerging security threats. Collaboration with the Security Operations Centers (SOCs), Information Security Engineering Team (ISET), Professional Security Services (PSS) and Managed Device Team (MDT) allows NTT Security clients to benefit from our proactive approach to security research and the continuous evolution of detection capabilities.

The GTIC Quarterly Threat Intelligence Report provides a glimpse inside the research conducted by NTT Security researchers over the last three months. In addition to a wide variety of open-source intelligence tools and honeypots, the GTIC also analyzes data from global NTT Security managed security service (MSS) platforms. These patented, cloud-based NTT Security service platforms collect, correlate and analyze security events across systems for our clients around the world, providing researchers with an even deeper understanding of the overall threat landscape.

The quarterly report focuses on several different areas of research and analysis:

- Findings from our analysis of events as observed within client environments and our honeynet infrastructure
- Findings related to research from specific threats
- Observations from recent publicly-disclosed breaches and recommendations on how to mitigate and prevent similar attacks
- Analysis of malicious actor tactics, techniques and procedures (TTPs)

This quarterly threat report takes a closer look at activity associated with China, and at the insider threat — both issues have garnered a significant amount of attention over the quarter. China's cyber activities have had a significant impact on global cybersecurity. Over the past five years, China has never ranked lower than third on the list of countries most attributed with cyberattacks. Some of China's objectives can be directly observed in their Five-Year Plan (FYP), and China's Internet Security law only serves to reinforce China's level of control over their own environment.

Many of the breaches discussed over the past months have had at least some component of an insider threat. But not all insider threats are equal, and not all insider threats are overtly hostile. This report includes a look at different types of insider threats.

Quarterly Highlights

During the third quarter of 2017 (Q3 '17), NTT Security researchers and analysts uncovered information through the research of significant events, identified via global visibility of the NTT Security client base. Some of the key findings based on this research include:

Global Threat Visibility

- NTT Security GTIC observed a notable increase in the number of security events during Q3 '17, up 24 percent from Q2 '17.
- Finance had the most detections for malicious activity in Q3 '17 with 25 percent overall. Rounding out the top five targeted industries were manufacturing (21 percent), business services (16 percent), health care (13 percent) and technology (12 percent).
- NTT Security researchers noted a significant increase in phishing campaigns and malware infections — both up more than 40 percent since Q2 '17.
- Attacks from sources in China moved up from the number three spot in Q2 '17 to number two in Q3 '17.
- As an attack source, India also made a huge jump from outside the top 10 up to number three, most likely due to outside actors leveraging vulnerable and/or compromised infrastructure.

China's Cybersecurity Position is More Complicated Than You Realize

- With nearly 731 million internet users[1] as of March 2017 — 20 percent of the world's users — China has a significant impact on global economic and technological climates.
- According to NTT Security data, China has been one of the top three source countries for global cyberattacks each quarter since 2013.
- China passed its Internet Security law in November 2016, potentially impacting every organization which conducts business in, or with, Chinese entities.
- During Q3 '17, finance and manufacturing were the most heavily targeted industries from Chinese sources, with 40 percent and 31 percent, respectively.

The Face of the Insider Threat

- 30 percent of insider threats will put an organization at risk without the organization even knowing it.
- In 2016, large organizations with more than 75,000 employees spent an average of $7.8 million to address and resolve a single insider threat incident, while small organizations of between 1,000 and 5,000 employees and contractors spent an average of $2 million per incident.
- NTT Security has observed insider threats cost organizations more than $30 million.
- Since the beginning of 2016, only about 25 percent of insider breaches for which NTT Security has performed incident response engagements have been related to overtly hostile activity. The remaining 75 percent were due to accidental or negligent actions.

[1] https://www.techinasia.com/china-731-million-internet-users-end-2016

GTIC – Threat Research analysts observed a 24 percent increase in the number of security events during Q3 '17 from Q2 '17. Increases of over 40 percent in both phishing campaigns and likely malware infections contributed to this increase. Because the first two quarters of the year typically include a greater amount of reconnaissance activity, it is common to observe an increase in targeted malware detections from August through December. It appears attackers follow this trend each year; scoping out their targets in quarters one and two, then running their operations in quarters three and four, once vulnerable targets have been identified. This trend holds true during Q3 '17.

Attack techniques have shifted from formal reconnaissance and exploitation to an increased dependency on botnet infrastructure, phishing campaigns, malicious attachments and links. Attacks against the finance industry included focus on either HTTP brute-forcing financial websites, attempts to inject malicious iFrames or phishing campaigns. Vulnerability targeting accounted for only five percent of detections, however, 49 percent of vulnerabilities targeted in September were related to Apache Struts.

NTT Security analysts observed a 24 percent increase in the number of security events during Q2 '17 from the previous quarter. Analysis of MSSP data suggests this is the result of an increase in reconnaissance and phishing distribution efforts, as threat actors heavily focused on finding vulnerable public-facing servers. Additionally, the tactic of embedding malicious VBA macros into documents sent via phishing emails regained popularity during Q2 '17, as evidenced by an increase in phishing campaigns.

Targeted Industries

GTIC analysis of NTT Security monitoring data indicates the top five industries targeted were finance, manufacturing, business services, health care and technology. Finance was impacted by the most malicious activity in Q3 '17 with 25 percent overall.

Attack Volume by Industry

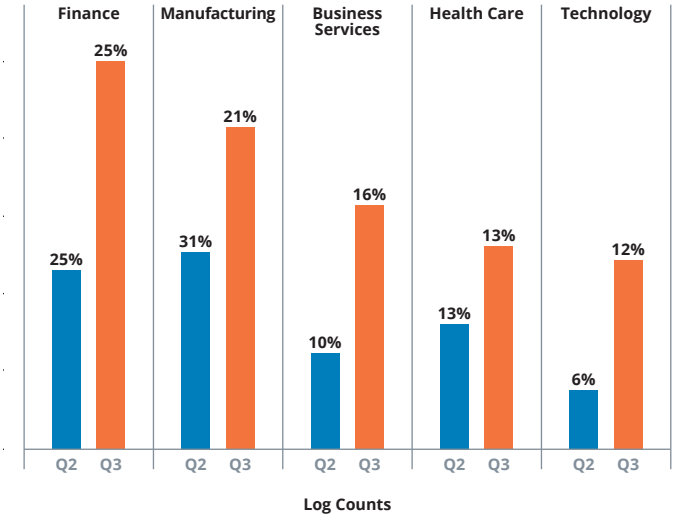


Figure 1. This graph represents the top targeted industries based on attack volume in comparison to Q2'17. Percentages represent the overall attack volume per industry in that quarter.

Finance Phishing Techniques

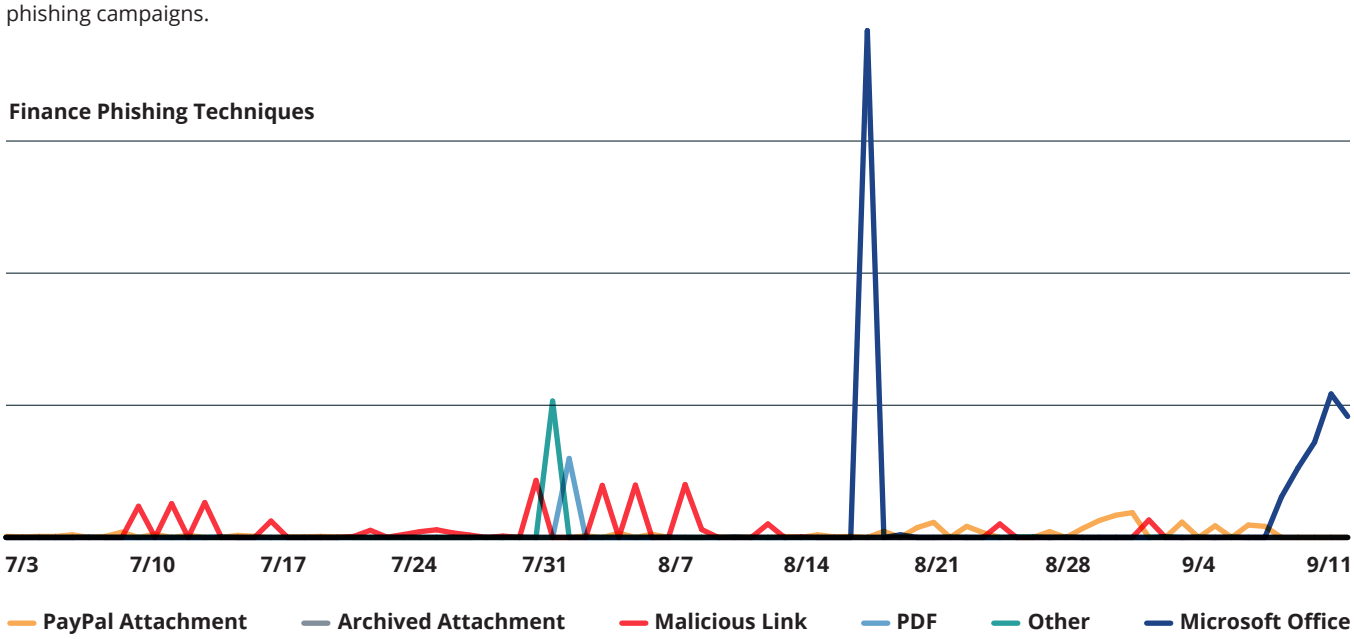


Figure 2. This graph represents the phishing techniques used over time against the finance industry.

A Closer Look at Attacks Against the Finance Industry

A large contribution to malicious activity detected against the finance industry in Q3 '17 was attributed to a 42 percent increase in phishing attempts followed by malware infections. GTIC primarily observed SMTP traffic related to phishing attempts from attackers. As shown in **Figure 2**, phishing against the finance industry was not as pronounced in July, but had several spikes in August, some of them significant.

Phishing campaigns observed against the finance industry were related to banking Trojans Trickbot, Emotet, Ursnif and a recent resurgence of Locky 'lukitus'[2] ransomware; the goal of these attacks appeared to be monetary gain. With an escalation in the delivery of ransomware, threat actors extorted victims for access to locked systems. In addition, banking Trojans scraped credentials from victim machines, which could be sold or used for additional fraudulent banking activity. In recent research, GTIC has discovered campaigns, such as Trickbot, delivering banking Trojan and ransomware payloads, potentially increasing monetary gains.

Attacks by Type

GTIC analysts compared the number of security events in attack categories between Q2 '17 and Q3 '17. Overall, GTIC observed continued attention from threat actors on web application attacks, which increased 42 percent from Q2 '17 to Q3 '17. Of the targeted web application/application specific vulnerabilities, 80 percent targeted or affected vulnerabilities in Microsoft Edge.

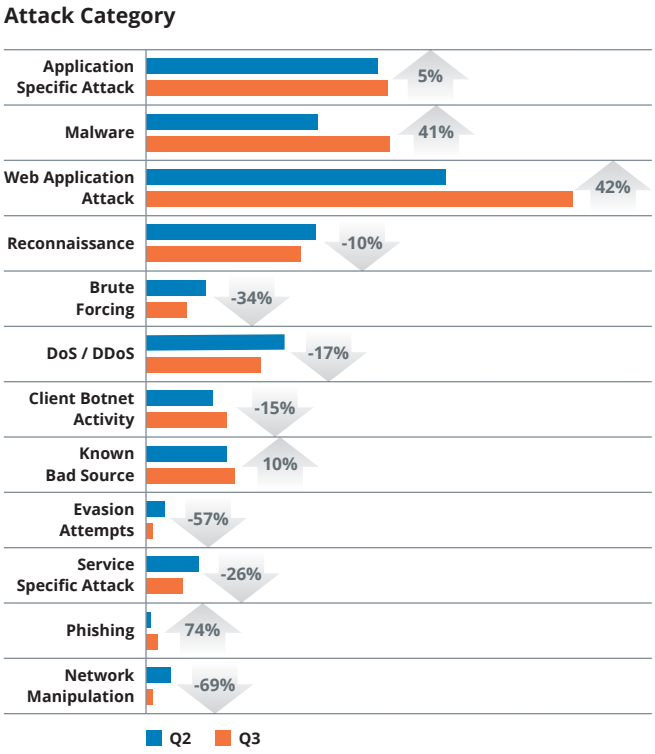


Figure 3: This graph represents the attack volume differences for attack categories across all industries between Q2 '17 and Q3 '17.

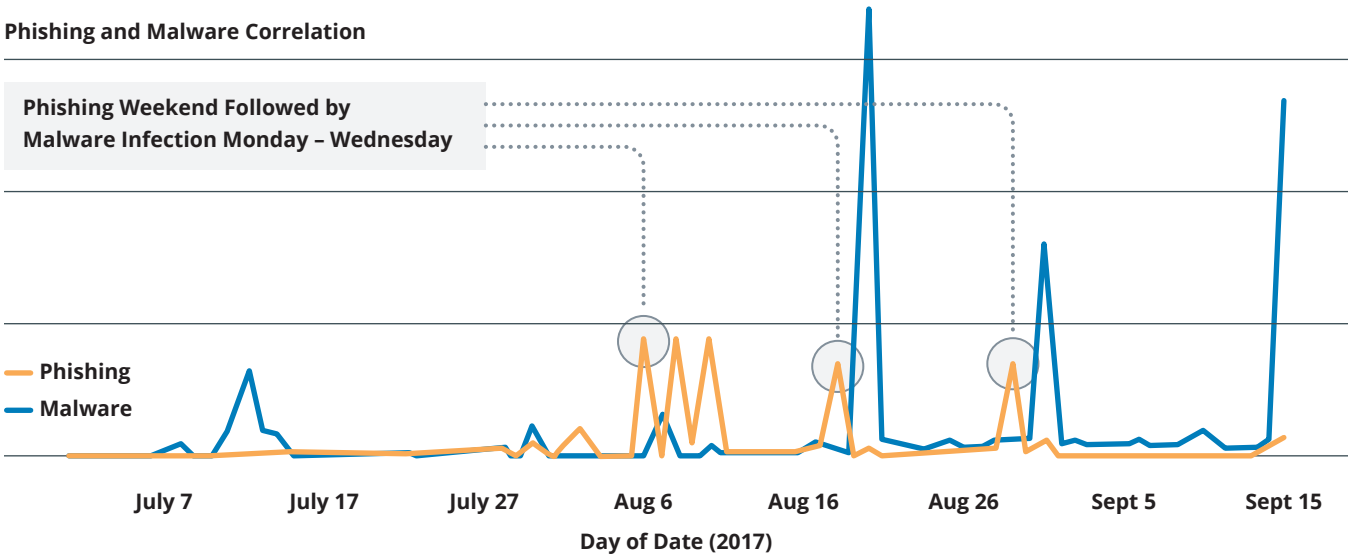


Figure 4: This graph shows a date and log count comparison between phishing and malware detections in Q3 '17.

[2] https://www.bleepingcomputer.com/news/security/locky-ransomware-switches-to-the-lukitus-extension-for-encrypted-files/

Change	Rank Q3 2017	Rank Q2 2017	Attack Source	% of Attack
▲	1	2	Netherlands	11%
▲	2	3	China	6%
▲	3	>10	India	5%
▲	4	8	Canada	5%
▼	5	1	France	5%
▲	6	>10	Russian Federation	4%
▲	7	>10	Philippines	3%
▲	8	>10	Seychelles	2%
▲	9	>10	Germany	2%
▼	10	5	United Kingdom	2%

Table 1: Top non-U.S. attack countries.

With a 41 percent increase in Q3 '17, malware was the second most detected threat. Historically, an increase in malware is typical in the second half of the year, following successful reconnaissance and application exploits. Historically, it has been uncommon to observe malware as the second most common type of attack. With phishing showing a 74 percent increase in Q3 '17, comparing the dates and counts to malware detections highlights some interesting trends as depicted in **Figure 4**.

In **Figure 4**, GTIC shows the relationship between when phishing emails were sent and the when infections were detected. In August, phishing campaigns such as 'mac1' by Trickbot[3] and 'lukitus' for Locky, generated either on Friday or over the weekend, with malware detections consistently spiking the following Monday, and in some minor cases, through Wednesday. This trend occurred three times in August, suggesting threat actors attempted to deliver hostile email meant for employees to open over the weekends, or along with the normal mass of Monday morning emails.

Attacks by Source

NTT Security analysts reviewed the top countries hosting systems generating malicious traffic between Q2 '17 and Q3 '17, as shown in **Table 1**.

Attacks from Netherlands, China, Canada and France continue to occur throughout each quarter. India, with five percent, jumped from out of the top 10 to the third spot. This is a significant jump, in which GTIC identified consistent web application attacks and phishing. In addition, analysis showed threat actors leveraging Indian infrastructure focused on outdated IIS servers with attempts to successfully upload malicious binaries, suggesting planting malware for later use. Additionally, analysts identified attempts in security control evasion and authentication bypass against IIS servers.

Top Targeted Vulnerabilities

Overall, only five percent of attacks detected by NTT Security were vulnerability-related. Interestingly, 49 percent of those vulnerabilities targeted during September were Apache Struts-related with most allowing remote code execution (RCE). RCE is where a remote attacker can have the targeted system, regardless of geographic location, execute arbitrary commands on behalf of itself or a user.

As shown in **Table 2**, vulnerabilities in Apache Struts were consistently targeted throughout Q3 '17. Prior to the Equifax breach[4], CVE-2017-5638 was targeted heavily in both reconnaissance and targeted attempts. Attack attempts were minimal until a few days after the breach was announced on September 7, 2017. On September 9, 2017, Apache released a statement[5] about the initial exploit being CVE-2017-5638, and four days later GTIC observed related attack attempts spike.

Several recent high-risk vulnerabilities in Apache Struts were reported recently, and NTT Security detected attack attempts almost immediately afterwards. Attacks ranged from reconnaissance to malware retrieval and reverse remote desktop protocol (RDP) connections post-exploit. GTIC analysts believe attempts to exploit the vulnerabilities addressed in **Table 2** will continue and all applicable patches should be applied.

[3] https://www.flashpoint-intel.com/blog/trickbot-targets-us-financials/
[4] https://technical.nttsecurity.com/post/102ef6u/equifax-breach-impacts-consumers-and-businesses-globally
[5] https://blogs.apache.org/foundation/entry/apache-struts-statement-on-equifax

CVE	CVSS	Allows Remote Code Execution	% of Attack
CVE-2017-5638	10	Yes	50.8%
CVE-2014-0114	7.5	Yes	17.8%
CVE-2017-9791	7.5	Yes	17.6%
CVE-2017-9805	6.8	Yes	6.7%
CVE-2013-2251	9.3	Yes	3.9%
CVE-2016-3081	9.3	Yes	1.2%
CVE-2013-2134	9.3	Yes	<0.1%
CVE-2017-12611	7.5	Yes	<0.1%
CVE-2016-4438	7.5	Yes	<0.1%
CVE-2016-3087	9.3	Yes	<0.1%
CVE-2013-1966	9.3	Yes	<0.1%
CVE-2013-2115	9.3	Yes	<0.1%
CVE-2013-2248	5.8	No	<0.1%
CVE-2014-0112	7.5	Yes	<0.1%
CVE-2014-0094	5	No	<0.1%

Table 2: This table shows the top 15 Apache Struts CVEs targeted during Q3 '17.

Global Threat Visibility Summary

Overall, NTT Security observed a 24 percent increase in attacks from Q2 '17 through Q3 '17. Based on analysis, the finance industry was a primary target for phishing campaigns and malware infection attempts with banking Trojans and ransomware. NTT Security observed a common infection method leveraging malicious URL links or attachments against other industries, typically used for monetary gain. Primary targets of attackers during Q3 '17 were vulnerabilities in Microsoft products, such as IE and IIS. Attackers, though, shifted their focus to Apache Struts during September, with Struts vulnerabilities being targeted in 49 percent of all attack activity.

Apache Struts has consistently included several vulnerabilities which can be exploited using custom HTTP requests and allows RCE. GTIC believes the constant disclosure of related vulnerabilities has raised awareness of Apache as a viable attack vector. This helps explain why attacks have been regularly observed several days after vulnerability announcements. Based on these trends, GTIC believes more targeted attempts will occur, which will result in the download of malware and additional actions.

The NTT Security GTIC recommends the following to help mitigate the threats discussed above:

- Conduct regular vulnerability scans and penetration testing to identify security gaps, vulnerabilities and flaws.
- Implement Domain-based Message Authentication, Reporting and Conformance (DMARC) to reduce spoofed email phishing.
- Consider whitelisting approved applications which run on internal networks and public-facing applications.
- Educate users to the risks of phishing. Specifically, identify high profile targets who are likely to be at potential risk of spear phishing, and educate them on their elevated exposure.
- Always take a Defense-in-Depth (DiD) approach to security controls, including defining internal segmentation and segregation, which increase roadblocks for threat actors.
- Establish an Incident Response Team with formal and documented processes and procedures.

- Enforce effective patch management via automated and manual processes to ensure software and hardware patches are applied.

- Ensure critical data, information, operating systems, applications, tools and configuration files are backed up and stored offline. Processes and procedures to revert to backups during an incident should be documented and tested on a routine basis.

China's Cybersecurity Position is More Complicated Than You Realize

Year	China's Rank
2016	3
2015	3
2014	2
2013	2
2012	2

As news of the latest security breaches is revealed, many cyberattacks appear to stem from China. China's cybersecurity position isn't cut and dry, however; new laws are being enacted which will shore up their defenses and connectivity, keeping the country up-to-date with many other cybersecurity laws across the globe. The general perception is that China is responsible for a significant number of cyberattacks seen around the world on a regular basis. As a matter of fact, NTT Security's own Global Threat Intelligence Reports for the past five years attest to this fact, as IP addresses in China have ranked within the top three of all source countries (consider also that IP addresses within the United States have always been the number one source of attacks).

Worldwide Economy

As worldwide economies grow around the internet and constant connectivity, the world seems to shrink, and appears as though it's growing into one market.

But with increasing global connectivity and operations come an increased need for regulations, like the General Data Protection Regulation (GDPR[6]) and new Chinese cybersecurity regulations and laws. According to the Internet World Stats[7], China reached 731 million internet users in March 2017, which shows as nearly 20 percent of the world's internet users, and this number is probably incomplete as it does not include Taiwan, Hong Kong and Macau. China is a world-class economy, and shares a significant footprint in internet space.

Bringing its internet base and economic power to bear, China is often seen as a leader in the world's economy. The country's influence runs wide and deep, affecting issues from world policy to Bitcoin trade to data privacy. New regulations regarding issues, like data privacy, will further alter how the world does business with China.

China's Internet Security Law of 2016

One law in particular has companies conducting operations in China somewhat perplexed, particularly given the law's ambiguity. Foreign firms may suddenly find conducting the same business is much more difficult than they had previously experienced.

On November 7, 2016, China passed a cybersecurity law — which translates to the "Internet Security Law of the People's Republic of China[8]" — which impacts any organization conducting business in, or with, China. More than 40 business groups worldwide have subjected this law to intense scrutiny, as it would require companies conducting business within China's borders to store data locally, as well as turn over encryption keys to the Chinese government. Beijing states this law is in response to threats such as hacking and terrorism.

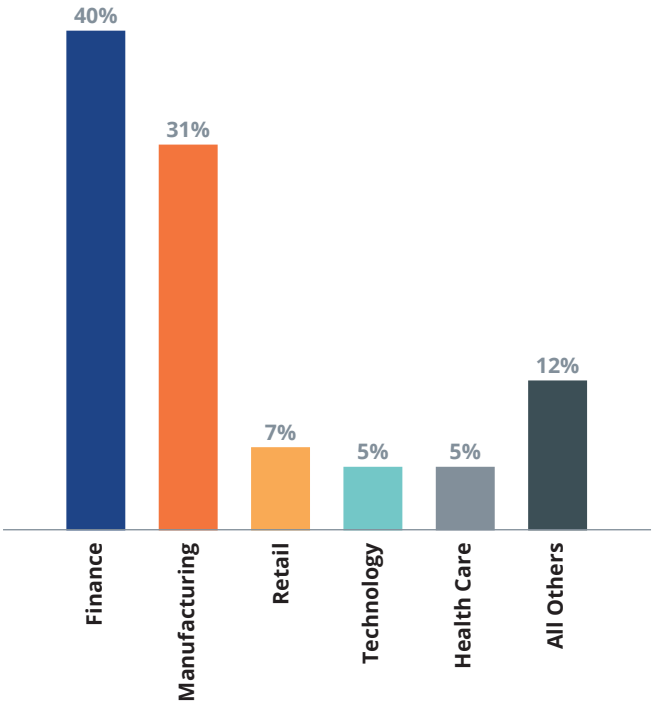
This law is not unique. Other countries (e.g., France, Germany, and the Russian Federation) have strict data sovereignty laws as well. GDPR, which goes into full effect in the European Union in May 2018, includes strict sovereignty requirements. Other countries have also at least discussed requiring companies doing business within their borders to provide master encryption keys. As recently as August 2017, a Deputy Attorney General for the United States suggested that the government would like to require technology companies to decrypt on demand[9]. More often, however, countries have followed the example of France who, in January 2016, publicly abandoned such initiatives for the sake of the privacy of business.

In the case of China, critics have their fears: namely, that this law requires companies conducting business within China's borders to store data locally, as well as turn over encryption keys to the Chinese government.

The law appears to effectively give China additional censorship powers, while simultaneously granting the government nearly unlimited access to user data, as well as the intellectual property of organizations doing business in China, all in the name of national security. Of additional concern to the private sector is that the legislation could potentially be a means of acquiring sensitive intellectual property, potentially undermining business dealings of affected organizations.

[6] https://insight.nttsecurity.com/post/102edwj/how-will-gdpr-impact-the-increasing-global-cyber-threats
[7] http://www.internetworldstats.com/stats3.htm
[8] http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm
[9] https://www.theregister.co.uk/2017/08/31/deputy_ag_rosenstein_calls_to_force_backdoors/

Activity from Chinese Sources: Q3 '17



This particular law is likely part of a broader initiative called "Internet Plus[10]," designed to increase internet control capabilities and "perfect cybersecurity laws and regulations[11]." Internet Plus also states China will "strengthen the struggle against enemies in online sovereign space and increase control of online public sentiment.[12]"

At another level, this new law is bringing China in line with global cybersecurity standards and best practices, which could prove beneficial to all those affected.

Although multinational corporations will likely be hardest hit in both logistics and cost, including introducing data protection measures and data transfer regulations, the new legislation will affect both foreign and Chinese domestic firms. Additionally, even though parts of this law became effective June 1, with an 18-month phase-in period, many businesses based outside of China still aren't fully aware of the law and its potential implications, especially since much of the law's verbiage, along with how it will be enforced and implemented, is vague and broad in scope.

Due to continued global reaction and intense scrutiny of the law, the Cyberspace Administration of China, the country's internet regulator, has decided to delay parts of the implementation of the new law, particularly the regulations overseeing cross-border data flow, now slated to be carried out toward the end of next year.

Although this law, ultimately, is not likely to discourage investment in the Chinese business arena, it will introduce an additional layer of internet regulation on businesses operating in China, which could reduce productivity or weaken long-term competitiveness.

Impact on China's Five-Year Plan (FYP)

China has strived to modernize their technical capabilities, and has made great progress in reducing their reliance on Western technology. This legislation was likely a huge impetus toward progression of these efforts. Historically, industries such as finance, technology, manufacturing and health care have all been featured prominently in China's Five Year Plans. Since then, those industries have experienced high volumes of attacks from China, along with many other sources. NTT Security's own analysis of attacks has identified these trends.

While China's technological self-reliance will likely continue to increase, partially due to Internet Plus measures, it is unlikely that we will see a drop-off in cyberattacks focusing on the most targeted sectors. Organizations in industries outlined in the current Five Year Plan (FYP), in effect through 2020, especially those in the finance, manufacturing and technology industries, should remain vigilant, as these industries may be more heavily targeted, at least until that time.

Activity from Chinese Sources: Q3 '17

Based on analysis of NTT Security's monitoring data, finance and manufacturing were the most heavily targeted industries from Chinese sources during Q3 '17, with 40 percent and 31 percent, respectively. This as manufacturing activity in the U.S. hits a 13-year high. Rounding out the top five were retail at seven percent, technology and health care, each at approximately five percent.

It is important to note that the term "Chinese sources" does not imply attribution, necessarily, to any entity associated with China. Threat actors often route through several nodes, making it difficult to determine the true source of malicious activity. Just like for most attack sources, attacks from China can show in a number of ways:

1. Attacks from China IP addresses which are from government-sanctioned sources

[10] https://en.wikipedia.org/wiki/Internet_Plus
[11] http://www.reuters.com/article/china-parliament-tech/china-lays-out-its-vision-to-become-a-tech-power-idUSL3N16D08V
[12] http://www.reuters.com/article/china-parliament-tech/china-lays-out-its-vision-to-become-a-tech-power-idUSL3N16D08V

2. Attacks from China IP addresses which are from independent sources

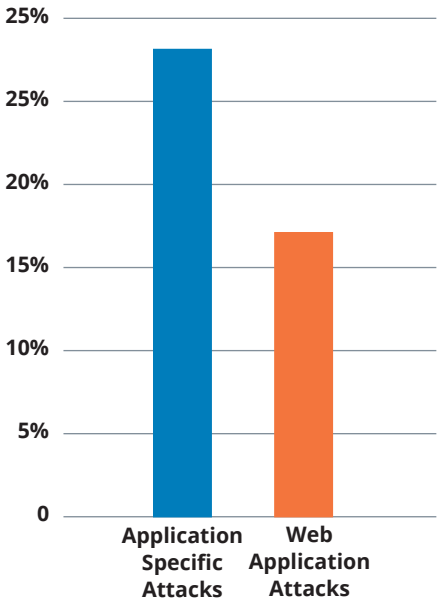
3. Attacks from China IP addresses from sources other than Chinese attackers

4. Attacks from Chinese attackers which actually source from a non-China IP address

Application-specific attacks and web application attacks, 23 percent and 17 percent, respectively, were the top attack categories from Chinese sources against NTT Security clients during Q3 '17.

Specifically, there was a notable amount of botnet traffic against manufacturing devices. Together, BASHLITE and Mirai accounted for 98 percent of this botnet traffic. Telnet port 23 was targeted in this traffic for BASHLITE and Mirai propagation.

Two Most Common Attacks from China



Research from NTT CERT in Japan indicates an enormous amount of vulnerable Chinese hosts, possibly exacerbating the botnet situation. A ransomware WannaCry campaign spread rapidly among Windows hosts in China, as many hosts, as in many countries worldwide, remain without appropriate patches, Windows updates or network segmentation. To boot, there are innumerable vulnerable Android phones within China.

Larger-scale botnets are also taking advantage of vulnerable Chinese hosts; one Mirai botnet, the An-yun botnet[13], has 1.62 million bots, and 99.9 percent of bots are in China.

Analysis by NTT CERT researchers indicates this botnet activity within China is likely used for extortion activity. Smaller threat groups typically run these botnets, hoping to avoid detection by law enforcement. For this reason, some exploits or malware are not detected and not patched outside the Chinese "Great Firewall."

Activity of this type may suggest that manufacturing devices – perhaps internet of things (IoT) and operational technology (OT) devices, specifically – remain unsecured. GTIC research analysts observed propagation techniques in which a compromised host in China attempts to setup a Telnet connection and then copy itself over to organizations in the U.S. manufacturing industry.

These targets may have been chosen after reconnaissance during the first two quarters of 2017, in which Chinese hosts searched for, and found, vulnerable IoT/OT devices in manufacturing organizations' infrastructure.

In addition, GTIC research analysts noted Sundown Exploit Kit activity from 114.55.105[.]132, associated with the domain daoxiangcun[.]cn. Use of this EK, while not often observed in recent months, may suggest Sundown is specifically targeting Internet Explorer (IE) exploits. This may indicate manufacturing PCs used by end users still contain default applications, where Windows 7 and older operating systems may be in use, and IE may be the browser of choice.

Also of note is that 62 percent of the attacks from China against manufacturing in Q3 '17 targeted Apache Struts-related vulnerabilities — either CVE-2017-5638[14] or CVE-2017-9791[15]. While a majority of this activity was reconnaissance-related, some activity attempted to establish reverse tunnels or download malware post-exploit, which may indicate attempts to establish and maintain a foothold in targeted networks. This continues a trend from Q2 '17, when 76 percent of all attacks targeting Apache Struts originated from IP addresses in China.

China Cyber Activity: Conclusions

NTT Security and other researchers' analysis of the types and nature of attacks used can characterize some of these attacks. Chinese actors' operations have historically tended to be longer-term; they seek to maintain persistent access to their targets. In fact, Chinese actors have been known to maintain persistence for several years without detection, siphoning data as it becomes available or as it is needed. With China's new Internet Security Law, NTT Security would not be surprised to observe some moderation of attacks in some industries, but organizations in the most targeted industries (finance and manufacturing) should not expect significant relief any time soon.

Unsecured IoT/OT devices, targeting of the technology and manufacturing sectors, both outlined in the FYP as industries of focus, all promote — and suggest — continued attacks on the supply chain. As this type of attack becomes more common, users are encouraged to be aware of all vendors in their supply chain.

[13] https://www.ithome.com/html/it/312946.htm
[14] https://nvd.nist.gov/vuln/detail/CVE-2017-5638
[15] https://nvd.nist.gov/vuln/detail/CVE-2017-9791

When dealing with external attacks, from China or any other source, baseline security controls are important. Maintaining a mature backup and restore process, implementing an effective patch management system, and integrating defense-in-depth into business and security operations are solid steps in creating an effective security program.

In addition to baseline and advanced defensive measures, NTT Security recommends that multinational organizations which are (or plan to be) conducting business in China closely monitor further developments of the China Internet Security Law, specifically as it pertains to the data storage and encryption key requirements and the inspection of network products before they can be sold in China. Organizations contemplating doing business with (and in) China would be prudent to take this new law into account when conducting risk management assessments.

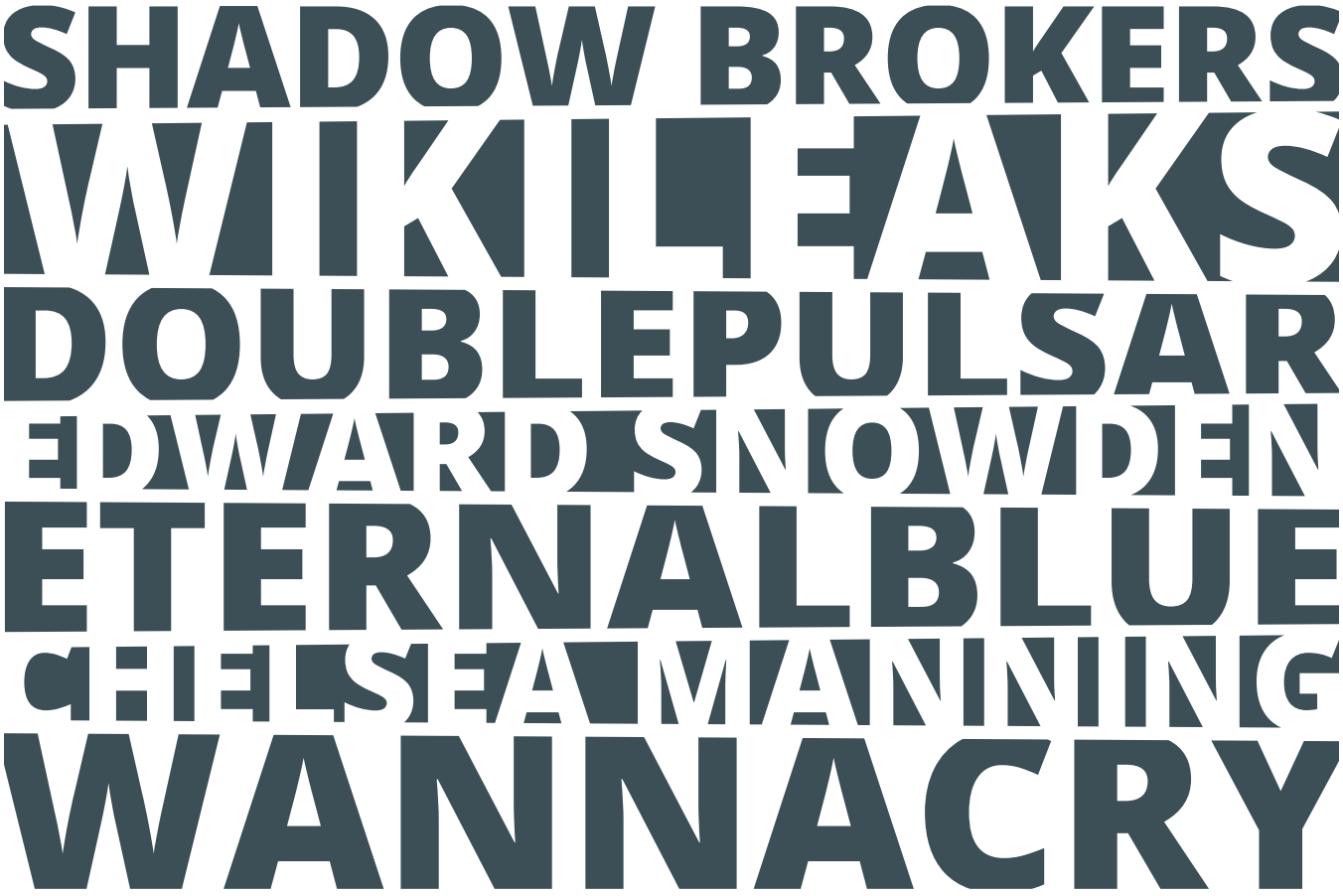
References:

China’s strict cybersecurity laws took effect today; potentially impacting foreign businesses

China's Cybersecurity Law: What You Need to Know

China’s cyber security law rattles multinationals

Overview of China’s Cybersecurity Law



Nearly every one of these people, exploits or groups is a household name today. Can you guess something they all have in common?

If you guessed "Insider Threat," you'd be correct. Without insider threats who breach – and leak – sensitive information, none of the items shown above would have seen nearly as much success.

The above list of entities continues to make headlines even today, but it's probably easy to believe an insider threat may not be a serious concern for your organization. Yet, nothing could be further from the truth. The reality is that insider threats are a danger to all organizations, big and small – and the worst part? Many of them, around 30 percent[16], will put your organization at risk without even knowing it.

About 10 percent of NTT Security incidents so far during 2017 have been related to insider breaches, which is consistent with incidents from previous years. This isn't to say that only 10 percent of companies are experiencing breaches or complications due to insider threats, but only that about 10 percent of companies have been asking for help in dealing with such breaches. While that number appears low, the characteristics of those engagements are actually more telling. Since the beginning of 2016, only about 25 percent of insider breaches for which NTT Security has been involved with incident response engagements has been related to overtly hostile

[16] https://www.securityforum.org/uploads/2017/01/Managing-The-Insider-Threat-ISF-Briefing-Paper.pdf

activity — an inside attacker stealing corporate resources or information. The remaining 75 percent of insider activity has been either accidental, or related to activity better classified as negligent, or perhaps "not compliant with corporate policy." NTT Security took a different approach to this section of the report and made great efforts to communicate the very human side of the insider threat.

Giving a "Face" to the Insider Threat

Insider threat – a term that found its birthplace on military bases in war zones, is an often-misunderstood term. Additionally, the entire concept is difficult to conceptualize. There are not always indicators of an insider who is about to wreak havoc on an organization from within.

Accidental Insider Threat

Meet Julia.

Julia is an accounting specialist at ABC Corporation of America (a fictitious company).

Julia has been an integral part of the ABC team for nearly five years, and her supervisors could not be happier with her performance. Julia is rapidly moving through the ranks. Always quick to lend a helping hand and share her deep and thorough knowledge of accounting and finance, Julia is the epitome of the term outstanding talent.

One Tuesday morning, as Julia was putting together one of the company's quarterly reports, she emailed a copy of the company's profit and loss report to Beth, a co-worker also in ABC Corporation's accounting department, and continued about her day.

That afternoon, Beth called Julia on the phone, "Hey, Julia, could you send me a copy of that profit and loss report for this quarter?"

Confused at the request, knowing she sent the report earlier, Julia checks her sent emails and realizes what happened. Julia accidentally sent the company's entire profit and loss report to their competitor, ABV Corporation of America.

Julia is mortified and informs her supervisor immediately. The question now is — what does ABC Corporation do? And what could the company have done prior to decrease the risk of something like this happening?

Julia, Accounting Specialist

ABC Corporation of America

Accidental Threat Facts

Julia is the perfect example of an accidental insider threat. She is a loyal employee who simply made a mistake — a grave mistake to be sure. But, with no ill intent and a pristine work history, Julia's actions are accidental in nature.

Accidental insider threats can take on a variety of forms:

- Accidental disclosure (e.g., unsecured databases, default internet-facing username and password logins, or as in Julia's case, because of a single letter in a domain name, an email sent to the wrong person)
- Improper or accidental disposal of physical records (e.g., disposal of paper without shredding, losing sensitive documents, documents or equipment being stolen, etc.)
- Accidental damage (e.g., accidental misconfiguration or command which results in loss of data or connectivity, like a network engineer who accidentally reverses the parameters in a command line and copies an old backup over the production system, instead of copying the production database to a backup)

Statistically, miscellaneous errors account for around 30 percent[17] of all accidental behaviors. These include publishing errors, disposal errors, or, as in Julia's case, misdelivery of information.

[17] https://www.securityforum.org/uploads/2017/01/Managing-The-Insider-Threat-ISF-Briefing-Paper.pdf

Accidental Insider Threat Mitigation

Thankfully, there are steps you can take to mitigate the effects of the accidental insider threat.

Notice we used the term "mitigate the effects", not the more common term "mitigate the risk." NTT Security chose this term carefully and believes it addresses the issue directly — accidental behaviors that put your organization at risk will occur, but here is what you can do to prepare for that:

- Have a written, established incident response (IR) plan in place. Keep in mind, this needs to be an IR plan to guide you and your organization through the aftermath of an accidental insider threat breach. You should periodically review your IR plan as if it is a living document, not a standard operating procedure manual created to take up space on an office bookshelf.

- If it does not impact your operations, consider implementing a solution that makes it more difficult to send attachments to email addresses outside your organization. (Note: While making it more difficult does not prevent a malicious insider from sharing privileged company data, it can reduce the risk of accidental breaches in your environment.)

- Align privileges/authorizations commensurate with employee roles. Or, put another way, don't hand out "admin access" like free candy. And remind administrators that, by the way, administrative accounts are to be used for admin functions, and that user accounts should be used for normal user duties. Reserve the admin account for truly privileged functions.

- While security awareness training does not "fix" anything, exposure to such training can raise employee awareness, and potentially elevate their level of care.

Negligent Insider Threat

Meet Ben.

Ben is a member of the sales team at DEF Company (another fictitious company), where he has been employed for nearly two years.

While the pay is good, and Ben has been relatively successful in his sales venture at DEF Co., Ben is rather bored with his job and often complains that IT security policies get in the way of real progress.

Ben, Sales Associate

DEF Co.

Since Ben works remotely, his IT team has given him administrator access to his machine. Ben used to only log in as an administrator if he needed to do simple things requiring administrator access — things like installing a new printer or downloading and installing new drivers. More recently though, Ben has been working from his administrator account "because it's just easier."

Although Ben has no ill intent toward DEF Co., he does not hesitate to install software from unauthorized sources if he thinks he needs it. DEF Company's IT director is aware of Ben's actions, but makes no effort to address Ben's behavior since "pretty much everyone does it anyway" (making the IT director equally guilty of being a negligent insider).

One day, while working on a sales presentation, Ben began searching the internet for new icons, and discovered what he thought was an icon generation program, which he promptly downloaded to his system.

Unfortunately for Ben, what he downloaded was malware which allowed an outside attacker to breach the company network via Ben's computer, obtain access to DEF Company's customer database and subsequently steal private customer information.

Negligent Insider Threat Facts

While organizations are increasingly trusting their employees and others who have insider access to keep information safe, research found that only 42 percent of this group[18] believed it was their personal responsibility to do so.

[18] http://www.cisco.com/assets/global/UK/products/security/How_to_be_agile_and_secure.pdf

Negligence can severely impact an organization's bottom line, with costs ranging significantly based on the incident, though the average incident cost due to negligence is nearly $207,000[19]. Carelessness is rampant in organizations, with negligent employees and contractors accounting for 68 percent of insider threats[20].

Negligent Insider Threat Mitigation

What can you do about an employee or contractor who seemingly has no regard for information security policies? NTT Security recommends the following:

- Implement a "no tolerance" policy, and ensure employees and contractors understand that intentionally circumventing information security policies will have consequences.
- Provide administrator-level access only to those for whom that level of access is critical to their role.
- Implement "protecting information security" into each employee's goals and objectives, ensuring each of them knows there is personal responsibility for protecting company data that comes with being employed by your organization.
- Implement security awareness training. Effective security awareness training can increase an employee's understanding of the impact their actions can have on the organization.

Malicious Insider Threat

Meet Alan.

Alan is a project manager for GHI Company (also a fictitious company), where he just passed his fourth anniversary.

Although he may not look it, Alan is angry. The executive leadership recently cut 75 percent of the budget for a project Alan is responsible for seeing through to completion. Alan knows the project's success is now virtually impossible, so he begins planning his exit.

Alan begins with copying as much proprietary information as possible and dropping it into a draft folder in his personal email account. Alan will use this information in the future to leverage his position with a future employer.

But that's not enough for Alan. Alan is a disgruntled employee, believing that his employer is setting him up for failure.

Alan, Project Manager
GHI Company

As a project manager, his company's IT department allows him access to nearly every folder on the company's network drive. Alan opens files from available HR folders, then copies and pastes a variety of personally identifiable information (names, addresses, social security numbers, birth dates, even salary information) into a cloud-based spreadsheet service, then waits for the perfect time (probably soon after his departure from the company) when he will "leak" that information to Pastebin, a website where users can store public-facing text online. And for Alan, the best thing about Pastebin is that he can upload everything anonymously.

Alan is his organization's worst nightmare. He has motive, means, and access to as much data as he wants to leak — and this leak will cost the company much more than it saved by cutting the budget for his project.

Malicious Insider Threat Facts

Alan is not alone in his plan to take proprietary company information with him to his next job. In fact, one study[21] found that around 15 percent of employees have taken "business critical information" with them when moving to a new company, and nearly 60 percent of those plan to use the information in their next job.

While coming up with hard and fast numbers to indicate dollar losses associated with a malicious insider threat, one study found that malicious insiders cost the organization nearly $350,000 per incident[22]. The same study concluded that 22 percent of insider threats could be categorized as malicious insiders.

[19] https://learn.dtexsystems.com/rs/173-QMH-211/images/2016%20Cost%20of%20Insider%20Threats.pdf
[20] https://learn.dtexsystems.com/rs/173-QMH-211/images/2016%20Cost%20of%20Insider%20Threats.pdf
[21] https://www.infosecurity-magazine.com/news/employees-willing-leak-sell/
[22] https://learn.dtexsystems.com/rs/173-QMH-211/images/2016%20Cost%20of%20Insider%20Threats.pdf

Malicious Insider Threat Mitigation

Guarding against a malicious insider is probably the most challenging aspect of an insider threat mitigation program, as these threat actors are going out of their way to steal or destroy company data. While raising awareness throughout the organization about insider threats can often reduce the risks associated with accidental or negligent insider threats, combatting malicious insiders presents a much more difficult challenge. There are, however, some steps your organization can take to mitigate your risk.

Evaluate your insider threat risk:

- A variety of open source risk documents are available to help organizations evaluate their risk in different areas, though it is often best to have a trained third-party risk professional perform these tasks.

- Another method is to use the International Security Forum's Information Risk Assessment Methodology 2 ($IRAM_2$ [23]) process, which uses numerous threat attributes, such as capability, motivation and intent, to evaluate your organization's risk level. (Note: The $IRAM_2$ can assist you in determining your risk from outside factors as well.)

Costs of an Insider Threat

Losses due to an insider threat can vary widely. Analysts involved with this report were involved in an incident where a misdelivered file was simply deleted by a person who was not supposed to receive it. While the event resulted in retraining of some staff members, it caused no actual loss.

At the same time, another breach included the theft of highly sensitive design documentation by a disgruntled employee. The ex-employee took the material to a competitor, who delivered a product to market before the company who had invested in the research and development process. The victim estimated their losses at over $30 million and followed up with a lawsuit which was eventually settled out of court.

When considering the cost of an insider threat, the main point is that insider threats can be devastating.

The one indicator which tended to remain consistent was that the average incident cost generally aligned with organization size.

In 2016, large organizations with more than 75,000 employees, contractors, etc., spent (on average) around $7.8 million to address and resolve a single insider threat incident, while organizations with between 1,000 and 5,000 employees and contractors spent an average of $2 million per incident[24].

Insider Threat: Summary

This section of the report focused on helping security practitioners better understand the insider threats that they may not normally consider, and to appreciate that the insider threat is a very real threat to your organization.

Just as outside threats (i.e., hackers) are not wearing ski masks while they're attempting to infiltrate your network, the insider threat may be the person in the office just down the hall — not every insider threat is a truly malicious insider.

While instilling a security-minded culture is a critical aspect of mitigating insider threat risk, assigning personal responsibility for protecting company data, as well as determining your organization's risk profile, will also contribute to a stronger security posture.

References:

Managing the Insider Threat: Improving Trustworthiness

How to be Agile and Secure - The Fundamental Challenge Facing Organisations Today

"Comply or die" is dead: Long live security-aware principal agents

2016 Cost of Insider Threats - Benchmark Study of Organizations in the United States

Employees Willing to Leak and Sell Corporate Access

[23] http://www.infosecurityeurope.com/en/Exhibitors/2173827/Information-Security-Forum-Ltd/Products/1193963/IRAM2
[24] https://learn.dtexsystems.com/rs/173-QMH-211/images/2016%20Cost%20of%20Insider%20Threats.pdf

Summary

While the eyes of the world have been on North Korea during Q3 '17 from a geo-political perspective, NTT Security shifted its analytic focus to cyber activity coming from Chinese sources.

Since 2013, China has ranked in the top three on the list of countries most attributed with cyberattacks. This trend continued into this quarter, where activity from suspected Chinese sources rose from third to second. Some of China's objectives can be directly observed in their Five-Year Plan (FYP), and China's Internet Plus laws only serve to reinforce China's level of control over their own environment.

As a reminder that not all attacks rely on technical vulnerabilities, many of the breaches in the news over the past several months included some facet of an insider threat. As a result, NTT Security took a deeper look into the three major types of insider threat personas. Again, the insider threat is not a technological one; it is a human one and is all too often overlooked.

During Q2 '17, GTIC analysts noted an uptick in reconnaissance activity across many industries. This typically translates into an increase in targeted attack activity during the third and fourth quarters; this held true for Q3 '17.

With a 24 percent increase in overall attack activity, Q3 '17 was characterized primarily by phishing campaigns and malware infections, which both skyrocketed — each up more than 40 percent from the previous quarter. The significant increase in phishing campaigns is likely due to the simple fact that these attacks work; attackers can leverage almost any malware within a simple and innocuous, yet effective, email. And Apache Struts continues to be a vulnerability of focus, again heavily exploited during Q3 '17.

As the second most detected attack category, malware saw a 41 percent increase in Q3 '17. Historically, an increase in malware is typical in the second half of the year, following successful reconnaissance and application exploits.

GTIC analysts observed a significant jump in activity from what appear to be sources in India, which moved up from outside the top ten to the third most active source of attacks. GTIC observed a similar trend during Q2 '17: a higher number of attacks from countries not normally high on the list of sources, like the Netherlands and Canada, both in the top four this quarter. This may suggest compromised infrastructure being leveraged by threat actors.

With 25 percent of all attack activity, finance was the most targeted industry in Q3 '17, as it was during Q3 '16. A large contribution to activity targeting finance during the third quarter was a 42 percent increase in network traffic over common email ports — primarily phishing campaigns laced with banking Trojans, which peaked in August.

Manufacturing was again highly targeted, garnering 21 percent of all attack activity. GTIC researchers expected a higher level of attacks within this industry, as manufacturing saw a significant (33 percent) uptick in reconnaissance activity during the previous quarter.

Overall, much of the attacks NTT Security sees show that attacks and attack sources are not static. Attacks change as attackers use different sources and techniques and take advantage of different vulnerabilities. With a sustained focus on Apache Struts, NTT Security observes an attack vector in which GTIC researchers expect to see continued exploitation. And, while many of the details change, if trends from previous years repeat, NTT Security expects both attacks and malware to continue to increase throughout Q4 '17.

About GTIC

The NTT Security GTIC protects and informs NTT Security clients through security threat research, vulnerability analysis and the development of effective countermeasures. For more information, including vulnerability disclosures[25] and threat reports[26], visit the research page on www.nttsecurity.com, our blog[27] or download related whitepapers[28].

About 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.

About NTT Security

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

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

For sales inquiries, please visit:
dimensiondata.com, www.ntt.com/en/index.html, www.nttdata.com/global/en/ or speak to your NTT account representative for more information.

[25] https://www.solutionary.com/threat-intelligence/vulnerability-disclosures/
[26] https://www.solutionary.com/threat-intelligence/threat-reports/
[27] http://www.solutionary.com/resource-center/blog/
[28] http://www.solutionary.com/resource-center/white-papers/