Global Threat Intelligence Center (GTIC) Quarterly Threat Intelligence Report

NTT Security

2017 Q2

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, security professionals and analysts, spanning the last three months. In addition to a wide variety of open-source intelligence tools and honeypots, GTIC – Threat Research (TR) 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 actual 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)

In previous editions of the GTIC Quarterly Threat Report, NTT Security analysts have focused on the retail, financial and health care industries, providing a glimpse into cyber threats unique to each industry. This issue focuses on several threats the manufacturing industry is facing. And, although the manufacturing industry covers an incredibly broad list of segments, this report addresses several common denominators across the board.

While not typically thought of as highly 'attackable,' manufacturing has been one of the most consistently attacked industries over the past several years. And, in addition to potential threats unique to manufacturers, the industry also faces a variety of threats, prevalent across many industries, including insider and technical threats. This quarterly report takes a closer look at some of these problems.

Quarterly Highlights

NTT Security

During the second quarter of 2017 (Q2 '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

- Overall, NTT Security observed a 24 percent increase in attacks against our clients during Q2 '17 over the previous quarter.
- Based on NTT Security client data, cyber criminals appear to be leveraging phishing emails with malicious attachments containing PowerShell commands in VBA macros as a primary attack vector.
- 67 percent of all malware distribution in Q2 '17 was email-based.
- Public-facing Microsoft SQL (MSSQL) servers were popular targets for brute-forcing by cyber criminals during Q2 '17.
- Web application attacks accounted for 21 percent of all attacks. 60 percent of those were SQL and PHP injection-based.
- Vulnerabilities allowing code execution accounted for 73 percent of attacks.
- Activity against Adobe Flash Player vulnerabilities accounted for 98 percent of all activity targeting Adobe products.
- Five out of the Top 10 most hostile countries were new to the Top 10 since the fourth quarter 2016 (Q4 '16).

Attack Profile of the Manufacturing Industry

- The manufacturing industry was the most heavily targeted industry across NTT Security clients during Q2 '17, accounting for 34 percent of attack activity.
- The manufacturing industry was also heavily targeted across NTT Security client networks throughout 2016, appearing in the "top three" in five of the six geographic regions. No other industry appeared in the top three more than twice.
- 58 percent of malware distribution in manufacturing environments was via web-based downloads.
- 86 percent of malware in the manufacturing industry were variants of Trojans and droppers.
- Reconnaissance accounted for 33 percent of all activity aimed at manufacturing clients in Q2 '17.

Apache "Struts" its Stuff

- NTT Security detected attacks for Apache Struts, CVE-2017-5638, less than 48 hours after the initial Apache advisory, and less than 24 hours after the release of proof-of-concept (PoC) code.
- Apache Struts became a "top five" attack type within about a week of being initially detected, and at the end of June, was still a "top seven" attack.
- 76 percent of all attacks targeting Apache Struts originated from IP addresses in China.
- 69 percent of Struts attacks from China attempted to disable local firewalls and install malware from remote servers, mostly located in the United States, China and South Korea.
- In the U.S., the most targeted industries of attacks against Apache Struts were education (37 percent) and health care (28 percent); in Japan, the most targeted industry was government (46 percent).

Introduction

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

Analysis shows the top five industries targeted were manufacturing, finance, health care, business services and technology. Manufacturing was the most heavily targeted industry, with 34 percent of attacks.

A Closer Look at Attacks Against Manufacturing Industry

Since clients in the manufacturing industry were targeted in 34 percent of all malicious cyber activity, NTT Security analysts focused on the threats in this industry.

Top Targeted Industries

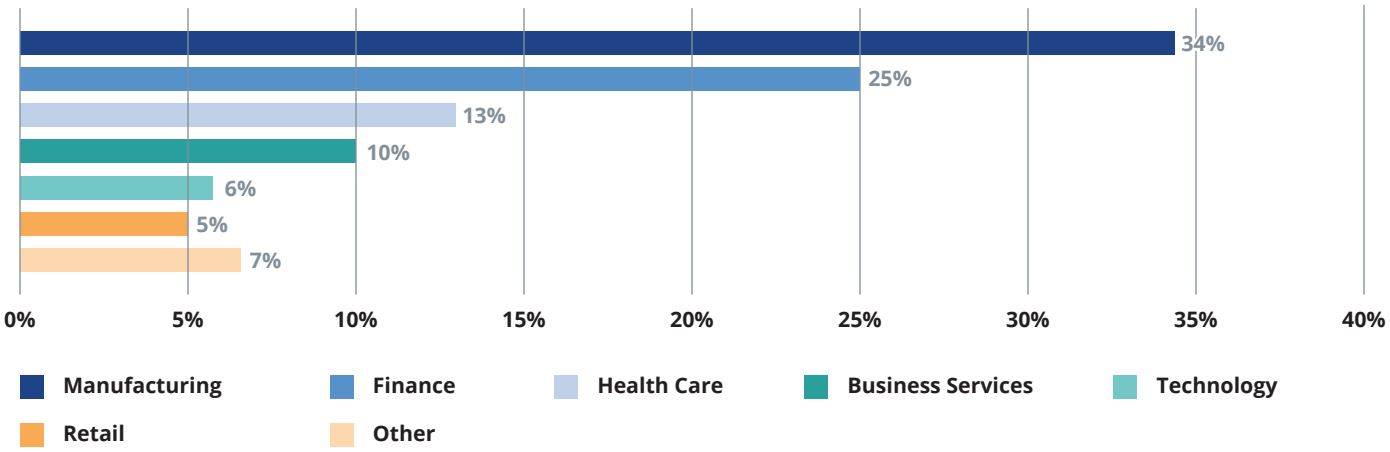


Figure 1. Q2 '17 top targeted industries based on attack volume.

Manufacturing Attack Timeline

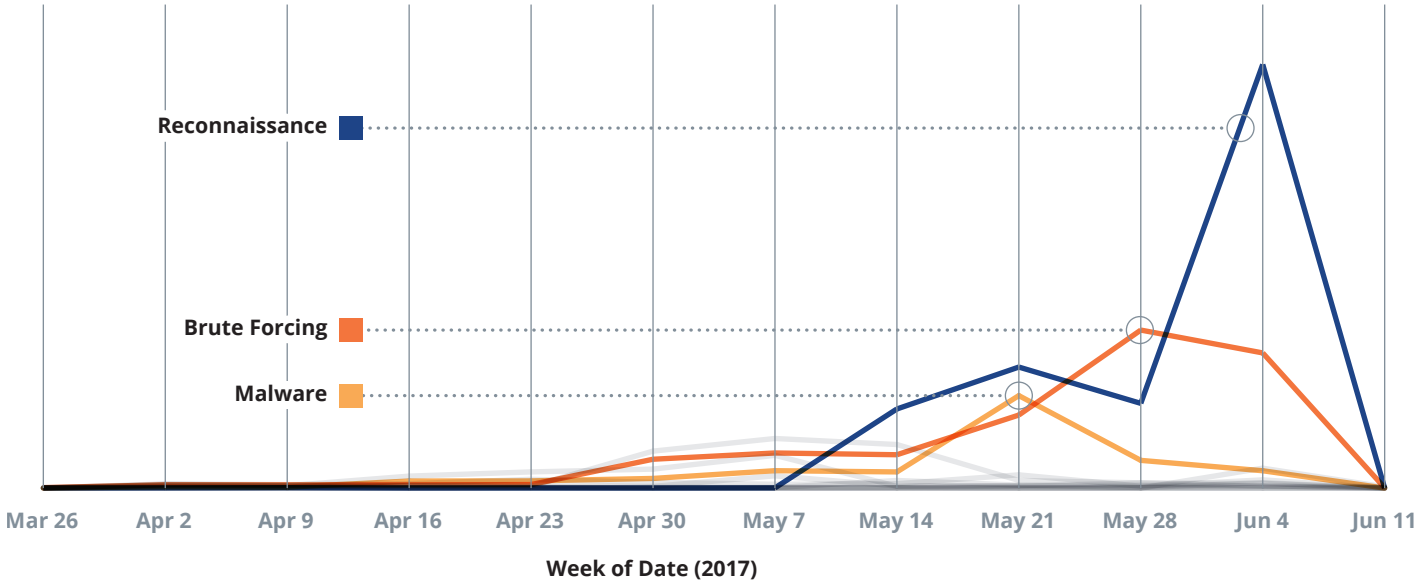


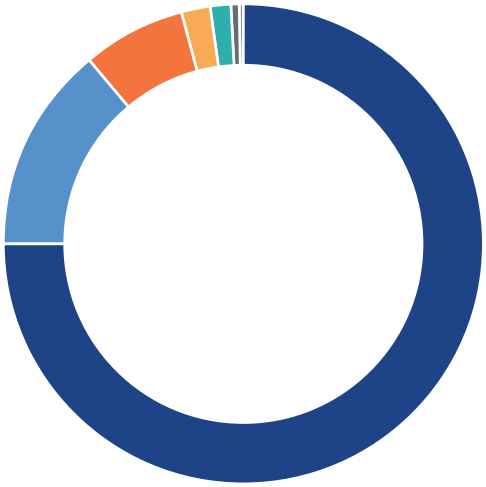
Figure 2. Attack category timeline against manufacturing.

The top three attack categories in the manufacturing industry were: reconnaissance (33 percent), brute-force attacks (22 percent) and malware (nine percent). **Figure 2** shows lower activity against manufacturing throughout April, before several spikes occur in May and June. While there was a general increase in activity against manufacturing organizations throughout the quarter, the most significant increase in malicious activity was related to these three categories.

Reconnaissance Against Manufacturing

Reconnaissance accounted for 33 percent of all activity aimed at manufacturing clients in Q2 '17. Analysis suggests cyber criminals used several different popular scanning tools such as ZmEu, Metasploit and Muieblackcat to scan public-facing systems. These tools come equipped with several plugins, allowing for even beginner cyber criminals to scan and find vulnerabilities in systems and applications. NTT Security identified the intended purpose of recorded reconnaissance traffic as shown in **Figure 3.**

Manufacturing Reconnaissance Targets



75.0% PHP Applications
14.0% DNS Servers
7.00% SNMP or ICMP Protocols
2.00% Web Servers
1.25% All Others
0.70% WordPress
0.05% NetBIOS Ports

Figure 3. Targeted applications of reconnaissance traffic based on volume.

As shown, PHP-based applications accounted for 75 percent of all reconnaissance efforts against the manufacturing industry. A majority of this traffic was via the use of ZmEu and Muieblackcat scanning tools, which scan for vulnerabilities in common PHP files and plugins behind web applications and content management systems (CMS) like WordPress. In 2016 WordFence[1] conducted a survey which indicated roughly 56 percent of all hacked WordPress sites were compromised via exploited plugins. The phpMyAdmin plugin was developed to simplify database administration, is the front-end to MySQL databases, and a popular target to gain full access over a database. Although these scans are common, they can be effective if web applications, websites, etc. are not configured following best security practices. This becomes a larger issue if the website or web server being used in a manufacturing organization sets up the web server in a "security unaware" manner, or does not apply automatic updates potentially leaving the company or organization blind to its vulnerabilities.

The following vulnerabilities associated with PHP applications were targeted in both reconnaissance and exploitation efforts against the manufacturing industry.

CVE	Product	Version(s)	CVSS	Result of Exploitation
CVE-2015-2208	phpMyAdmin	1.1.2	7.5	Remote Code Execution
CVE-2012-1823	sapi/cgi/cgi_main.cin PHP	< 5.4.2	7.5	Remote Code Execution
CVE-2012-2311	sapi/cgi/cgi_main.c	< 5.4.3	7.5	Remote Code Execution

Table 1. Top three targeted PHP vulnerabilities via reconnaissance and exploitation efforts against the manufacturing industry.

[1] https://www.wordfence.com/blog/2016/03/attackers-gain-access-wordpress-sites/

Brute-forcing Manufacturing Systems and Applications

Brute-forcing traffic accounted for 22 percent of all attacks against the manufacturing industry. NTT Security focused on the server/application targets of this traffic, discovering FTP servers were of highest interest at 64 percent, followed by HTTP (18 percent) and SSH (11 percent). Figure 4 shows manufacturing brute-force target volumes for Q2 '17.

Per **Figure 4**, although FTP and HTTP had several large spikes for brute-force attempts, MSSQL was consistently targeted with several thousand events each day in April, May and June across multiple clients. MSSQL is a relational database management system (RDBMS) which is a popular target in manufacturing in terms of brute-forcing. NTT Security discovered thousands of public-facing MSSQL servers with default port 1433 open. **Figure 5** shows a simple Shodan query for public-facing MSSQL servers. These queries reveal important details to an attacker such as server name, instance name, version, and port used. Combine this readily available information with a generic brute-forcing tool, and the return on investment for a cyber criminal could be exponential. In January 2017, thousands of public-facing MongoDB databases were compromised[2] and held for ransom by cyber criminals. Not long after, CouchDB and Hadoop Servers were compromised[3] using the same attack process. For this reason, it is not only best-practice, but essential that databases/servers not be public-facing and not have default credentials and/or ports to defend against brute-force attacks.

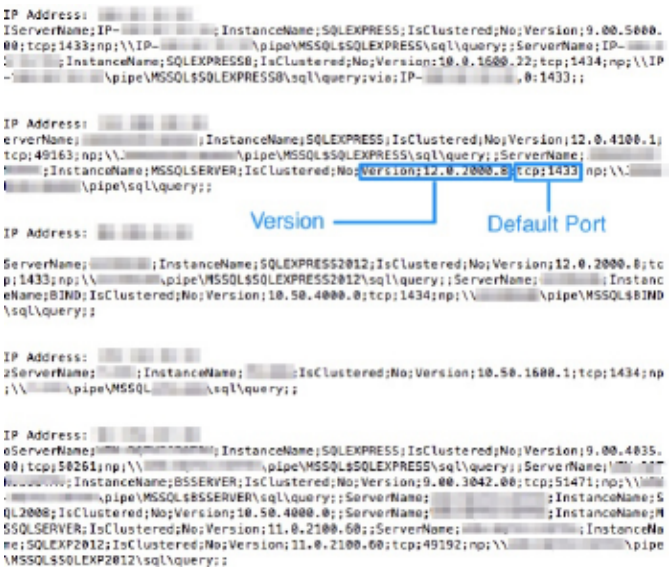


Figure 5. Simple query using Shodan's API for public facing MSSQL servers.

Manufacturing Brute-Force Targets

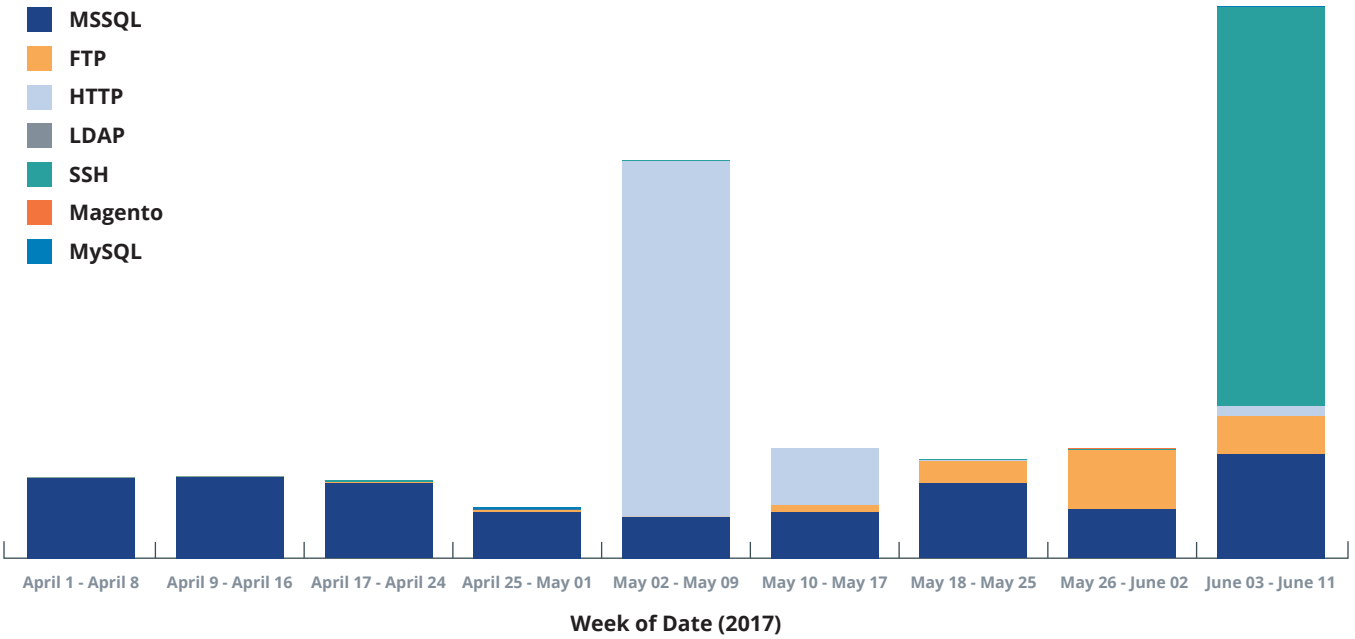


Figure 4. Manufacturing brute force target attack volume.

[2] https://nakedsecurity.sophos.com/2017/01/11/thousands-of-mongodb-databases-compromised-and-held-to-ransom/
[3] https://www.bleepingcomputer.com/news/security/database-ransom-attacks-hit-couchdb-and-hadoop-servers/

Malware in the Manufacturing Environment

NTT Security discovered 86 percent of malware in the manufacturing industry were Trojan/dropper variants; in other words, software or applications which drop additional malicious binaries whether they appear to be legitimate or not.

NTT Security analyzed the distribution efforts for delivering malware to systems in the manufacturing industry. The most common technique used to distribute malware was drive by downloads. **Figure 6** shows malware distribution efforts throughout Q2 '17 in the manufacturing industry. In addition to the data shown in the chart, NTT Security detected a small volume of attempted malware distribution via email against the manufacturing industry. Since this typically amounted to less than a few attempts per day, it does not display well in Figure 6.

Fifty-eight percent of malware distribution in manufacturing environments was via web-based downloads. Web-based downloads resulting in malware installations via the web could occur when one of the following conditions exist:

- Visiting a compromised website which directly provides the malicious content, or
- Visiting a compromised website which has malicious content provided to it, for example, via malvertising.

NTT Security MSSP data indicates that cyber criminals often rely on web resources to deliver malware to the manufacturing industry.

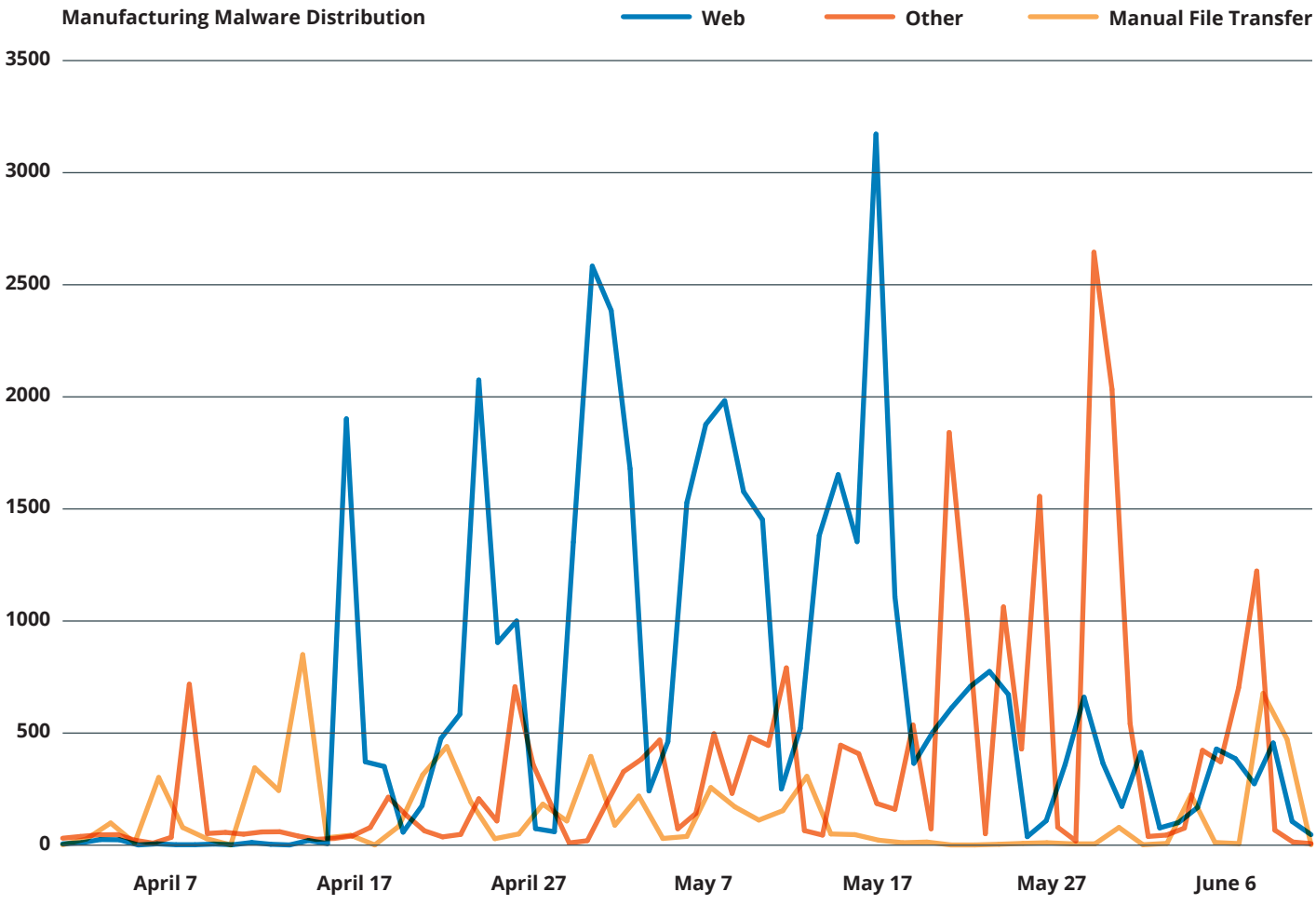


Figure 6. Malware distribution efforts in the manufacturing industry in Q2 '2017.

Attack Category Volume

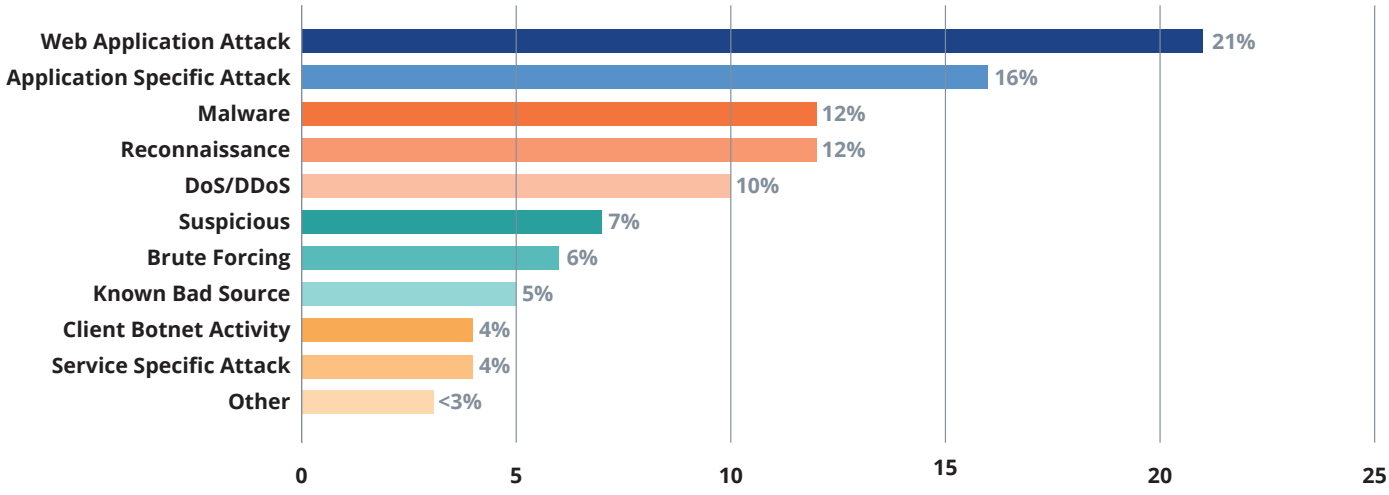


Figure 7. Attack category volume.

Attacks by Type

NTT Security analysis indicates 21 percent of all attacks across all industries were web application focused, followed by application specific (16 percent) and malware (12 percent) based attacks. **Figure 7** depicts a simple bar graph for the representation of these findings.

Web Application Attacks

As stated, 21 percent of all attacks were against web applications. Sixty percent of these attacks were injection-based. This includes, but is not limited to, SQL and PHP-based applications as well as including arbitrary commands in HTTP packets to be executed on the target server.

A Closer Look at Web Injections

While it is common to observe and detect SQLi against public facing devices, NTT Security identified several types of web injections in Q2 '17; this includes, but is not limited to, PHP-based applications, LDAP, and HTTP.

PHP-based Injections

With thousands of libraries, PHP is one of the most commonly used server-side programming languages. According to W3 Techs[4], PHP is deployed on about 83 percent of web servers. As developers continue to introduce vulnerabilities into applications, threat actors will continue to target PHP-based applications. Based on NTT Security observations, command injection attempts against PHP-based applications gained popularity as a specific type of web application attack in Q2 '17.

The primary goal of these attacks is arbitrary code execution, the execution of machine code on a target machine or target process typically leveraged after exploiting a vulnerability. The execution of arbitrary code allows the cyber criminal to tell the machine or process what to do. **Figure 8** shows web application injection targets according to MSSP data. NTT Security discovered a majority of the SQL-based injections were generic and likely being generated via common tools such as Havij or sqlmap, which tend to be noisy. Meanwhile, PHP-based injections are usually more focused, and based on the application or vulnerability being targeted.

Web Application Injection Targets

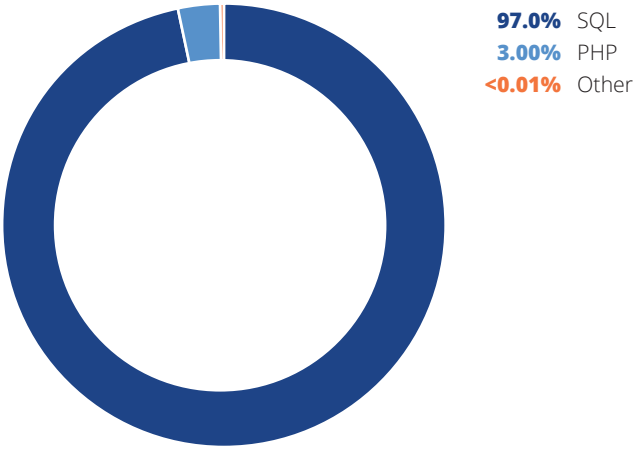


Figure 8. SQL-based injections versus PHP-based injections.

[4] https://w3techs.com/technologies/details/pl-php/all/all

Q4'16 and Q2'17 Malware Variant Comparison

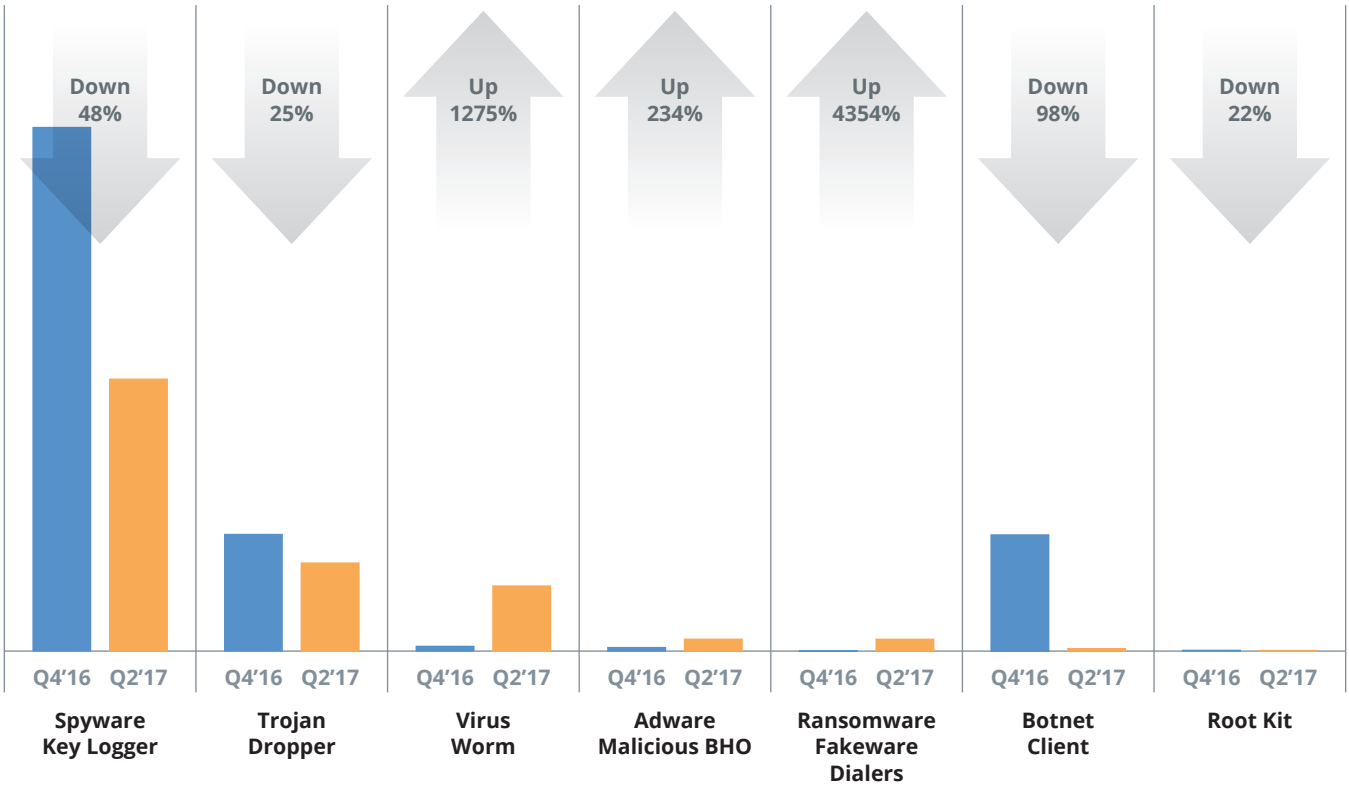


Figure 9. Attack volume differences in malware variants between Q4 '16 and Q2 '17.

Analysis of Malware Detections

NTT Security analysts analyzed the differences in malware variants between Q4 '16 and Q2 '17.

Overall, malware detections dropped 41 percent between Q4 '16 and Q2 '17. As shown in **Figure 9**, Virus/Worms, Adware, and Ransomware all increased in Q2 '17 while the volume of other malware variant detections fell.

NTT Security observed that malware campaigns commonly combine phishing emails with a malicious attachment containing embedded VBA macros. These macros often contain obfuscated PowerShell commands, used to download the final malware payload. While analyzing MSSP data, NTT Security observed 67 percent of all attempted malware distribution was through email. Please note these statistics do not include successful versus unsuccessful malware installations. **Figure 10** details these findings.

Q4'16 and Q2'17 Malware Variant Comparison

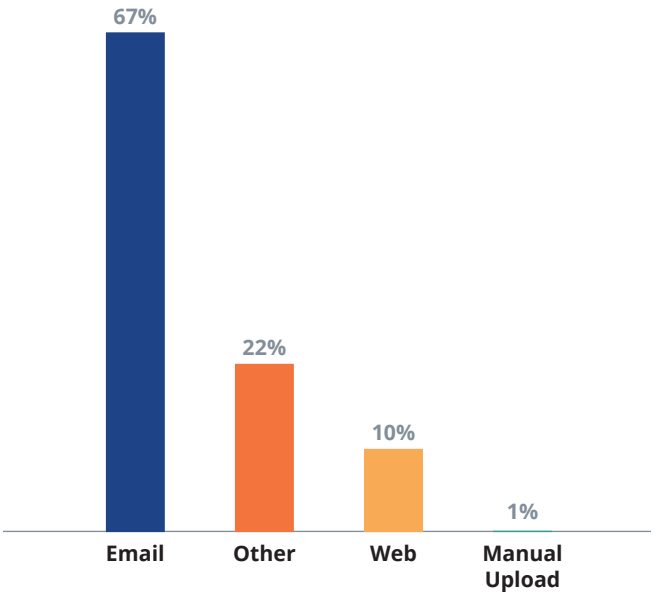


Figure 10. Malware distribution across all industries.

For example, while analyzing the malware category, MD5 hash e5f6bf18b4b8024c0fd3e17595e8fb36[5] was discovered in several logs for NTT Security clients. This was the hash of a malicious Excel file sent in a phishing email with the file name "FW 20-05-17 Dokument - VAT I.xls." At initial glance, the document seemed harmless, however, as shown in **Figure 11**, analysis of one of the two embedded VBA macros detailed obfuscated code.

Several strings in each variable value were backwards or represented by ASCII numbers. Variables *epitiimsor* and *marvells* were both obfuscated in the same manner, but once decoded and combined, they revealed a PowerShell command used to deliver Windows malware.

NTT Security expects the continued use of phishing attacks with documents containing embedded VBA macros will occur where attackers use a mix of Windows tools such as PowerShell, Windows Management Instrumentation Command-Line (WMIC), or PsExec to download the malware payload. This technique is effective and distribution can be automated to increase the likelihood of successfully compromising victims.

Figure 11. _VBA_PROJECT_CUR/VBA/ThisWorkbook Source Code.

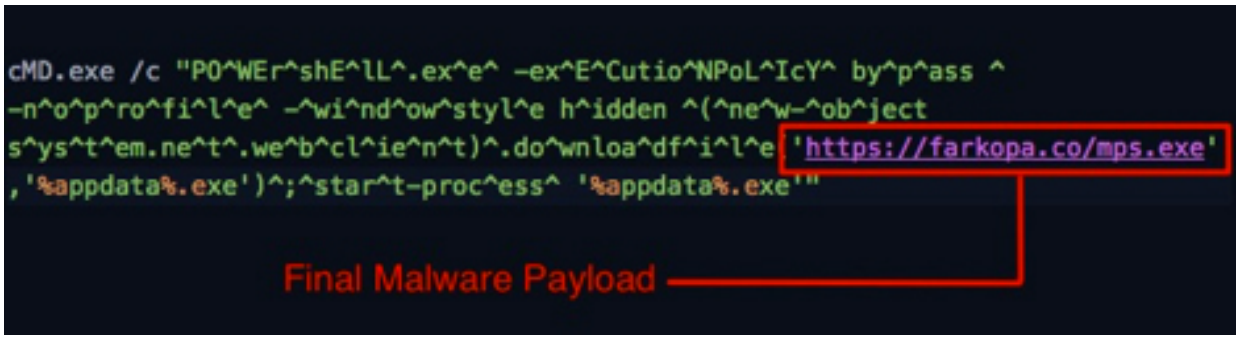


Figure 12. Deobfuscated PowerShell command to retrieve mps.exe (365c4b6e651034daaebd4363efa4b0f)[6].

[5] https://www.virustotal.com/en/file/e3fff8975c852e6a7e4909033a2dec9c1c7ae794be2dd0e45398a6541293101b/analysis/
[6] https://www.virustotal.com/en/file/96c8aea7d0f65dfc41ccaf5384abfe19d5ea0f1f1e9c6359ae985932ac4db1e8/analysis/

Attacks by Source

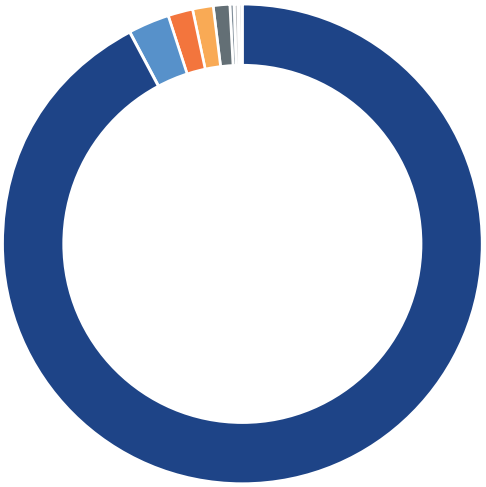
NTT Security analysts reviewed the top countries hosting systems which generated malicious traffic between Q4 '16 and Q2 '17.

During Q2 '17, two countries stood out due to the pattern or uniqueness of activity. Over the past few years, the infrastructures located in France and the Netherlands have improved significantly. Each offers a wide range of services to support individual and specific needs, including telephony, hosting, cable, and in some cases, all the above. The hosting and virtual private server (VPS) market has created a surge in affordable offshore hosting. Threat actors are starting to migrate and or exploit vulnerable servers in these two countries more and more. Regardless of the actor's purpose or reasoning, they will continue to use and exploit vulnerable services.

France

France accounts for 47 percent of hostile attack traffic, most of which appears to be probing or scanning-related activities. However, monitoring data includes multiple examples of exploit and unauthorized access attempts. The largest cluster of exploit events is associated with Online S.A.S., a major telecommunications entity providing internet access to France, Netherlands and possibly other EU countries, as this provider continues to expand its reach. Some of the servers appear to be running Nginx and or other proxy configurations. Because of this, it is likely the true attackers are operating from other locations. This type of activity will likely increase, as few provisions are historically taken by the users and Tier 1 providers to remedy the situation by securing users and enforcing policies. Overall, **Figure 13** displays the top ten attacks originating from France. Reconnaissance activity is the most common, at 93 percent of all detected activity.

France Attack Categories



93%	Reconnaissance
3%	Known Bad Source
<1%	Brute Forcing
<1%	DoS/DDoS
<1%	Web Application Attack
<1%	Application Specific Attack
<1%	Malware
<1%	Suspicious
<1%	Client Botnet Activity
<1%	Service Specific Attack

Figure 13. Top ten attacks originating from hosts in France.

Change	Rank Q4 2016	Rank Q2 2017	Attack Source	% of Attack
▲	5	1	France	47%
▲	8	2	Netherlands	8%
◀ ▶	3	3	China	6%
▲	>20%	4	Brazil	4%
▼	1	5	United Kingdom	4%
◀ ▶	8	8	Canada	4%
▲	>20%	7	Germany	3%
▲	>20%	8	Chile	1%
▲	>20%	9	Puerto Rico	1%
▲	>20%	10	Hungary	1%

Table 2. Top non-U.S. attack countries.

Attack Categories from Hosts in Netherlands

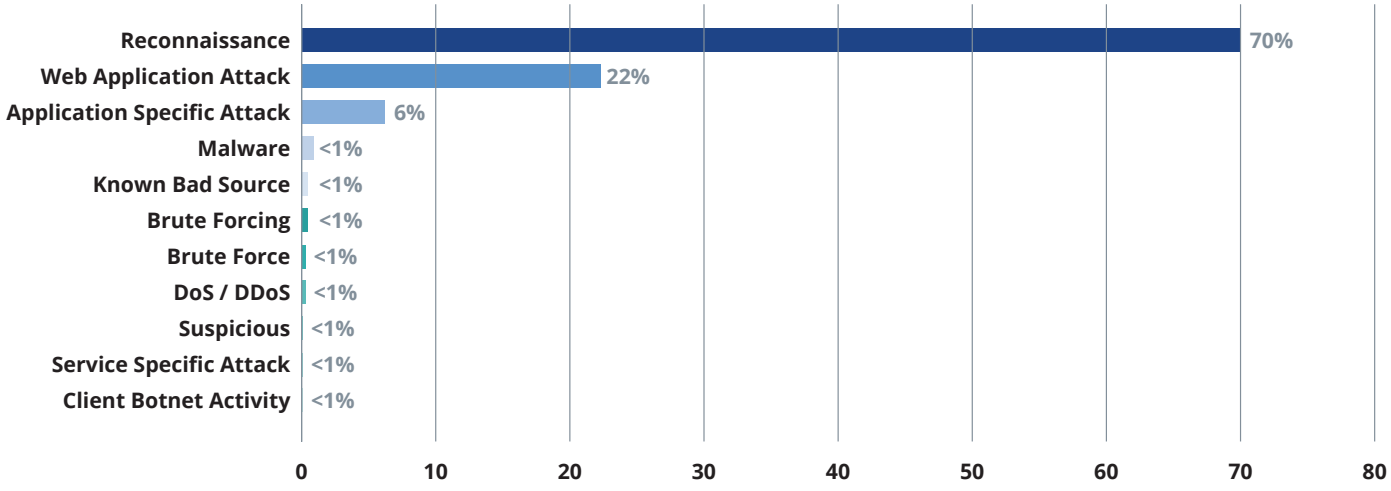


Figure 14. Top Ten Attacks Originating from Hosts in Netherlands.

Netherlands

The Netherlands came in a distant second. Unlike France, whose traffic originated from multiple ISP/providers, sources in The Netherlands originated from only three IP addresses allocated to KPN B.V., a Dutch-based telecommunications company providing internet and mobile phone access. Based on the event data, a three-day initiative from two of these IP addresses targeted a single victim in the manufacturing industry. Activity from 145.129.22[.] 220 accounted for 75 percent of the activity; 25 percent was from 145.129.21[.]42. Activity from the third IP address was ultimately insignificant. Their primary goal was host and network discovery via DNS zone transfers. Zone transfers can disclose a large amount of information about a network and organization, depending on the resource records (RR) being used and host nomenclature.

Overall, **Figure 14** displays the top ten attacks originating from Netherlands, showing that reconnaissance was the most commonly detected attack type with 70 percent of all hostile activity.

Top Targeted Vulnerabilities

During Q2 '17, code execution-based vulnerabilities accounted for 73 percent of the top attacks. The top three CVEs listed in **Table 3** were most popular.

These vulnerabilities were observed being exploited from sources in 68 countries. The most prolific attempts originated from China, Poland and France. This trend spanned across 15 industries with manufacturing and finance as the top two affected, and technology as a distant third place. In a change from previous analysis, the telecommunication industry was targeted relatively lightly during Q2 '17. The exception to this was a small subset within telecommunications, specifically businesses that provide hosting or other connectivity services, which were highly targeted by attempts to exploit vulnerabilities in Apache Struts and Bash (Shellshock).

CVE	Event Percentage	Target/Campaign
CVE-2016-4116	57%	Adobe Flash
CVE-2017-5638	24%	Apache Struts
CVE-2014-6271	10%	ShellShock
CVE-2017-0147	3%	WannaCry (EternalBlue)
CVE-2009-0183	3%	Free Download Manager
CVE-2011-3230	3%	Safari Exploit

Table 3. Code execution target-campaign event percentage.

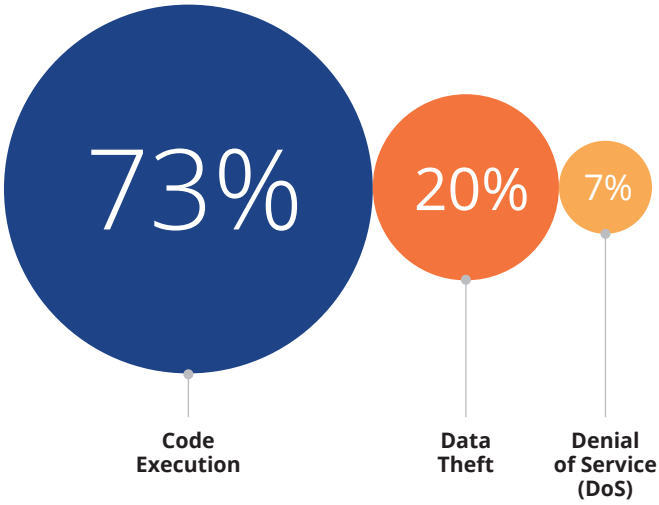


Figure 15. Attack method visualization according to CVE.

The identified CVEs in the top-ten can be categorized into three attack methodologies:

- code execution
- data theft
- denial of service (DoS)

Adobe Flash Exploits

Signatures for CVE-2016-4116 triggered on specific port traffic used to laterally move files. Flash has been, and will for the foreseeable future, continue to be a highly-targeted product due to its widespread use across multiple operating systems, and its history of vulnerabilities. In comparison to other Adobe products, Flash accounted for a staggering 98 percent of all Adobe-based vulnerability events. Of that total, the most targeted vulnerability was CVE-2016-4116.

Adobe Product	Event Percentage	CVE Total
Flash Player	98.40%	14
Adobe AIR	1.30%	2
Acrobat Reader	0.10%	5
Air SDK	0.10%	1
Acrobat	0.10%	4

Table 4. Top five Adobe Flash Player vulnerabilities being targeted.

Apache Struts, ShellShock and WannaCry

There is a reason why attackers from each of the top countries consistently target these vulnerabilities. Each can be used to gain access or remotely control Windows and Linux-based systems. The exception is WannaCry which utilized the EternalBlue exploit, and specifically targets Windows systems. The success of exploiting these vulnerabilities is dependent on the premise that many vendors and administrators have not patched, updated systems or taken additional precautions. Until industry improves the consistency and regularity with which they update systems, such attacks will continue. NTT Security analysts observed the CVEs associated with these now infamous names trending across fifteen industries. The heaviest concentration of this activity was in the manufacturing and finance industries.

Financial institutions can lose millions of dollars as a result of money stolen from accounts, or money paid for ransomware. Manufacturing can lose just as much from theft of product ideas, and intellectual property sold to competitors. All the industries on the list have valuable information to protect.

Industries Targeted with Top 10 CVEs

29% Manufacturing
26% Finance
8% Technology
8% Health Care
7% Non-Profit
7% Construction/Real Estate
6% Retail
9% Other

Figure 16. Industries targeted via the top 10 CVEs.

Global Threat Visibility: Final Thoughts

NTT Security analysts observed a small overall increase in detections in Q2 '17. The first half of 2017 included a heavy focus on manufacturing and the distribution of malware through large phishing campaigns. Web applications based on PHP continue to be a popular target by hackers who understand the lack of security implementations into plugins and applications. As brute-forcing continues to be popular, NTT Security analyzed several brute-forcing attempts against public MSSQL servers with default ports and out-of-date versions. This should be an important reminder to not allow RDBMS and databases to be public-facing, as attackers focus more on the monetization of ransom-style attacks. As Adobe Flash Player remains to be riddled with RCE vulnerabilities being targeted by cyber criminals, it is crucial to understand drive-by and web-based attacks continue to be prevalent; targeting not only unpatched servers, but common web visitors in the organization, including the organization's employees and clients. With recent attacks involving a Petya variant, WannaCry, Trickbot and others, NTT Security predicts cyber criminals will continue to support their efforts with phishing campaigns throughout 2017 to deliver ever more robust malware. After analyzing attacks from hosts in several countries, it is evident compromised hosts in countries which typically fly under the radar – such as the Netherlands – are coming back into the spotlight. NTT Security expects this trend to continue as these countries build their infrastructure, which could become compromised and leveraged in future cyberattacks.

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

- Conduct regular vulnerability scans and penetration testing to identify vulnerabilities.
- Always take a defense-in-depth (DiD) approach to security controls, including defining internal segmentation and segregation, which increases the complexity for cyber criminals to become more successful during attacks.
- Establish an Incident Response Team supported by formal and documented processes and procedures.
- Enforce effective patch management through both automated and manual processes to ensure necessary software and hardware patches are applied, mitigating successful exploitation attempts.
- Consider whitelisting approved applications.
- 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.

> "Most manufacturing systems today were made to be productive — they were not made to be secure. Every manufacturer is at risk — it isn't a matter of if they will be targeted, it's a matter of when."
>
> **Rebecca Taylor, Senior Vice President for NCMS**

The cost of cybercrime to businesses is expected to reach $6 trillion annually by 2021[7]. Globally, the manufacturing industry is now one of the most frequently attacked industries, second only to health care, making potential losses in this industry catastrophic.

The manufacturing industry is increasingly being targeted, as threat actors perceive the prospective gains in attacking networks in this industry. Per the National Center for Manufacturing Sciences (NCMS), 33 percent of all cyberattacks in 2015 were against the manufacturing sector. In 2016, 39 percent of manufacturing firms said they'd been breached, with breaches costing between $1-10 million. This trend will certainly continue.

Targeting of the manufacturing industry was also seen in NTT Security client data over the last year. The most recent NTT Security Global Threat Intelligence Report (GTIR)[8] showed the manufacturing industry was heavily targeted across client networks during 2016, appearing in the top three targeted industries in five of the six geographic regions evaluated. No other industry appeared in the top three more than twice. Manufacturing was the most attacked sector in Africa and the Americas, and the second most attacked sector in Asia (32 percent, trailing only finance), so geographic areas with significant manufacturing capabilities are seeing the impact of this focus.

This trend continues into 2017. In fact, the manufacturing industry was the most heavily targeted industry across NTT Security clients during Q2 '17.

Global estimates, across all industries, of losses in the trillions of dollars over the next five years are not surprising given the threats industries across the globe face daily, particularly threats to the manufacturing industry, which are becoming progressively more difficult to defend against, as technology and connectivity continue to increase at an astounding rate.

The industry itself covers an incredibly broad range of organizations: fabrics and textiles, food products, construction materials, pharmaceuticals, plastics, metals, computer components, automobiles, just to name a few. The reasons for any given segment to be targeted are innumerable – from intellectual property (IP) theft to espionage to using a firm as a stepping stone for further targeting (for instance, if a targeted manufacturing firm is in the supply chain of another firm or government organization).

What other factors make the manufacturing industry more susceptible to being targeted by hackers, cyber criminals and other threat actors? Is the industry fundamentally more vulnerable?

What Makes Manufacturing an Attractive Target?

Rebecca Taylor, Senior Vice President for NCMS, says, "Most manufacturing systems today were made to be productive – they were not made to be secure. Every manufacturer is at risk – it isn't a matter of if they will be targeted, it's a matter of when."

Intellectual property is at a premium, and in a market where fractions of market shares can mean millions – or billions – of dollars, competition is fierce. Industrial control systems (ICS) are often left unguarded, and worse yet, they are often built with little to no thought for security, sometimes making protection of the device itself impractical. There is a lack of investment in cybersecurity, as funds are being spent upgrading systems to be more productive or more efficient. In fact, almost half of top

[7] http://cybersecurityventures.com/cybersecurity-market-report/
[8] https://www.nttsecurity.com/en/what-we-think/gtir-2017/

executives in manufacturing firms neither feel confident in their technology to protect their networks, nor do they feel they have adequate funding.

And, connectivity is increasing. From Internet of Things (IoT) and Operational Technology (OT) devices to robotics to human-machine interfacing (HMI), this connectivity is improving automation, and, subsequently, cutting costs and increasing productivity. Unfortunately, this increases the attack surface. Many industries incorrectly believe "it can't happen to us. We don't have vast amounts of consumer data, health records, or credit card information. We just make 'widgets.'"

While the above line of thought may be the first inclination, remember that, year after year, the manufacturing industry has consistently been one of the top most frequently targeted industries.

Consider the consequences of a breach: fewer 'widgets' to sell, competitors gaining insight into your widget production processes or proprietary widget innovations, cyber criminals demanding a ransom to decrypt this same information or foreign nations using this same information to undercut a major bid. This could translate into decreased productivity, increased network down time, and, ultimately, a decrease in profits. How much decrease in "X" can your organization afford?

There is no question that cyber criminals are looking to capitalize on this highly attackable industry. Others may want to damage a firm's brand and reputation, perhaps to benefit their own.

But cyber criminals and competitors aren't alone in targeting those in this industry, as nation-state actors are doing the same.

Per China's newest Five Year Plan (FYP), the Chinese government continues to prioritize significant efforts within the manufacturing sector through 2020. In early December 2016, China released its newest FYP for intelligent manufacturing in attempts to increase its competitiveness in the "factory of the world," a long-term strategy to generate new growth in the country's manufacturing sector.

> ...year after year, the manufacturing industry has consistently been one of the top most frequently targeted industries.

Additionally, "Made in China 2025" targets ten key segments of the industry for additional government support:

- New energy vehicles
- Next-generation information technology (IT)
- Biotechnology
- New materials
- Aerospace
- Ocean engineering and high-tech ships
- Railway
- Robotics
- Power equipment
- Agricultural machinery

Chinese cyber actors have attacked industries listed in the FYP in the past, primarily to accrue IP and other data. Those segments identified as priorities for research and development can expect continued interest from these actors. Based on experience with attacks from China over the past several years, NTT Security expects these types of attacks to continue in all industries, but particularly in manufacturing.

Trends – and Associated Emerging Risks – in the Manufacturing Industry

In this rapidly changing industry, a top priority is cutting operational costs, while manufacturers leverage technology to ensure future growth.

Manufacturing organizations have taken on a much more widely-distributed environment and infrastructure. Increasing numbers of users and devices will greatly increase the number of avenues into your network from threat actors – from cyber criminals to nation-state actors.

[9] http://www.eweek.com/security/deloitte-survey-finds-manufacturers-highly-vulnerable-to-cyber-threats
[10] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_

The industry has become more vulnerable due to its focus on technological advances, while not investing as heavily in the cybersecurity budget as in other priorities. This is not to say that the industry is ignoring security, rather that the investment in technology and enabling services has taken a priority. As a result, cybersecurity may have taken a backseat. This holds true not only in the manufacturing industry, but in many sectors. In fact, the Cyber Security Breaches Survey 2017[10] , published earlier this year suggests manufacturers are less likely than many other industries to rate cybersecurity as a serious priority. Just 31 percent of firms in the manufacturing industry regarded cybersecurity as a high priority. In contrast, 61 percent in the financial sector held cybersecurity as a high priority, along with 49 percent in both the health care and education sectors. To some extent, this is understandable. Anyone can look at the data and think that "personal health care information" and "card holder data" are more sensitive than "widgets," right?

Operational Technology and "Smart Factories"

Perhaps the most influential of all trends results in one of the greatest emerging cyber threats to the manufacturing industry: smart factories. Hoping to add efficiency, productivity, quality of products and flexibility to the process, connected – or "smart" – factories are expected to add $500 billion to the global economy in the next five years, adding yet another avenue for threat actors to target the manufacturing industry.

This connectivity is expected to drive a 27 percent increase in efficiency during that timeframe, and by the end of 2022, manufacturers expect that 21 percent[11] of all factories will be fully connected. But all these additional tools, devices, and robots are redefining the attack surface in the manufacturing industry. Despite the benefits of connected devices, this creates an environment with a continually broadening attack landscape due to endpoint expansion. As these devices multiply, they can become crucial access points for an attacker to infiltrate a network, or become pawns in a botnet or even be victims of ransomware themselves. Simply put, the more systems you have, the more likely it is that an attacker is going to find something "interesting" in your environment.[12]

The rise of the OT also plays a critical role in integrating manufacturing processes, improving productivity and efficiency, so long as these technologies are properly secured. Integration efforts vary widely by industry segment. For example, 67 percent of industrial manufacturing and 62 percent of aerospace and defense organizations have begun to implement smart factory initiatives, while only 37 percent of pharmaceutical manufacturers are leveraging digital technologies.

Industry 4.0: Automation, Connectivity and Servitization

Manufacturers are amid one of the most exciting technological changes in history, known as the fourth industrial revolution, or Industry 4.0. The capabilities – and challenges – represented by connectivity via IoT and OT, robotics and automation offer manufacturers the opportunity to operate more efficiently and effectively, developing new business processes, such as servitization, (essentially, the evolution of an organization's capabilities to better create mutual value through a shift from selling product to selling Product-Service Systems), all taking customer service to a new level.

21%

of manufacturers have suffered a loss of intellectual property from cyberattacks.

Although some U.S. manufacturers are moving more slowly in adopting Industry 4.0, 75 percent[13] of respondents in a 2017 report feel they have sufficient understanding of the issues and implications of Industry 4.0 and its threats and opportunities. In addition, a significant proportion of respondents were either beginning to move to Industry 4.0 (23%), or were planning to do so (62%). About 66 percent had made further investments in automation in the past 12 months, and most had acknowledged an understanding of servitization.

New Technologies and Reuse of Old Software

As in many industries, and as noted earlier, manufacturing has historically been geared toward meeting its business objectives rather than a quest for greater security. Another symptom of this mentality is that old software is reused (efficiency!), potentially propagating existing security holes.

[11] http://enterpriseiotinsights.com/20170601/smart-factory/20170601smart-factorysmart-factories-economic-value-tag23
[12] http://enterpriseiotinsights.com/20170601/smart-factory/20170601smart-factorysmart-factories-economic-value-tag23
[13] http://www.nass.org.uk/Publications/Publication4261/Annual-Manufacturing-Report-2017.pdf

In addition, organizations are employing new technologies, potentially exposing firms to risks for which they may not yet have fully considered the impact on their security posture. For example, software may be built using open-source code already in existence on shared sites, possibly including some questionable sources, potentially putting an organization in danger if these hosts aren't segmented from the rest of the network. While most of this shared code is safe, not all of it is. With hardcoded backdoors written into software, vulnerability proof-of-concepts in insecure software code, and more available online, the risk that an attacker will use this to his advantage increases.

As mentioned at the beginning of this section, new technologies are increasing the attack surface, and properly securing these technologies is essential to reducing the risk to your organization.

90%

or more of material stolen by "cyber-spies" has been classified as "secret" or "proprietary."

Cyber Espionage and Theft of IP

Twenty-one percent of manufacturers have suffered a loss of intellectual property from cyberattacks.

In its 2016 Manufacturing Report, Sikich[14] cited IP theft as the primary motive behind an attack on a manufacturing organization. To further drive the point home, the FBI estimates that IP worth $400 billion is stolen from U.S firms alone, each year.

Cyber espionage is now considered to be the most common type of attack in this industry. A large part of this is due to the explosion of proprietary data and research.

These types of attacks can take many forms. Most commonly, though, attacks are attributed to competitors trying to obtain IP, whether that IP be proprietary manufacturing processes, patents or designs. Sadly, many international competitors are not highly ethical, viewing cyber espionage as another means to reach their own objectives.

Nation-state actors are heavily immersed in cyber espionage activities, with China dominating the cyber espionage space over the past two decades. Despite the cyber treaty signed in 2015 between the U.S. and China, the threat nevertheless continues, particularly in the manufacturing industry.

Cyber espionage is rampant and is not connected only to nation-state actors. In this global economy, goods can be produced virtually anywhere. If a competitor can steal the research and development behind those goods, then an unethical company, nation or cyber criminal will be able to undercut and win on price. It only costs the unsecured manufacturing firm, and its customers, money.

These attacks by "cyber-spies," and any subsequent breaches, particularly those backed by nation-states, were behind a significant number of breaches experienced by manufacturing firms last year. These attacks are typically highly targeted and well thought out, targeting specific data. Over 90 percent of the material stolen had been categorized as "secret" or "proprietary," indicating that the attackers successfully bypassed security controls currently in place, or simply that this is the type of data threat actors are seeking. That said, many state-backed threat actors have access to zero-days or other sophisticated tools. To combat these threats, manufacturers need to ensure they have, at the very least, best practices employed. Please note that these security shortfalls are not specific only to this industry, but seem to happen on a much broader, global scale.

Despite these emerging threats, the 2017 Cybersecurity Breaches Survey suggests that manufacturers are far less likely than many other sectors of the economy to rate cybersecurity as a serious priority for their organizations; it may be worth restating that just 31 percent of manufacturers regarded cybersecurity as a high priority. Hopefully this trend will reverse itself, as the industry faces huge changes in the coming years, requiring the utmost in network security if manufacturing organizations wish to remain competitive.

Recommendations

A paradigm shift in mindset is essential in all segments of the manufacturing industry and in all parts of the process. To successfully face current and future threats, cybersecurity must be built into all aspects of an organization's networks and operations rather than retrofitted as an afterthought, particularly as Industry 4.0 is implemented. It should be clear that without the proper mitigation efforts in place, all processes are at risk, impacting the bottom line.

[14] https://www.leadingedgealliance.com/thought_leadership/sikich_manufacturing_report_2016r.pdf

An organization greatly decreases the time it takes to bounce back from an attack if the paradigm shift has already occurred. Given the current state of cybersecurity in the manufacturing industry, where defenders are clearly at a disadvantage, attacks may be all but inevitable. With a renewed mindset, organizations in the manufacturing sector can become better equipped and more prepared to react to, and recover from, an attack. This is true for any organization, not just those in the manufacturing industry.

Threat actors and cyber criminals will continue to target victims in two areas: organizations with highly valuable data, and organizations with poor security practices. The manufacturing industry is one of those industries which has historically fallen into both categories. Like any organization, manufacturing organizations can take actions on network/program/software/platform levels to optimize security and reduce your risk of data compromise. If these recommendations can be successfully implemented, the environment can be made more secure in a practical, efficient manner.

NTT Security recommends manufacturing organizations consider the following preventative and mitigation strategies:

- Educate users on identifying and avoiding phishing emails – particularly since employees are the most often targeted, and may be the first – or only – line of defense.
- Ensure computers, network and other internet-connected devices, particularly industrial control systems, are running the most current versions of operating systems and software. Please note that the most current software versions are typically the most secure, but this is not always the case.
- In addition to outside actors, don't forget to secure against the rogue insider – someone trusted within your organization, who perhaps has "the keys to the kingdom."
- Enforce "least privilege" – vary the level of individual access, granted based on specific user needs and scenarios.
- To every practical extent, isolate sensitive systems and network functions. Group associated sensitive functions onto protected networks whenever possible, to include segmenting ICS from other network functions.
    - Industrial networks are often not well segmented between IT/OT, so an infection in the former can easily spread to the latter.
- Let malware such as WannaCry serve as a recent lesson: although the manufacturing industry seemed almost immune to WannaCry, many Windows machines inside ICS environments are not fully patched, and are often running outdated, unsupported versions.

Threats to Manufacturing: Final Thoughts

The manufacturing industry will continue to mature through automation, servitization and Industry 4.0. NTT Security fully expects attacks in the manufacturing industry to continue. As the implementation of technology increases and attacking becomes more profitable, cyber criminals at all levels will continue to view the industry as incredibly lucrative, vulnerable, and attackable. Securing all facets of your organization is essential. Just one opening creates an opportunity for threat actors to gain, and maintain, a foothold in your network.

Expect IoT, OT and automated devices to continue playing an increasing role as manufacturing organizations consider how to harden their security infrastructure to support Industry 4.0 implementation efforts. Manufacturing organizations must maximize the effectiveness of security controls to protect these technologies as they are implemented.

As the number of endpoint devices increases, the attack surface will also increase, putting further strains on already burdened network infrastructure. This will leave many manufacturing firms striving to find ways to simplify and streamline cybersecurity controls.

Analysts anticipate seeing a blending of attack vectors, as the capability and motivation of threat actors increase and adapt to the ever-changing landscape.

This all means that somehow, manufacturing organizations need to force themselves to prioritize security as part of their evolution. Attackers have identified manufacturing firms as valuable targets, so it becomes incumbent on the industry to make themselves less attractive targets.

References:

http://www.eweek.com/security/deloitte-survey-finds-manufacturers-highly-vulnerable-to-cyber-threats

http://www.themanufacturer.com/reports-whitepapers/annual-manufacturing-report-2017/

http://www.nass.org.uk/Publications/Publication4261/Annual-Manufacturing-Report-2017.pdf

Introduction

Petya, WannaCry and the SMB vulnerabilities associated with MS17-010 dominated much of the news over the last half of Q2 '17, but were by no means the only threats organizations faced. NTT Security GTIC and NTT Computer Emergency Response Team (CERT) collaborated for a closer look at one of those threats, attacks seeking to exploit vulnerabilities in Apache Struts.

There was some buzz around Apache Struts (CVE-2017-5638) after Apache released its security advisories (S2-045 and S2-046) in March 2017. At the time of release, the vulnerabilities, which could allow remote code execution (RCE), were assigned a CVSS of 10, the most critical.

The bigger news about Struts is that attackers quickly jumped on the Struts bandwagon, and have remained there. Apache Struts exploit attempts quickly jumped into the top five attacks most commonly detected in client environments, and have remained in the top seven through June 2017.

So, no one should really be surprised that attackers are taking advantage of the Struts vulnerabilities – but how bad are they *really?*

What is a Struts Attack?

The RCE vulnerabilities are based on Struts' use of Object Graph Navigation Language (OGNL) as a template language. Attackers exploit both S2-045 and S2-046 by crafting a malformed HTTP request, along with an OGNL payload, which forces Struts to create an exception. OGNL includes security restrictions on creating and accessing an object, so attacks must bypass those limitations.

Attack vectors for S2-045 and S2-046 are different, so errors occur in different phases of a process.

- S2-045: HTTP Content Type header field
- S2-046: HTTP Content Disposition header field and Content-Length field

The process flow related to each attack vector is shown in **Figure 18**.

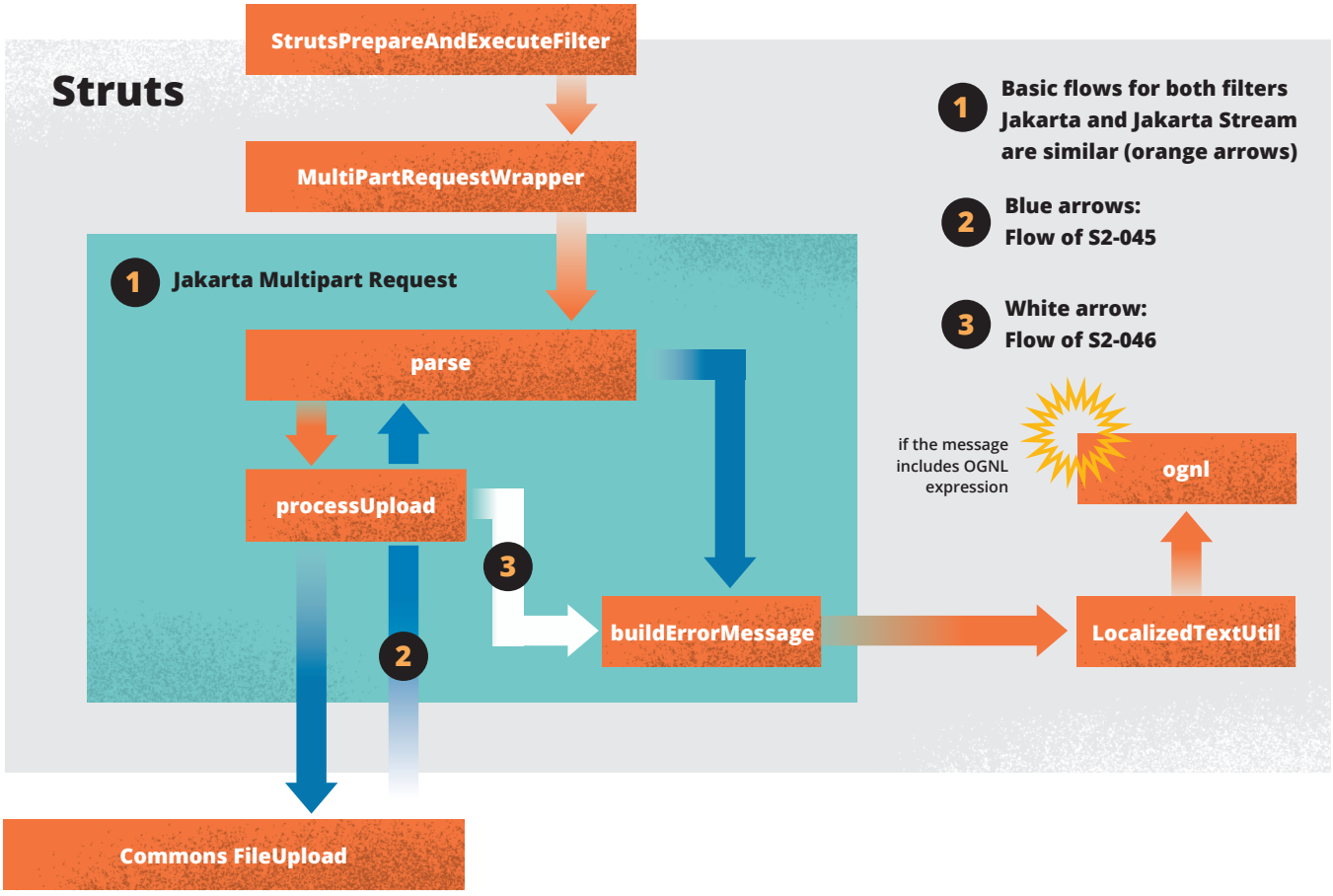


Figure 18. Struts attack vector flow

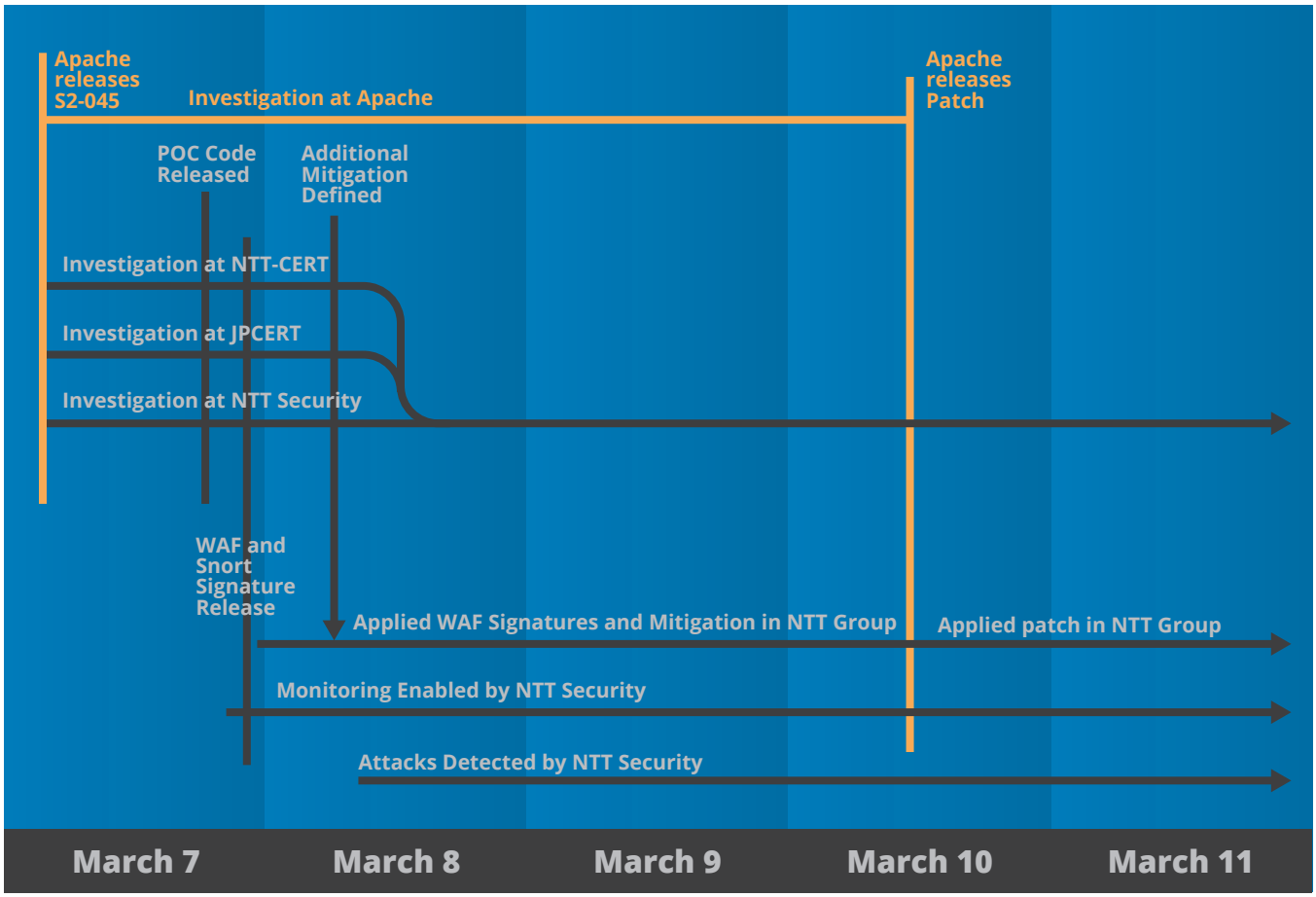


Figure 19. Struts timeline

Struts Attacks Timelines

NTT Security researchers and NTT-CERT both tracked the Struts announcement and attacks on a global scale. The timeline in **Figure 19** summarizes activity over the first several days.

Attackers tend to exploit public vulnerabilities quickly, taking advantage of exploits before security professionals can fully evaluate the vulnerabilities and before patches can be applied. The speed with which Apache Struts attacks (and others) were weaponized helps highlight the importance of effective vulnerability management. Organizations must be able to identify, classify, remediate, mitigate and track vulnerabilities in their environments to minimize the impact new vulnerabilities can have, and to react in an effective manner.

NTT Security and NTT Group resources began investigating Apache Struts within hours of the release of Apache's security advisory. A researcher released proof-of-concept (PoC) code to exploit the vulnerability on March 8 and web application firewall (WAF) signatures were developed soon after. NTT Security detected what appeared to be malicious attack activity within 24 hours of the release of the PoC code. NTT Security and NTT-CERT analysts evaluated the effectiveness of the Apache patch, as well as WAF signatures in mitigating the impact of the observed attacks.

In this process, the goal of NTT-CERT's analysis was to provide current information for internal NTT Group resources, including NTT Security and supporting operating companies. The goal of NTT Security analysis was to provide current information for NTT Security operations and clients.

Early on March 9, NTT Security was already detecting significant levels of exploit attempts. As shown in **Figure 20**, NTT Security detected consistent levels of attacks for several days before the sharp increase in attack traffic on March 17, which is almost completely attributable to activity from China-based sources.

While attacks originated from many countries around the world, 76 percent of all attacks targeting Apache Struts originated from IP addresses in China.

Observed Attacks

Sixty-nine percent of attacks from China attempted to disable local firewalls and install malware from remote servers using Linux retrieval commands such as wget. This often included attempts to pull down Linux 32-bit and 64-bit malware over POP port 110. Malware names ranged from UpTip60 through UpTip97. This malware was most often hosted in the United States, China or South Korea.

In some instances, *wget* was used but did not pull down any malicious binary. These were likely attempts to identify vulnerable servers, potentially to retrieve additional binaries for future attacks.

Struts Targets

Researchers specifically evaluated detections in Japan and U.S. operations. There was little overlap in the industries targeted in each region. In the U.S., 65 percent of all Struts detections were identified in the education and health care industries, while in Japan, 46 percent of all Struts attacks were reported in the government sector alone. Detections in each industry in the different geographies are shown in **Figure 21**.

The fact that attackers continue to target different industries in different geographic regions should not surprise anyone. While

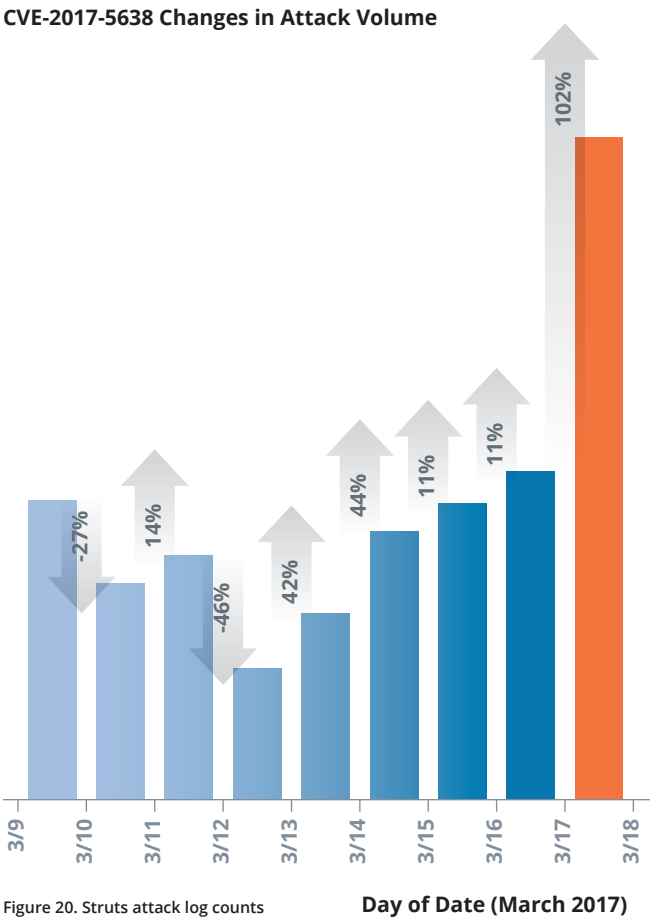


Figure 20. Struts attack log counts

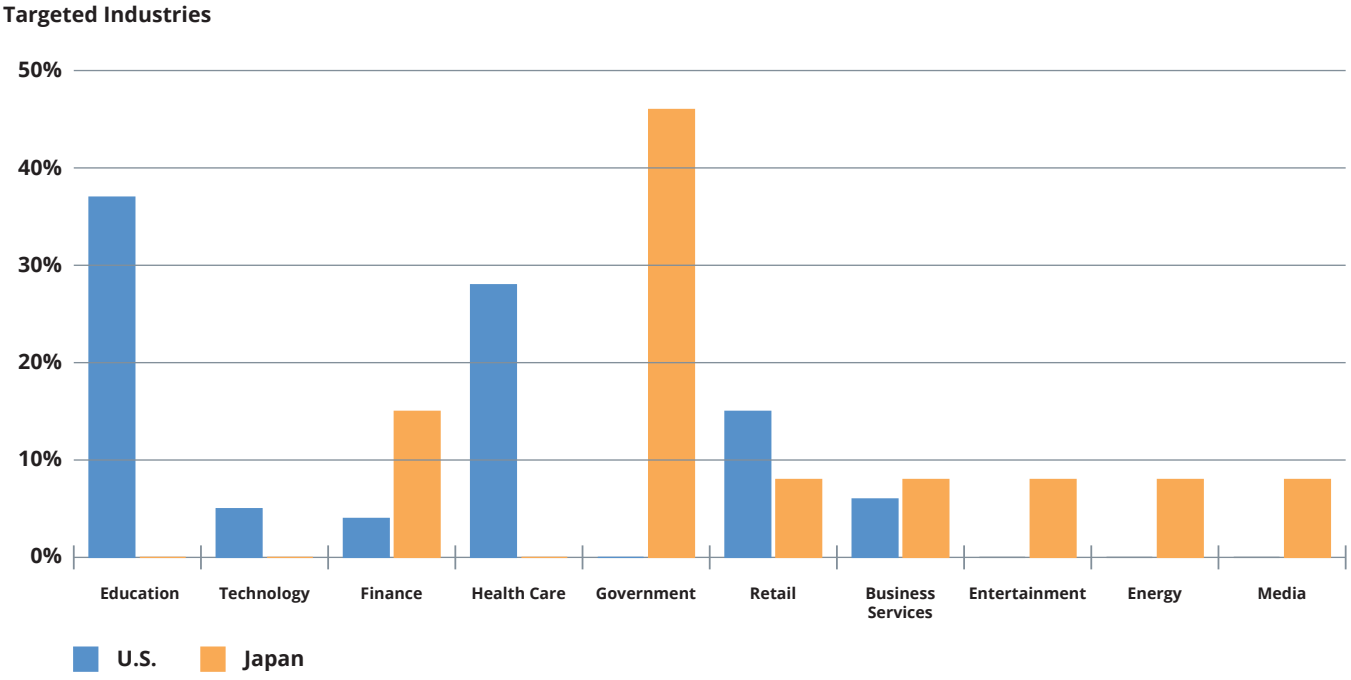


Figure 21. Targeted industries in U.S. and Japan

the basics of an Apache Struts attack are similar across all geographies, the motivations of attackers change, as do the targets which attackers in each region find interesting.

Why Target Struts?

Globally, Struts seems an unlikely target. Apache Struts has relatively low global market adoption when compared to other common web frameworks. **Figure 22**[15] shows the relative market share of several web frameworks.

However, market share changes when regional impact is considered. A 2013 survey completed in Japan[16] showed that Struts had a 17 percent market share in Japan, which may have helped contribute to elevated levels of attacks in some markets.

NTT Security anticipates cyber criminals will continue targeting Apache Struts installations because of the wide installation base, the simplicity of the attack, and the fact that the attack includes the ability to execute code remotely.

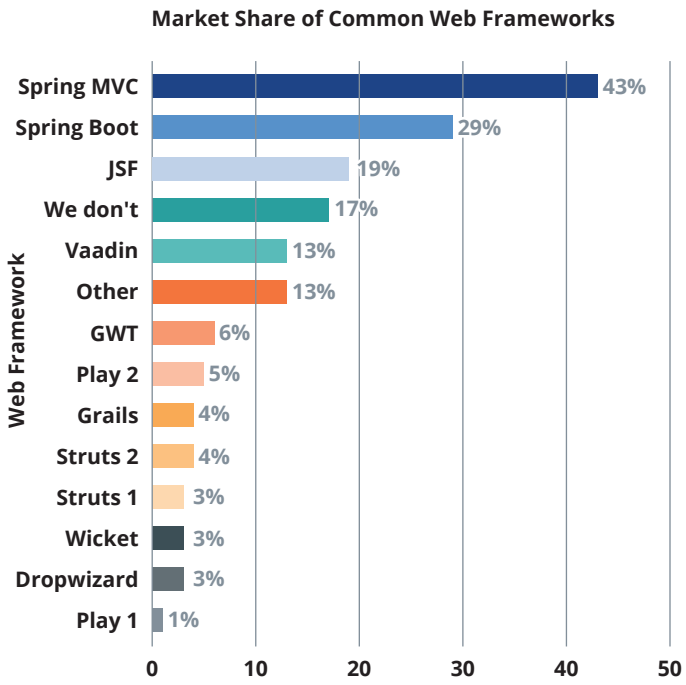


Figure 22. Market share of common web frameworks

Signature ID	Description
41819	SERVER-APACHE Apache Struts remote code execution attempt
41818	SERVER-APACHE Apache Struts remote code execution attempt
41923	SERVER-APACHE Apache Struts remote code execution attempt
2024038	ET WEB_SPECIFIC_APPS Possible Apache Struts OGNL Expression Injection (CVE-2017-5638)
2024044	ET WEB_SPECIFIC_APPS Possible Apache Struts OGNL Expression Injection (CVE-2017-5638) M2
2024045	ET WEB_SPECIFIC_APPS Possible Apache Struts OGNL Expression Injection (CVE-2017-5638) M3

Figure 23. Snort Signatures.

```
headercontent:"_memberAccess"; nocase; re2:"/\b_memberAccess\b/Hi";
headercontent:"OgnlContext"; nocase;
valuecontent:"OgnlContext"; nocase;
headercontent:"MemberAccess"; nocase;
valuecontent:"MemberAccess"; nocase;
```

Figure 24. F5 BIG IP.

```
Signature pattern: part="_memberAccess", rgxp="\b_memberAccess\b"
Protocol(s): http,https
Field(s) for search: header

Signature pattern: part="OgnlContext"
Protocol(s): http,https
Field(s) for search: header

Signature pattern: part="OgnlContext"
Protocol(s): http,https
Field(s) for search: parameter
Signature pattern: part="MemberAccess"
Protocol(s): http,https
Field(s) for search: header, parameter
```

Figure 25. Imperva SecureSphere.

[15] https://zeroturnaround.com/rebellabs/java-tools-and-technologies-landscape-2016/
[16] http://www.sbbit.jp/article/cont1/26911 (Please note that this article is only available in Japanese.)

Apache Struts Mitigation

Criminals continue to target Apache Struts installations. To help mitigate these attacks, organizations should consider the following actions:

- Upgrade to Struts versions 2.3.32 or Struts 2.5.10.1 (or later).
- Implement a servlet filter which will validate Content-Type and throw away requests with suspicious values not matching multipart/form-data.
- Change to a different multipart parser such as pell or the parser from the Commons-File Upload Library[17].

Struts Signatures and Rules

NTT Group has identified the following signatures and rules which may help mitigate attacks. While other detections may be available, NTT Group has identified these signatures and rules as particularly reliable.

Apache Struts: Summary

Attacks against Apache Struts have not reached the same level of attention as WannaCry, Petya, or many other attacks, but attackers have made consistent attempts to exploit the vulnerabilities in Apache Struts since the PoC code was released. Apache Struts has probably not received the level of attention it deserved, given that it has been a "top 7" attack consistently since its release.

As is true with many current vulnerabilities, the single most effective mitigating control is to patch systems in your environment, in this case, Apache Struts. That said, don't expect Apache Struts attacks to disappear until a lot more organizations have completed that patching.

[17] http://commons.apache.org/proper/commons-fileupload/

Summary

With a 24 percent increase in overall activity, Q2 '17 was characterized by a wider blend of attack methods compared to Q4 '16. Attacks observed in Q2 '17 included a variety of web application attacks, attacks allowing for remote code execution, and phishing-based attacks. Within these phishing campaigns, however, cyber criminals appeared to have a narrower focus, as their preferred vector was leveraging PowerShell commands in VBA macros within malicious attachments.

NTT researchers also noted an uptick in reconnaissance – possibly indicating attack preparation during the upcoming 3rd and 4th quarters. This is a trend NTT Security researchers have observed in previous years, including during Q3 and Q4 '16, when recon activity declined. There is a strong likelihood that this trend will continue during the last two quarters of 2017 as well, as attackers again shift to more targeted attacks as they determine their targets' vulnerabilities.

This may not bode well for the manufacturing industry, as a large part of overall reconnaissance activity was aimed at the manufacturing industry during Q2 '17, and 33 percent of overall activity against the manufacturing industry was reconnaissance-based. If trends from the past few years continue, this probably indicates that attacks and malware are likely to increase in manufacturing organizations in the second half of 2017.

Even without the looming threat of increased attack volumes, the manufacturing industry faces a variety of security challenges in its ongoing evolution. With more technology and connectivity continually being introduced into the industry, manufacturing is quickly becoming a high-value target for cyber criminals. While not typically thought of as highly 'attackable,' manufacturing has been one of the most consistently attacked industries over the past several years, and was the most targeted industry in Q2 '17. In addition to potential threats unique to the manufacturers, the industry also faces a variety of threats, prevalent across many industries, including insider and technical threats.

The tactics of cyber criminals will continue to evolve, as does the technology available to them. That being said, many threat actors continue to use tried and true methods (e.g., unpatched vulnerabilities), with many organizations failing to properly secure these attack vectors – a lesson many organizations learn the hard way.

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[18] and threat reports[19], visit the research page on www.nttsecurity.com, our blog[20] or download related whitepapers[21].

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[22].

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 nttsecurity.com to learn more.

[18] https://www.solutionary.com/threat-intelligence/vulnerability-disclosures/
[19] https://www.solutionary.com/threat-intelligence/threat-reports/
[20] http://www.solutionary.com/resource-center/blog/
[21] http://www.solutionary.com/resource-center/white-papers/
[22] http://www.ntt-cert.org