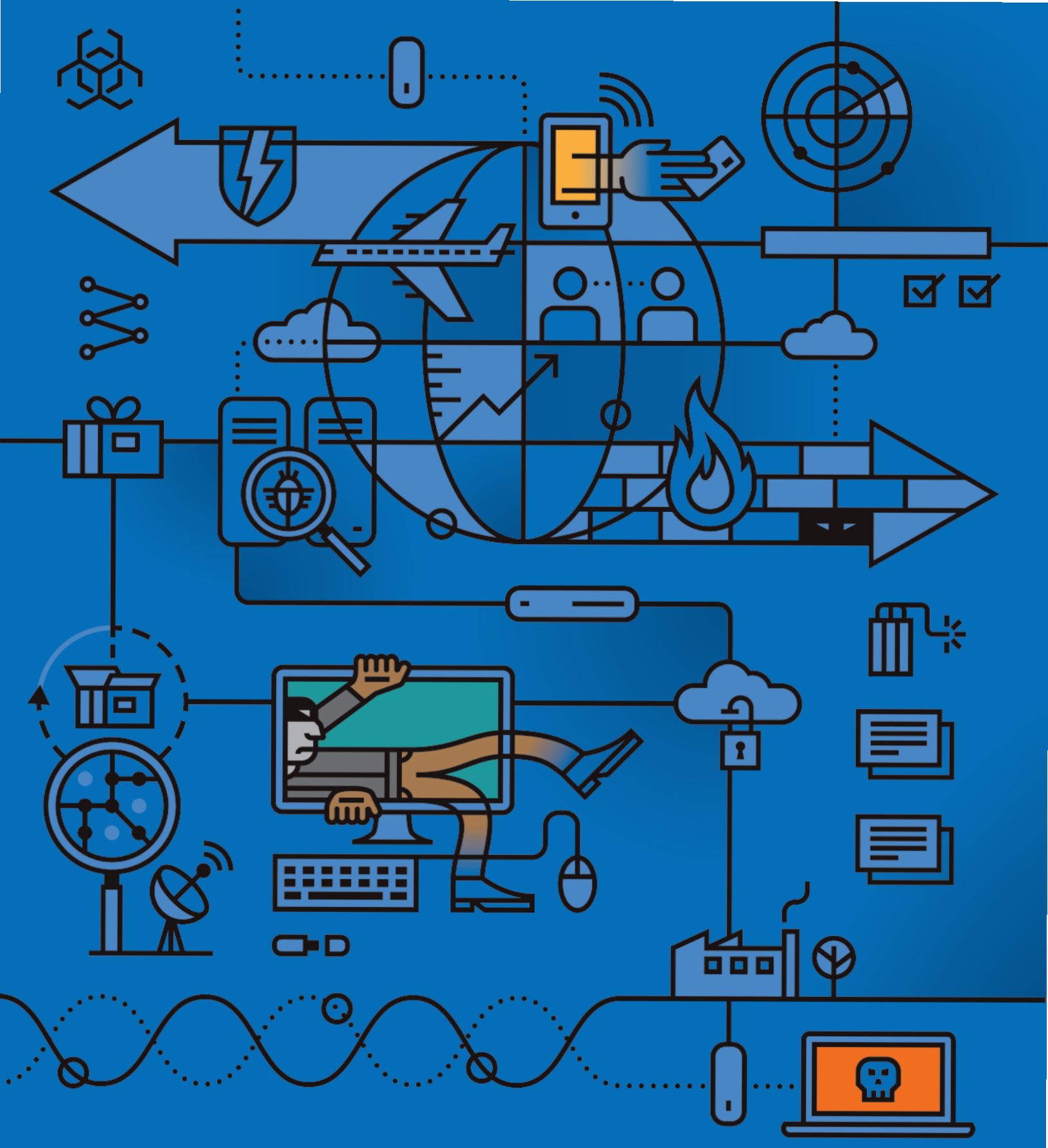


2016 NTT Group
Global Threat Intelligence Report

Table of Contents

Table of Contents Continued

Executive Summary

THE NTT GROUP 2016 GLOBAL THREAT INTELLIGENCE REPORT

Every day, organizations must decide how to best allocate security budgets and resources. With advances in malware, attacks and technology, that situation is only getting more complicated. In reality, we don't need new point solutions to fix niche problems. If we truly want to move our security programs forward and manage our limited resources more effectively, we need a comprehensive solution to apply across our entire infrastructure. Defense in depth really does matter. Architecting a comprehensive, integrated and cohesive solution will not only help enable efficiency and effectiveness, but also support the security life cycle of the entire organization.

This year's GTIR utilizes the Center for Internet Security's **Critical Security Controls** to identify controls that can be effective at each stage of the **Lockheed Martin Cyber Kill Chain®** (CKC). By ensuring that controls exists for each stage of the CKC, organizations can increase their ability to disrupt attacks. We've dedicated an entire section and case study to a Practical Application of Security Controls to the Cyber Kill Chain.

An effective security program understands the current threat environment in order to detect what attackers are doing now. To help support this understanding, we have included a summary of hostile activity in this year's Global Data Analysis and Findings and an expanded perspective in the Global Honeynet Analysis section.

> "An effective security program understands the current threat environment, to detect what attackers are doing now."

The ultimate goal of a security program is to increase the resilience and survivability of the organizational environment. Oddly enough, malware developers have some of the same goals. The Anti-sandbox Techniques section focuses on how malware has incorporated resilience and survivability into its own capabilities.

The Role of the Cyber Kill Chain in Threat Intelligence discusses the significant impact an active threat intelligence program can have on an organization's entire security program. It includes a well-thought-out plan for acquiring properly vetted data, information and intelligence sources, and applying that intelligence to the current environment.

As the GTIR enters its fourth year, NTT Group has expanded our view of the threat landscape to include findings from some of our key collaborators. We are pleased to include Lockheed Martin, Wapack Labs, Recorded Future and the Center for Internet Security as contributing partners.

We hope you find the NTT Group 2016 Global Threat Intelligence Report insightful and worthwhile. Thanks for reading.

Key Findings

Geographic and Vertical Market Trends

In the 2016 GTIR, NTT Group evaluated threats against clients and honeynets across industry sectors and geographic regions.

- **The retail sector experienced the most attacks per client of any industry sector.** Retail was followed by the hospitality, leisure and entertainment sector, then insurance, government and manufacturing. Retail clients experienced 2.7 times the number of attacks as finance clients.

- **U.S.-based IP addresses accounted for 65 percent of attacks detected in 2015.** The U.S. remains the largest source of hostile IP addresses observed by NTT Group in 2015, up from 49 percent in 2013 and 56 percent in 2014. A U.S.-based attack doesn't mean that the attacker is actually U.S. based – non-U.S. attackers often use the U.S. infrastructure to evade geographic IP blocking.

- **Three sources accounted for 38 percent of all non-U.S. based attacks.** Attacks from the United Kingdom, Turkey and China made up 38 percent of the non-U.S. based attacks. Attacks from 199 other countries combined to make up the remaining 62 percent.

- **NTT Group observed an 18 percent rise in malware detected for every industry other than education.** NTT clients from the education sector tended to focus less on the more volatile student and guest networks, but malware for almost every other sector increased.

Vulnerabilities, Attacks and Exploitation

Vulnerability and attack details from 2015 reveal much of what exists in client environments, and what attackers are taking advantage of.

- **Nearly 21 percent of vulnerabilities detected in client networks were more than three years old.** More than 12 percent were over 5 years old, and over 5 percent were more than 10 years old. Results included vulnerabilities that were from as far back as 1999, making them over 16 years old. This is for vulnerabilities with a Common Vulnerability Scoring System (CVSS) score of 4.0 or higher.

- **The top 10 external vulnerabilities accounted for nearly 52 percent of all identified external vulnerabilities.** Thousands of vulnerabilities account for the other 48 percent.

- **The top 10 internal vulnerabilities accounted for over 78 percent of all internal vulnerabilities during 2015.** All 10 internal vulnerabilities are directly related to outdated patch levels on the target systems.

- **All of the top 10 vulnerabilities targeted by exploit kits during 2015 are related to Adobe Flash.** In 2013, the top 10 vulnerabilities targeted by exploit kits included one Flash and eight Java vulnerabilities. That has changed as new Java vulnerabilities have dropped steadily since 2013. The number of publicized Flash vulnerabilities jumped by almost 312 percent from 2014 levels.

- **Brute force attacks jumped 135 percent from 2014 levels.** Throughout the year, NTT Group detected SSH brute-force attacks across its entire client base, from 75 different source countries.

- **DoS/DDoS attack volume fell 39 percent over levels observed in 2014.** Implementation of better mitigation tools, along with fewer attacks, combined for a drop in detections of denial of service (DoS) and distributed denial of service (DDoS) activities. But, extortion based on payments by victims to avoid or stop DDoS attacks became more prevalent.

Key Findings

- **24 percent of web application attacks during 2015 were injection-based.** This continues the trend in 2014 that saw 26 percent of web application attacks being injection-based. Injection attacks allow remote command execution, and can support exfiltration of data.

- **With an average of 128,000 attacks per day, attacks on SMB, NetBios and Samba were the highest volume attacks detected on the NTT Group global honeynet.** Honeynet data included nearly 105 million events from over 372,000 unique IP addresses. SSH, HTTP, SQL, and VoIP (SIP) also contributed to the top five attacks.

Incident Response and Case Studies

- **22 percent of all incident response engagements originated from the retail vertical market client base with the finance vertical coming in a close second at 18 percent.** Many of the attacks against retailers involved spear phishing attacks.

- **Trend data from incident response activities supported over the last 3 years illustrates on average only 23 percent of organizations are capable of responding effectively to a cyber incident.** 77 percent have no capability to respond to critical incidents and often purchase incident response support services after an incident has occurred.

- **Spear phishing attacks accounted for approximately 17 percent of incident response activities supported in 2015.** Spear phishing rose dramatically from less than two percent of incident response engagements in 2014.

- **Command and Control (C2) activity for clients required to comply with PCI was just over half the C2 activity of non-PCI clients.** Clients who were required to be PCI compliant tended to observe 57 percent less C2 traffic than clients without PCI requirements.

- **Malware and DDoS related attacks required less incident response support compared to previous years.** Malware-specific response activities were down approximately 33 percent and DDoS was down 12 percent. We observe DDoS activity is down overall, not only in incident response, but also based on observations derived from log and event monitoring.

Global Data Analysis and Findings

This section presents an analysis of global attack data gathered by NTT Group security companies during 2015. It is based on log, attack, incident and vulnerability data from clients and NTT Group research sources, including our global honeypots and sandboxes, that operate in a different environment than our managed services. This allows us to observe different views of the available data. This year's GTIR also includes important observations from some of our key partners, including Lockheed Martin, Wapack Labs, Recorded Future and the Center for Internet Security. Each organization brings a unique view of the data and the security concerns associated with our observations. The analysis of these combined organizations makes this year's results stronger than ever.

Global Data Analysis covered over 3.5 trillion logs and 6.2 billion attacks

During operations, NTT Group gathers security log, alert, event and attack information; enriches it to provide context; and analyzes the contextualized data. NTT Group processes trillions of logs and billions of attacks each year. The size and diversity of our client base makes this data representative of the threats encountered by most organizations.

The data presented in this section is derived from correlated log events identifying validated attacks in 2015. The use of validated attack events, as opposed to raw log data or network traffic volumes, more accurately represents actual attacks. NTT Group observed a large volume of untargeted network reconnaissance traffic and DDoS activity throughout 2015. Without active analysis and categorization of attack events, such activity could obscure the actual incidence of attacks.

Global Data Analysis and Findings

To show the results of this analysis, the Global Data Analysis and Findings are presented in related sections:

1. **Sources of Attack** – analysis of the country sources of the observed attacks against clients
2. **Attacks by Sector** – analysis of attacks against clients in related industry sectors
3. **Types of Attacks** – analysis of the types of attacks employed against clients
4. **Vulnerability Summary** – analysis of the types and age of vulnerabilities observed in client environments
5. **Malware Observations** – analysis of the malware observed in client environments
6. **Exploit Kit Summary** – analysis of exploit kits and their exploits observed in client environments

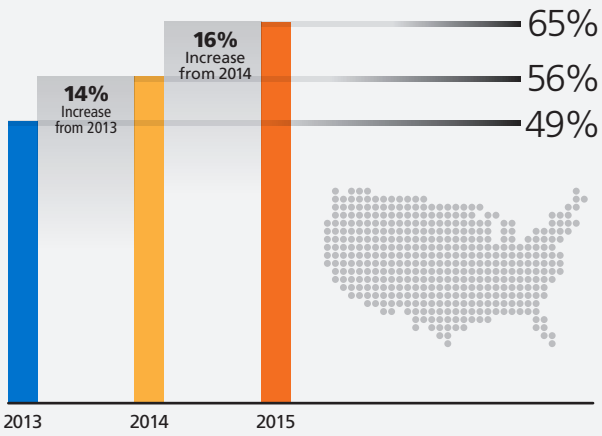


Figure 1: U.S. as an attack source

The greatest value of the Global Data Analysis section is that it is based on details observed in actual client environments. This is not data gathered from labs or from anecdotes, but details from actual logs, events, vulnerabilities and attacks observed by real organizations throughout the year.

Sources of Attacks

As shown in Figure 1, 65 percent of attacks detected against the NTT Group client base originated from IP addresses within the United States. This continues the trend NTT Group has observed over the past several years. Past analysis revealed 49 percent of attacks originated from within the U.S. during 2013, and 56 percent in 2014. Internet use and connectivity continues to increase within the U.S., and this can account for some of this gain, but the rate of increase in attacks is currently exceeding Internet growth.

This continues the history of the United States serving as a major source of hostile activity due to the ease of provisioning, cheap cost and high quality of U.S. based cloud hosting services. A significant number of the detected attacks are targeting U.S. clients, so attackers tend to host such attacks locally, in the same geographic region as their victims. Many of these attacks appear to be truly originating from within the U.S., perhaps indicating attackers have less concern about their origin due to the challenge of tracking down and stopping a dedicated attacker. While the source IP address is based in the U.S., the actual attacker could be anywhere in the world. Due to the ease with which attackers can disguise their IP addresses, attack sources can often be more indicative of the country in which the target is located, or perhaps of where the attacker is able to compromise or lease servers, rather than where the attack actually originates.

As can be seen in Figure 2, during 2015, the top five attack source countries accounted for 81 percent of all identified attacks.

In 2015, attacks from addresses based in the United Kingdom (UK) rose slightly, while attacks from addresses within China dropped, and the UK became the number one source of non-U.S. based attacks. As presented in Figure 3, 38 percent of the attacks that originated outside the U.S. showed IP addresses from the top three source countries. Beyond the top ten source countries, the distribution of source IP addresses was flat. NTT Group detected attacks from a total of 217 different countries during 2015. The 197 countries that individually accounted for less than one percent of attacks have each been included in the "Other" category.

Attacks by Sector

Figure 4 shows the distribution of NTT Group clients in the data set by industry sector.

Global Data Analysis and Findings

Figure 5 presents the attack data in a different manner than in previous NTT Group reporting. For 2015 data, NTT Group normalized attack data by dividing the volume of attacks per sector by the number of clients in each sector. So, although the finance sector showed the highest volume of attacks across all sectors, that was because NTT Group has more clients in the finance sector than any other sector. After attack data was normalized by considering the number of clients in each industry, the retail sector showed the highest number of attacks per client, at just under 11 percent – nearly three times as many attacks as clients in the finance sector.

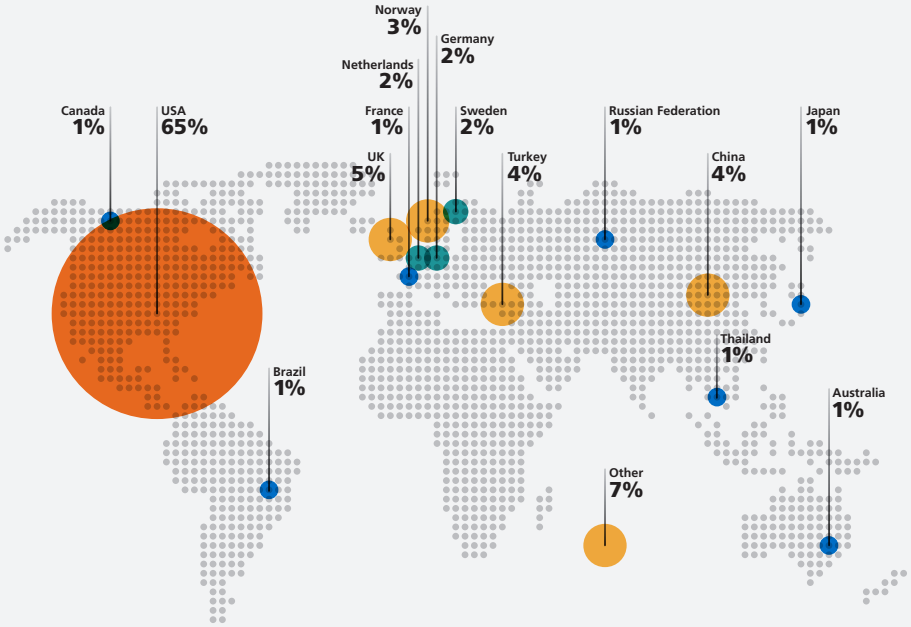


Figure 2: Attack source countries, 2015

Retail companies are still popular targets. Retailers often process large volumes of personal information – including credit card data – in highly distributed environments with many endpoints and point of service devices. Such diverse environments can be difficult to protect.

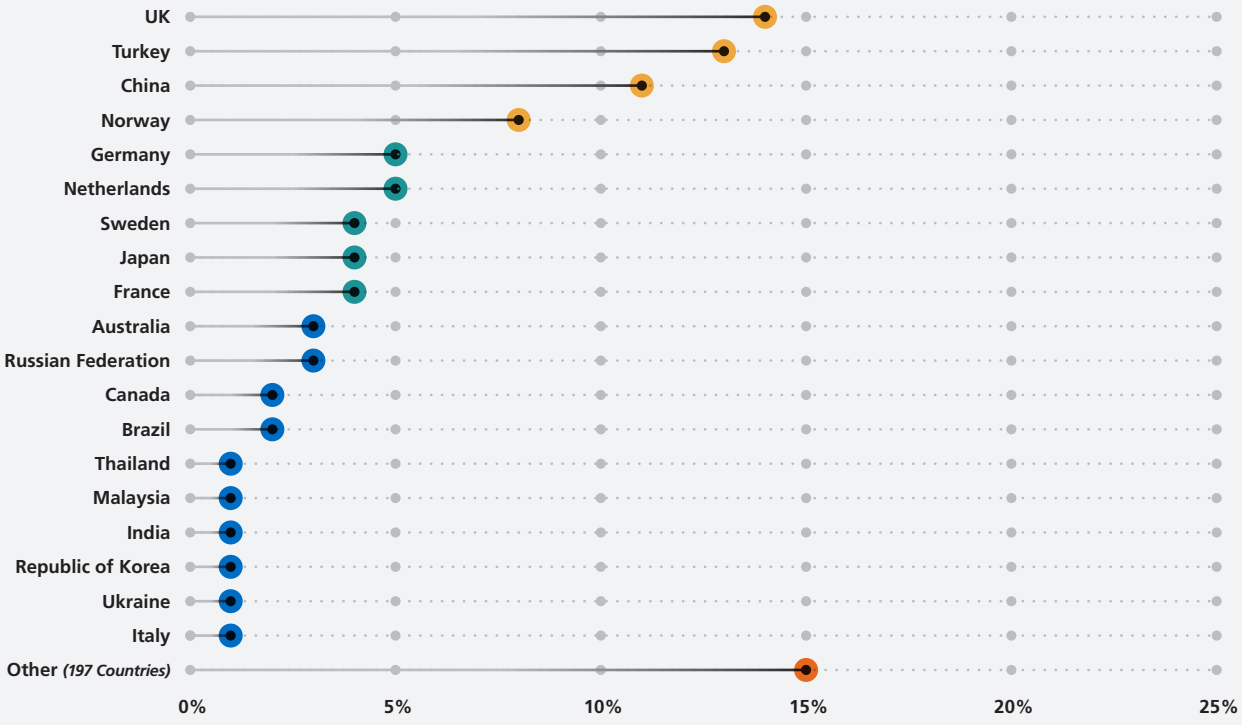


Figure 3: Non U.S. attack source countries, 2015

Global Data Analysis and Findings

During 2015, NTT Group also observed an increase in attacks related to the hospitality, leisure and entertainment sector. This sector faces many of the same challenges as the retail sector, also processing high volumes of sensitive information including credit card data. Transactions in the hospitality sector, which includes hotels and resorts, tend to be sizable, that can make compromising those card numbers more attractive to attackers. The hospitality sector also includes a significant number of loyalty plans that house even more personal information. This sector fell victim to several high profile breaches during 2015, including properties from Starwood Hotels & Resorts, the Trump Hotel Collection, Hilton Worldwide, Mandarin

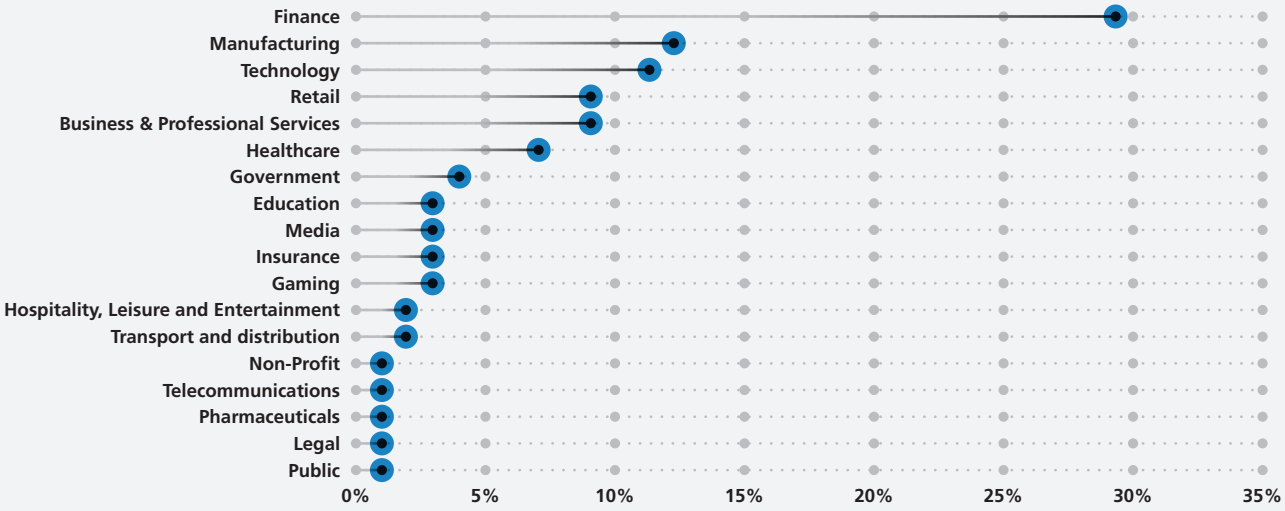


Figure 4: NTT Group security clients by sector, 2015

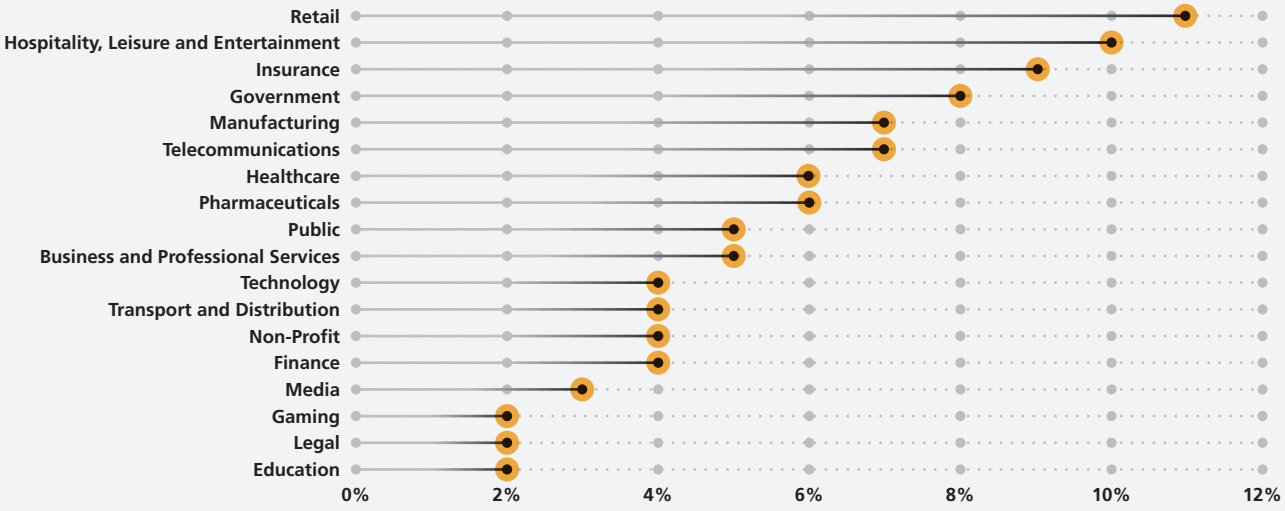


Figure 5: Attacks by sector

Global Data Analysis and Findings

Oriental and White Lodging Services Corporation. Not all of these properties were attacked directly – many of the breaches involved point-of-sale malware directed against providers and retail companies that offered service on hospitality properties. The end result targets the same clients, without directly targeting the property's information security program.

The insurance and government sectors both ranked in the top five most attacked sectors in 2015. The manufacturing sector continued to detect significant attacks, consistent with levels experienced in previous years. Overall, clients in the top five sectors experienced over 44 percent of the attacks observed by NTT Group during 2015.

Industry Sector Cyber Attacks: Recorded Future Observations

Recorded Future[1] offers a variety of security information and security intelligence services, including tools to facilitate and automate the gathering of threat-relevant data from across the Internet.

Recorded Future evaluated Internet traffic volume related to attacks against each industry sector by analyzing "reference counts" – the number of times the industry was talked about in the context of cyberattacks. As shown in Figure 6, Recorded Future's data illustrates fluctuations throughout the year in the number of attacks against industry sectors. January, September and October of 2015 saw peaks of cyberattack discussion on the internet. In January, key events included attacks against manufacturing organizations and follow on from earlier technology sector breaches. In September and October, the increase was due (in part) to the malware impact on high profile technology retailers, along with significant breaches in the financial sector. Recorded Future tracked activity against the retail sector compared with detections by NTT Group, and identified retail as one of the most targeted – and talked about – industry sectors.

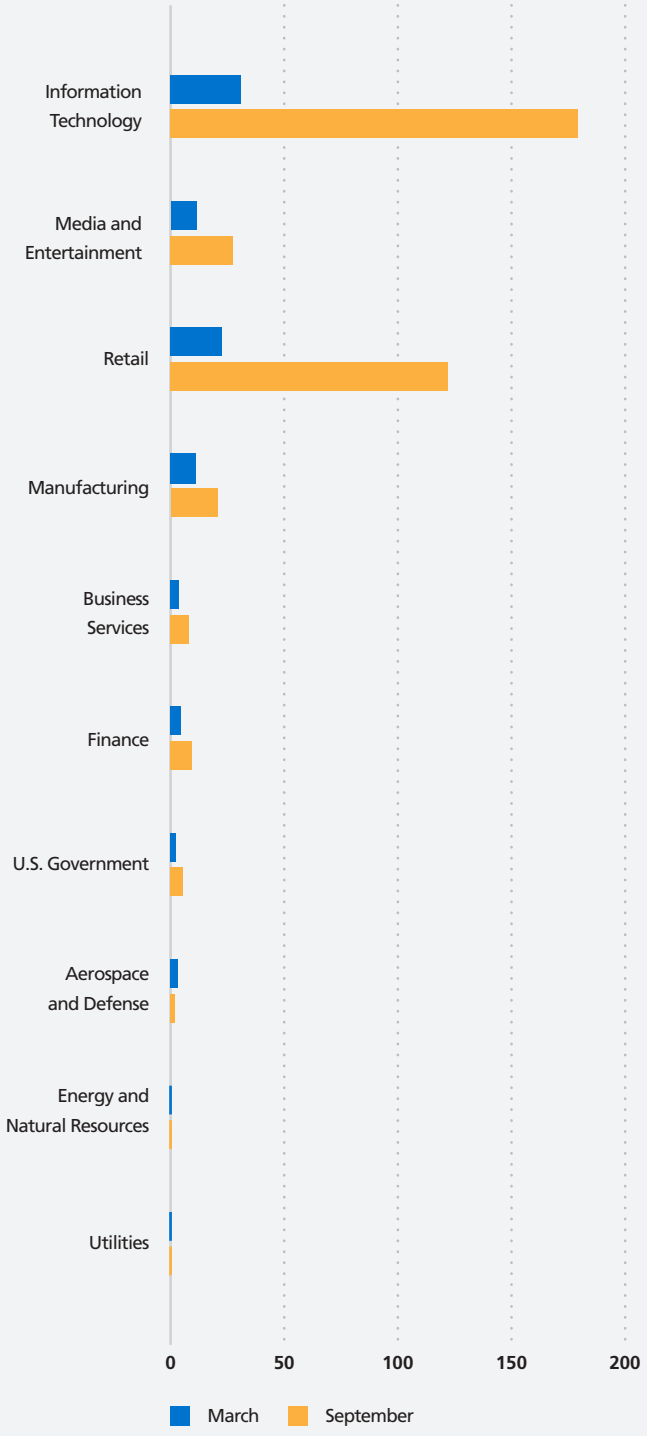


Figure 6: Cyberattack Reference Counts, 2015

[1] www.recordedfuture.com

Global Data Analysis and Findings

Types of Attack

Analysis of 2015 data revealed changes in the types of attacks detected. Anomalous activity, which includes privileged access attempts, exploitation software and other unusual activity, jumped from 20 percent of all attacks in 2014 to 36 percent during 2015. Web application attacks claimed the second highest volume of attacks.

Malware detection rose gradually throughout 2015, including a six percent jump in malware during the fourth quarter alone. Over the year, malware jumped from less than two percent of attacks in 2014 to five percent during 2015. This increase in malware was not due to a specific campaign, malware or source, but resulted from increases in most malware categories throughout the entire year.

Brute force attacks jumped from less than two percent in 2014 to almost seven percent in 2015. The volume of brute force attacks jumped 135 percent from 2014 levels. Throughout the year, NTT Group detected SSH brute force attacks across its entire client base, from 75 different source countries.

Another notable decrease during 2015 was the 39 percent drop in the volume of DoS/DDoS attacks, down from 5 percent of attacks in 2014 to 3 percent in 2015. It appears this drop was due to a combination of events. First, attackers simply conducted fewer DoS/DDoS attacks during 2015 than they had in previous years. Second, 2015 saw the adoption of more effective DoS/DDoS mitigation techniques and services. NTT Group also experienced a reduction in the number of DoS/DDoS incident response engagements, as shown in the section titled Incident Response: Trend Shows Organizations Are Not Prepared.

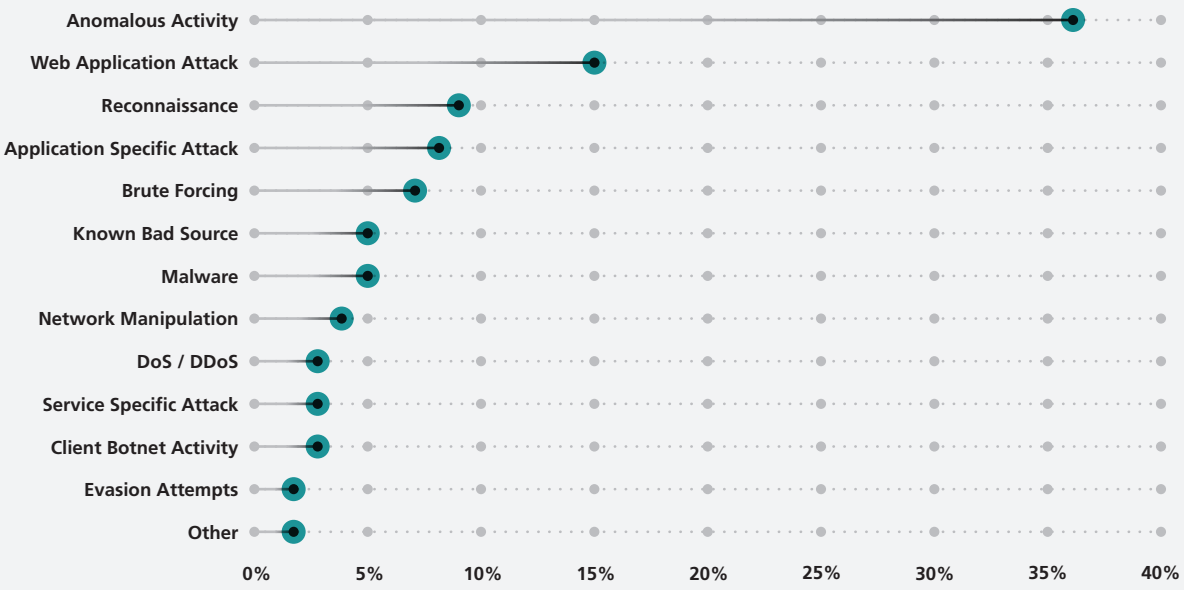


Figure 7: Attacks by type, 2015

Global Data Analysis and Findings

Given the numerous types of web application attacks, NTT Group chose to conduct additional analysis. Web application attacks typically reflect attacks against an organization's Internet-facing applications. Figure 8 presents the results of this analysis.

24 percent of observed web application attacks in 2015 were injection-style attacks, such as PHP command injection or SQL injection. This directly correlates with the OWASP[2] (Open Web Application Security Project) Top Ten Web Application vulnerability list, where "injection" is the top vulnerability. It is also not a significant change from the 26 percent detected during 2014.

Vulnerability Summary

NTT Group compiled vulnerability data for 2015 from clients in every industry sector and geographic location serviced. Vulnerability results included information from a wide range of scanning data, and from multiple scanning vendor products, including Qualys, Nessus, Saint, McAfee, Rapid7, Foundstone and Retina. The findings are based on analysis of any vulnerability with an assigned common vulnerability scoring system (CVSS) score of 4.0 or higher.

Figure 9 lists the top ten vulnerabilities from external and internal scans. In general, the types of vulnerabilities seen in 2015 match those seen in 2014. The top 10 external vulnerabilities of 2015 accounted for nearly 52 percent of identified external vulnerabilities. External vulnerabilities reflect what attackers are observing from outside of the targeted organization.

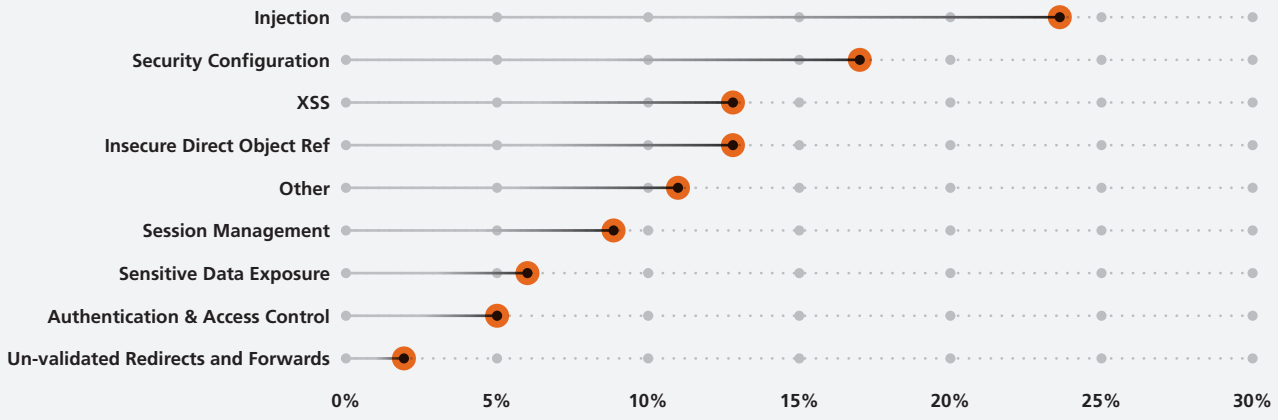


Figure 8: Injection attacks lead Web application attack types

[2] www.owasp.org

Global Data Analysis and Findings

Top 10 External Vulnerabilities	
Outdated PHP Version	8%
Cross-Site Scripting (CSS/XSS)	7%
Outdated Apache Web Server	7%
SSL/TLS Information Disclosure	6%
Web Clear Text Username/Password	5%
Weak SSL/TLS Ciphers/Certificate	5%
Outdated Apache Tomcat Server	4%
Weak/No HTTPS cache policy	4%
Cookie without HTTPOnly attribute set	3%
SSL Certificate Signed using Weak Hashing Algorithm	3%

Top 10 Internal Vulnerabilities	
Outdated Java Version	51%
Outdated Adobe Flash Player	11%
Outdated Adobe Reader and Acrobat	5%
Outdated Microsoft Windows	3%
Outdated Microsoft Internet Explorer	3%
Outdated Mozilla Firefox	2%
Outdated Microsoft Office	1%
Outdated Linux Kernel	1%
Outdated Novell Client	1%
Outdated OpenSSH Version	1%

Figure 9: Top 10 external and internal vulnerabilities, 2015

The top 10 internal vulnerabilities are exclusively related to patch levels, and accounted for more than 78 percent of all observed internal vulnerabilities during 2015.

Along with considering the volume and types of identified vulnerabilities, NTT Group evaluated their ages, as presented in Figure 10.

Over 79 percent of identified vulnerabilities were disclosed within the past three years, that means nearly 21 percent of vulnerabilities were more than three years old. Continuing the trend from previous years in which old vulnerabilities are remaining in client environments, more than 12 percent of vulnerabilities observed were more than five years old. NTT Group observed vulnerabilities as old as 16 years, and over 5 percent of vulnerabilities were more than 10 years old.

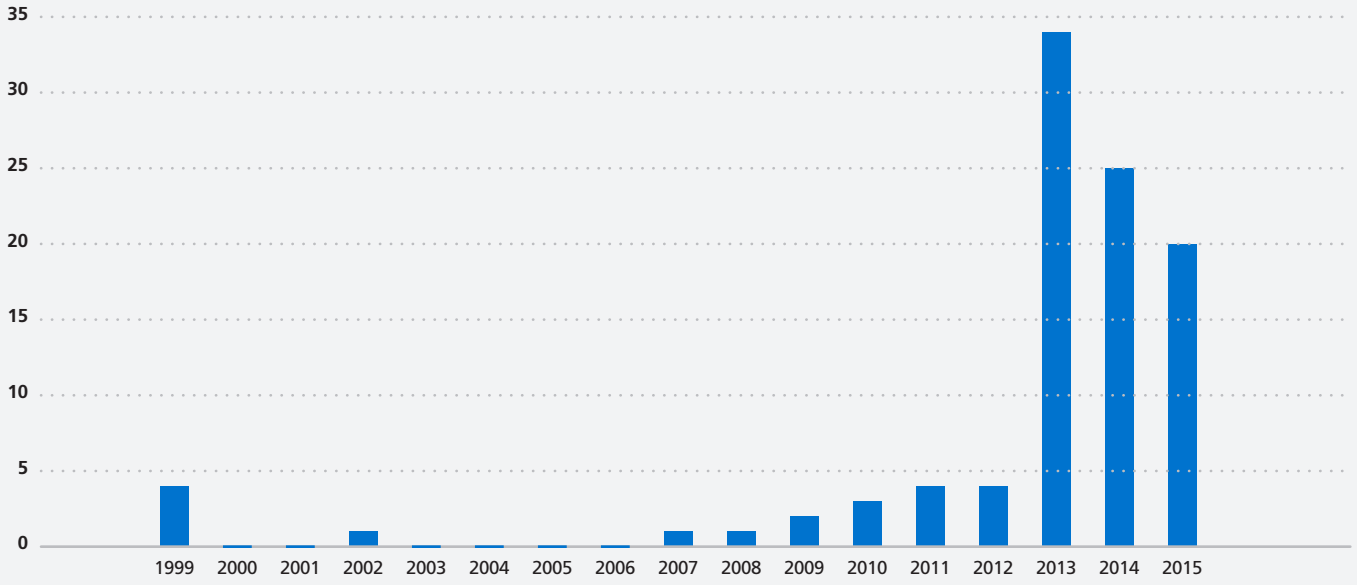


Figure 10: Percent of vulnerabilities by year of disclosure

Vulnerability Details: Recorded Future Observations

Some of the older vulnerabilities NTT Group detected in 2015 were Heartbleed and POODLE. Since 2015 included some notable breaches in the finance sector, Recorded Future analyzed exploited vulnerabilities in the finance industry and identified Heartbleed, POODLE and a vulnerability tied to Dyreza as the top three.

First identified by researchers in June 2015, updated versions of Dyreza used CVE-2015-0057 and CVE-2013-3660 to target banking customers using spam campaigns.

CVE-2014-0160 (Heartbleed) appeared prominently in part due to linkage with a large financial breach the previous year. Multiple banks were identified as vulnerable to CVE-2014-3566 (POODLE) in August 2015 – months after the exposure of the vulnerability.

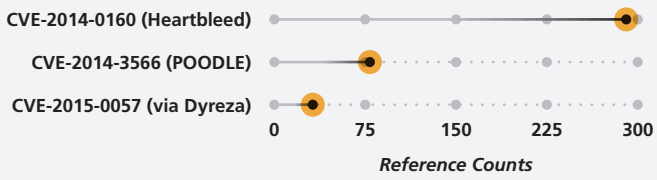


Figure 11: "Popular" vulnerabilities in the finance sector

Malware Observations

NTT Group analyzes malware samples from a wide range of sources, including security platforms, incident response investigations, malware repositories, malware feeds, interaction with clients and privately maintained honeypot networks. These analyses allow for development of proprietary detection and prevention signatures.

The U.S. was the source of over 62 percent of malware detected during 2015. NTT Group detected malware from 191 different countries during 2015. Almost 79 percent of all non-U.S. malware originated from the top five non-U.S. sources.

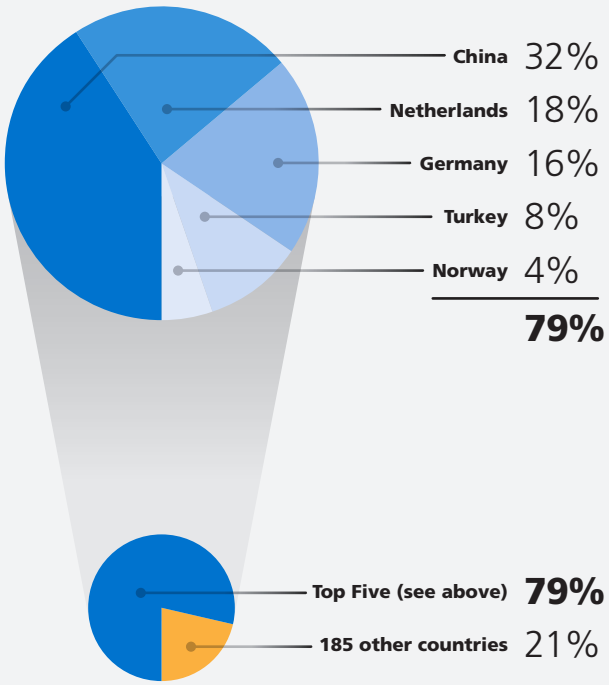


Figure 12: Top five non U.S. countries as sources of malware

2015 showed a decrease in total malware volume compared to 2014. This was largely due to results within a single industry. The volume of malware detections with the education industry showed a 94 percent decrease from 2014 to 2015. This was after a drop from 2013 to 2014. This most recent drop does not necessarily represent a decrease in malware as much as it indicates a shift in the way the education industry managed their environments. During 2015, educational institution clients tended to reduce their focus on managing student and guest environments, and increased their focus on internal, institutional environments. Less focus on student and guest networks dramatically decreased the emphasis on the portions of their

networks that have historically been the most vulnerable, so resulted in drastically fewer logs and events for the entire education sector.

Malware detection for all other industries (excluding education) shows over an 18 percent increase in observed malware for the year. The majority of this malware increase was a combination of sustained, elevated activity across several industries throughout the year.

Rising from eight percent of malware detected in 2014, the government sector climbed to the top of the list of sectors affected by malware, as seen in Figure 13. This was primarily due to a sustained increase in a large variety of malware against multiple government clients throughout the year, and included campaigns against several government agencies in Europe.

The total volume of malware detected in the finance sector was up sharply, showing more than a 140 percent increase from 2014. Detections in the finance industry included both long-term sustained activity and targeted attack campaigns such as the Dyreza malware.

Malware detected within the manufacturing sector, along with the hospitality, leisure and entertainment sector, both rose over 30 percent during 2015. These sectors ranked second and third, respectively, for malware per client.

The retail sector also showed a modest increase over 2014 numbers. Retail clients experienced eight percent of detected malware, making retail the fifth most affected industry. These results show the retail; government; hospitality, leisure and entertainment; and manufacturing industry sectors appear in both the top five sectors targeted by malware and the top five sectors targeted by attacks, making them the most highly victimized of any sectors.

Malware is only one of many attack vectors used, and can be a key component of modern exploit kits.

Exploit Kit Summary

Software exploits take advantage of unpatched flaws in operating systems and applications. Exploits can allow attackers to install malicious software on vulnerable devices.

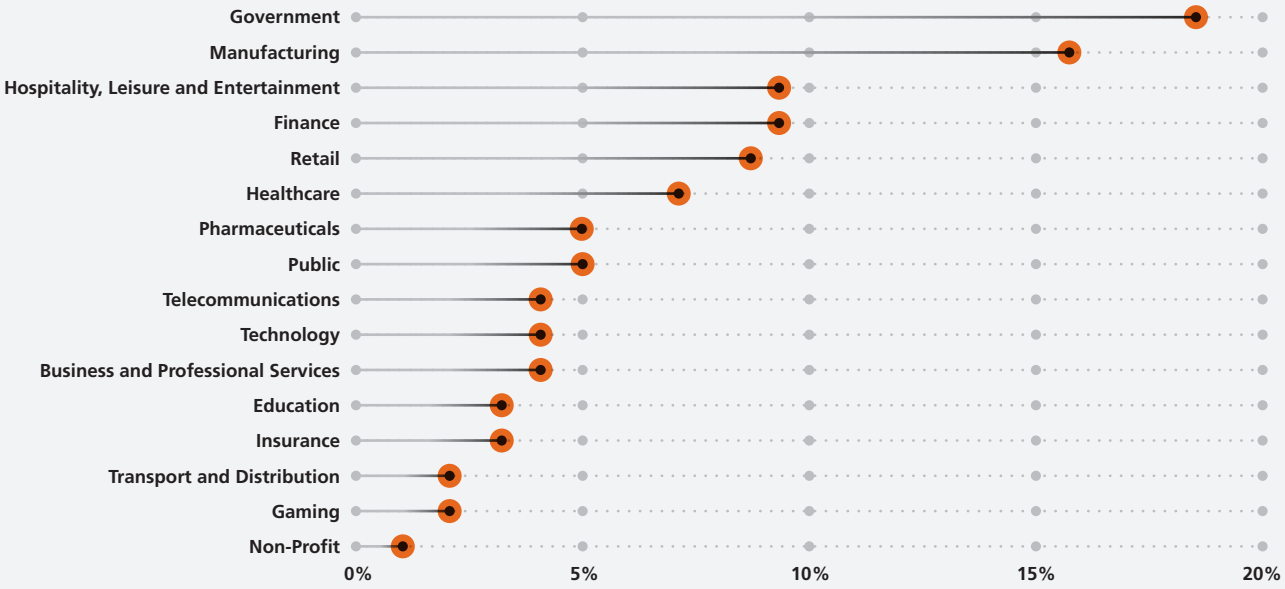


Figure 13: Malware by sector, 2015

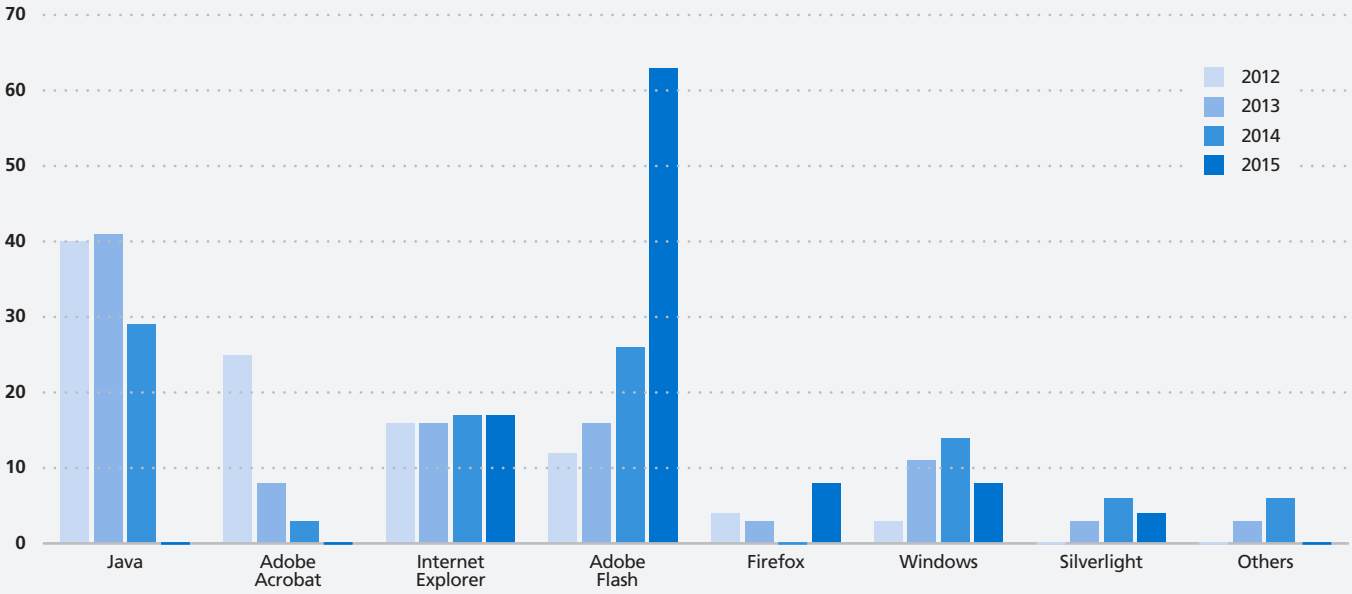


Figure 14: Technology targeted in exploit kits

Exploit kits are software packages commonly sold on hacking forums and IRC channels, and capitalize on software exploits for known vulnerabilities across a range of end-user technologies (Internet Explorer, Adobe Flash, etc.). Exploit kits enable attackers to execute large-scale attacks against vulnerable systems without needing a great deal of expertise.

Technologies targeted by Exploit Kits in 2015

NTT Group tracked unique exploits targeted by popular exploit kits released in years 2012-2015. This information, organized by the technology targeted, is presented in Figure 14[3]. There are three clear trends in this data:

- Adobe Flash was by far the software most targeted by exploit kits in 2015.
- New Java exploits virtually disappeared from exploit kits during 2015.
- Internet Explorer exploitation remained consistent.

The trends observed in this graph are discussed below.

- **Increase in Adobe Flash targeting** – There was a steady increase in Adobe Flash exploit usage in exploit kits from 2012 to 2014, followed by a dramatic increase in 2015. Exploit researchers have increasingly focused on Flash after significant improvements were made to Java security in 2014. The total number of Flash vulnerabilities identified in 2015 was the highest ever, with an almost 312% increase over 2014, as shown in Figure 15.

  Flash is in widespread use on the Internet, and is supported across all modern operating systems. These facts, coupled with a stream of significant security flaws that have not always been patched in a timely manner, explain the dramatic shift toward Flash in exploit kits since 2014.

- **Decrease in Java targeting** – The number of Java vulnerabilities targeted in exploit kits has decreased

[3] This chart includes data from http://contagiodump.blogspot.com, an excellent resource for historical and current exploit kit data. It also includes data from http://malware.dontneedcoffee.com/, an indispensable source for exploit kit analysis and exploit kit tracking.

steadily from 2013 to 2015, due at least in part to security improvements introduced in Java (including blocking of unsigned applets by default). These security improvements are reflected in the decrease of Java vulnerabilities identified over the last two years, as displayed in Figure 16.

- **Consistent targeting of Internet Explorer** – Internet Explorer is still the default browser on Windows operating systems and is common on end-user systems in the corporate environment. Internet Explorer continues to be a target of choice, not only because it is common, but because vulnerabilities continue to be discovered in Internet Explorer at a consistent rate, as shown in Figure 17.

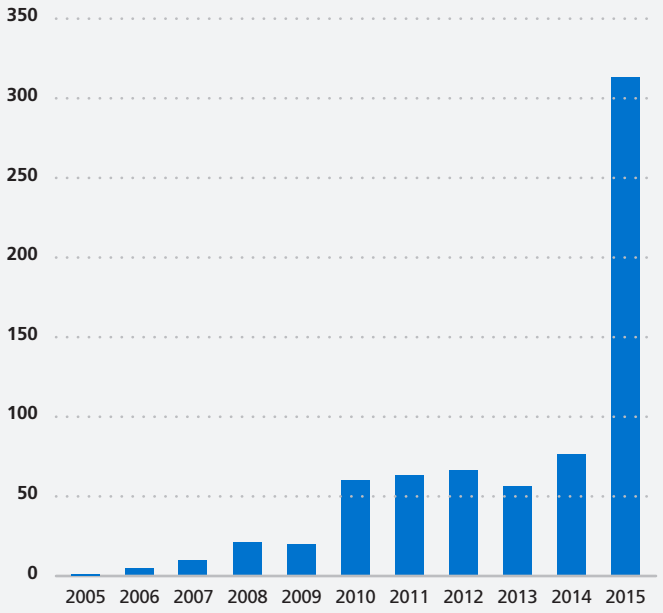


Figure 15: Adobe Flash vulnerabilities by year

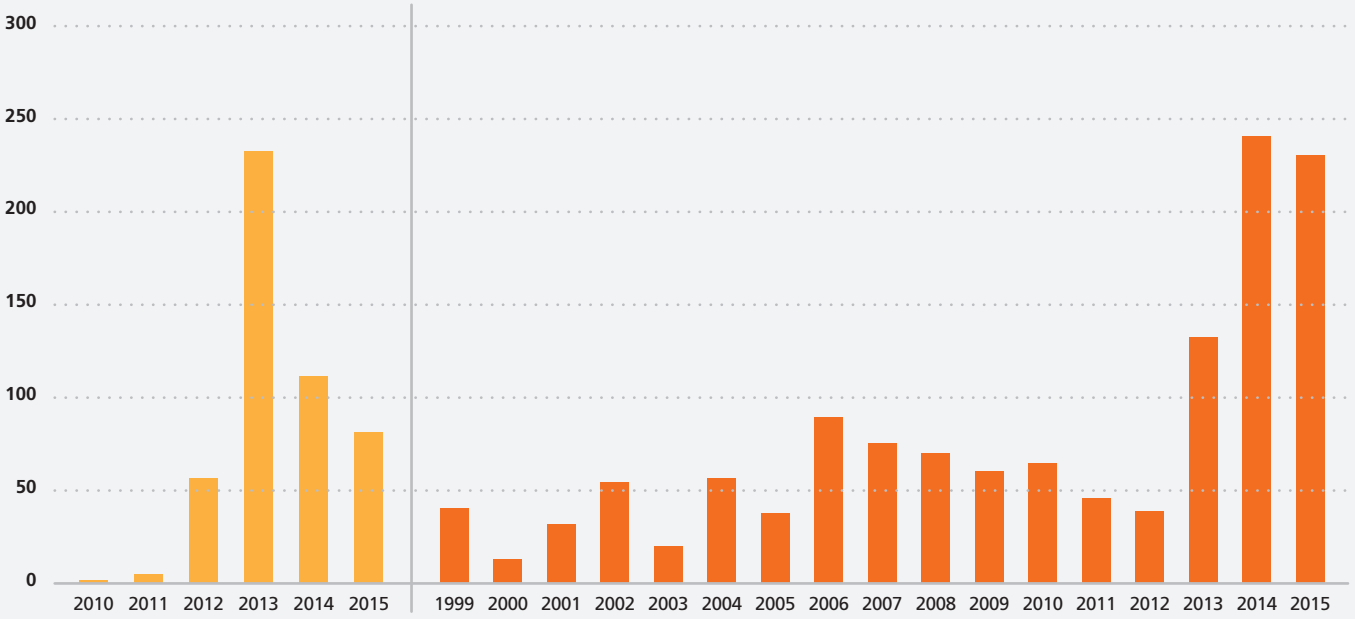


Figure 16: Java vulnerabilities by year

Figure 17: Internet Explorer vulnerabilities by year

Most popular vulnerabilities targeted in 2015 exploit kits

The 10 most popular vulnerabilities in exploit kits released in 2015 are listed in the table below[4].

CVE	Affected Technology
CVE-2015-0311	Adobe Flash
CVE-2015-5119	Adobe Flash
CVE-2015-5122	Adobe Flash
CVE-2015-0359	Adobe Flash
CVE-2015-0313	Adobe Flash
CVE-2015-2419	Adobe Flash
CVE-2015-3090	Adobe Flash
CVE-2015-3113	Adobe Flash
CVE-2015-0336	Adobe Flash
CVE-2015-7645	Adobe Flash
CVE-2015-3105	Adobe Flash

Figure 18: 10 most popular vulnerabilities in exploit kits

In 2013, only one Adobe Flash exploit was among the 10 most popular exploits included in exploit kits. In 2014, four Adobe Flash exploits were included in the top 10. In 2015, the top 10 list consists exclusively of Adobe Flash exploits.

In 2013, eight of the top 10 exploits were related to Java. In 2014, only four of the top 10 exploits involved Java. There are no Java vulnerabilities in the top 10 in 2015.

To reduce risks associated with exploit kits, organizations should consider the following:

- **Ensure effective patch management** – Exploit kits typically use exploits for which patches exist. Exploit kit developers take advantage of the time between initial vulnerability disclosure and the implementation of patches by end users or organizations. Ensuring effective patch management processes for end-user devices is a critical first step to protect against exploit kits. Organizations should pay particular attention to web browser plugins and technologies such as Adobe Flash. These do not have the same types of enterprise class rollout capabilities as Microsoft technologies, and organizations need to ensure there are tools in place to deploy and measure the adoption of patches.

- **Threat intelligence** – Threat intelligence services can help organizations identify vulnerabilities that are being actively exploited. These services act as a complementary control to patch management processes, helping ensure patching is prioritized for vulnerabilities that attackers are targeting.

- **Social engineering (phishing) training** – Exploit kits are most often delivered via social engineering and phishing attacks. Standard security awareness training is no longer adequate for organizations that maintain highly sensitive data. Organizations should implement real world social engineering testing for key employees, to confirm their ability to respond to actual phishing scenarios.

- **Ad blocking software** – Attackers frequently use malvertising to lure victims onto exploit kit landing pages. Use of ad-blocking software or Web proxies with content filtering can limit the effectiveness of this attack approach.

- **IP reputation services** – IP reputation services can warn or block users from visiting known bad IP addresses and domains. These services should only be considered a supplemental control. Addresses of exploit kits are constantly changing in order to evade detection, and the services are unlikely to maintain accurate and comprehensive real-time lists of landing page URLs. As discussed in the Global Honeynet Analysis section, attackers regularly use new IP addresses that have clean reputations, and URL blacklists take time to update.

- **Endpoint Protection** – Implementation of endpoint protection can help detect malware dropped on a device by an exploit kit before significant damage occurs.

[4] This table incorporates data from http://contagiodump.blogspot.com and http://malware.dontneedcoffee.com

Exploit Kit Details: Angler and Malvertising

NTT Group-CERT identified a series of malvertising attacks during 2015, most prevalently in Q3. Security researchers reported attacks against more than 3,000 Japanese websites with malvertising, with half a million users being exposed to the campaign. The targeted websites were mostly legitimate ones. The attack spread because users were infected through drive-by downloads from exploited legitimate websites.

NTT Group observed similar behavior during the same timeframe. The Angler exploit kit injected malware onto a victim's PC by exploiting vulnerabilities in Microsoft Internet Explorer, Adobe Flash Player and other client-based software.

Attackers installed additional malware – including ransomware and banking fraud malware – through the same process, summarized in Figure 19.

NTT Group worked with clients to identify and patch the vulnerabilities being exploited by Angler. NTT Group also helped blacklist URLs and IP addresses referenced in the campaign, and monitored the campaign to support additional updates. Once affected organizations began explicitly blacklisting sites involved, attacks were less successful. Forensic analysis of potentially exposed computers confirmed additional attacks had been unsuccessful. Because of blacklist management, the multistep redirection from legitimate website to malicious sites had failed.

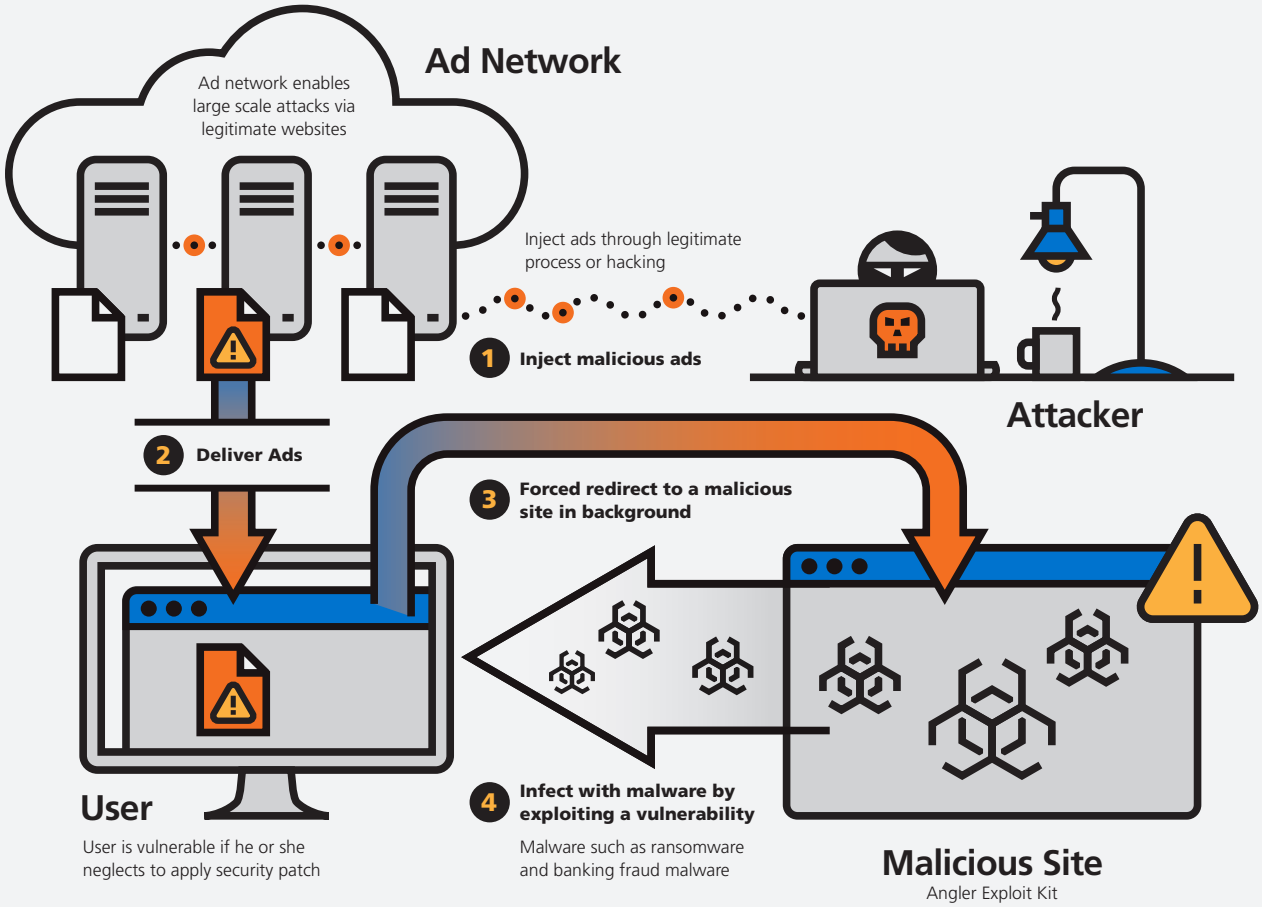
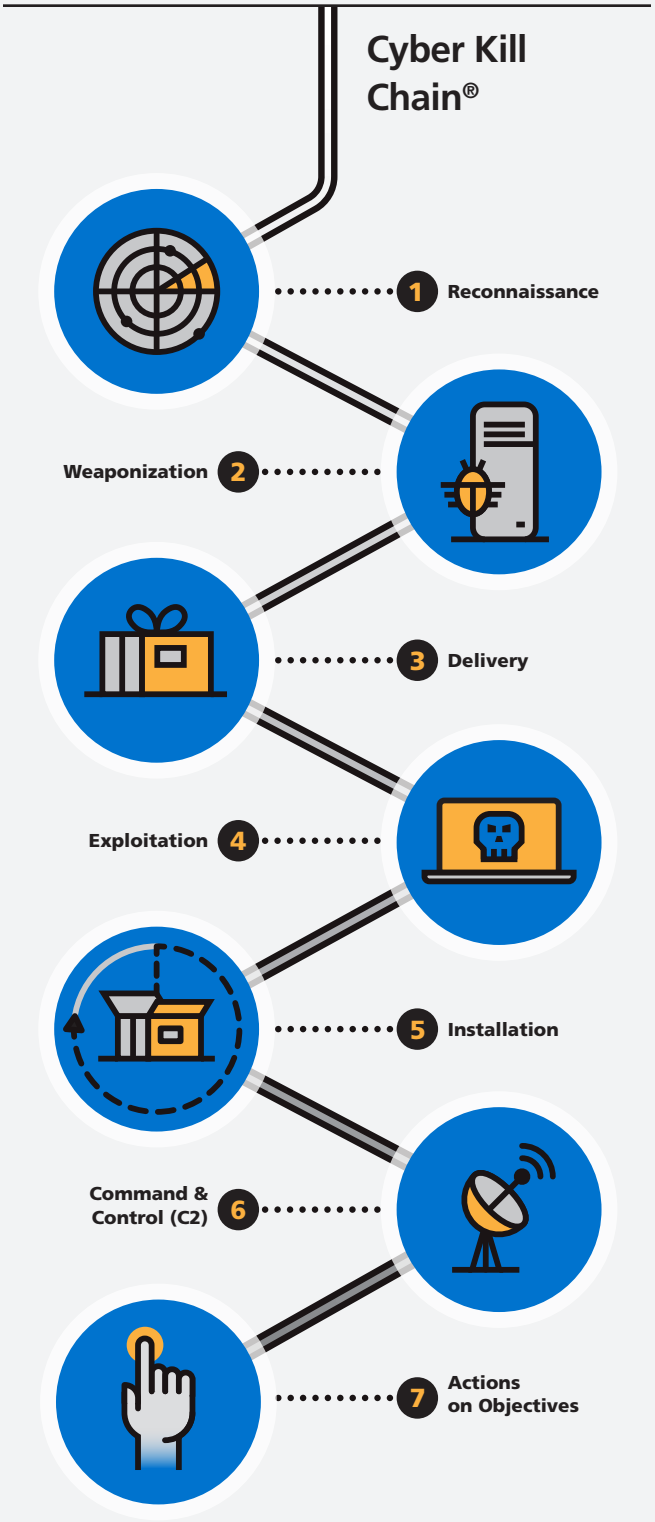


Figure 19: Malvertising via Angler

Practical Application of Security Controls to the Cyber Kill Chain®

The concept of a kill chain originated with the military, and was first applied to cyber intrusions in an influential 2011 paper by Hutchins, Cloppert and Amin of Lockheed Martin Corporation. It describes an "Intrusion Kill Chain" for cyber attacks using these phases:



The Cyber Kill Chain® analytical model proposes a few foundational elements. First, an attacker must progress through each of the above phases. Second, an attacker has not succeeded until they have accomplished Phase 7 (Actions on Objectives). Finally, defenders have an opportunity at each phase to interrupt the attack and prevent the intruder's success.

"The wonderful thing about standards is that there are so many of them to choose from."

– attributed to Andrew Tanenbaum, Grace Hopper, and others

Other paradigms exist for managing the cyber security process. One framework is the Center for Internet Security (CIS) Critical Security Controls (CSC) which include 20 detailed recommendations. The full text of the current version is available at https://www.cisecurity.org/critical-controls.

Why so many frameworks? Each provides its own view of the problem and points to potential solutions. The Solutionary whitepaper Defense Strategies for Advanced Threats: Mapping the SANS 20 Critical Security Controls to the Cyber Kill Chain relates these two frameworks with regard to defense against Advanced Persistent Threats (APTs). NTT Group recommends these frameworks because experience shows most organizations do not have a single plan for defending against cyberattacks. Following a framework for thinking about defensive and analytical actions leads to having a plan, and a successful defense absolutely requires a plan.

[5] http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Practical Application of Security Controls to the Cyber Kill Chain®

Why the Cyber Kill Chain?

Even among organizations lacking a cyber incident response plan, most have made significant investments in perimeter protection such as firewalls and intrusion detection/protection systems (IDS/IPS). This approach often depends on point solutions and a narrow view of the threat landscape. It leaves organizations vulnerable to phishing emails, browsing of infected websites, portable media devices, BYOD (mobile) devices and malicious employees. These and other paths to compromise lead us to conclude most organizations will be the victim of some level of compromise. It is important, however, to recognize that even if an attack occurs, the Cyber Kill Chain illuminates opportunities across the seven phases to limit the damage associated with attacks. Organizations need to focus on reducing the potential impact of attacks and creating reinforcing layers of defensive opportunities across the entire Cyber Kill Chain. This framework identifies numerous ways organizations can improve their defense against attacks, seizing on the inherent advantages defenders have over their adversaries[6].

To an attacker using commodity resources the cost of sending a million phishing emails is negligible, and the success rate correspondingly low. On the other end of the spectrum, targeted threats may require significant time and effort to orchestrate, moving through discrete phases of the Cyber Kill Chain. Kill chain analysis illustrates the adversary must progress successfully through each phase of the chain before it can achieve its desired objective, while just one successful mitigation can disrupt the chain and the adversary.
With the Cyber Kill Chain and the Critical Security Controls, organizations gain:

- Better visibility and understanding of layered controls that can protect against each step in the Cyber Kill Chain
- The opportunity to identify attacks earlier in the Kill Chain, minimizing their impact and maximizing defensive effectiveness
- Opportunities to detect late stage attacks after an attacker already has a presence in the network, but before they have been able to exfiltrate data from the environment.

Case Study Overview

In this, the 2016 GTIR, we are presenting a detailed case study of a real-world attack as responded to by NTT Group incident response teams. We follow the trail of an attacker progressing through the seven phases of the Cyber Kill Chain, ultimately exfiltrating data from a financial institution's membership database. The case study focuses on actions occurring during each of the attack's seven Cyber Kill Chain phases. In each step NTT Group presents an overview, with targeted and disruptive countermeasures, standard recommendations, and additional details to aid in understanding the case study. These recommendations are not meant to be all-inclusive, but to represent controls that can be effective at interrupting an attacker's progression through the Cyber Kill Chain-

CIS controls are defined in a practical, actionable way, enabling organizations to implement them in a meaningful manner.

Targeted and Disruptive Countermeasures highlight specific controls organizations can implement to address each phase of the Cyber Kill Chain, focusing on individual actions that can be taken to hinder or halt an attacker's progress. While many of these countermeasures apply to multiple kill chain phases, for this document they are only presented in the phase for that they are expected to have the greatest impact.

Standard Recommendations are listed in the introductory infographic, but not discussed in this document. Standard Recommendations are controls that should be well known, have proven valuable and have been promoted within the security community for some time.

[6] http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Practical Application of Security Controls to the Cyber Kill Chain®

Each step also includes references to areas in the CIS Critical Security Controls. The CIS controls are defined in a practical, actionable way, enabling organizations to implement them in a meaningful manner.

Organizations should expect the majority of well-implemented security controls to affect multiple phases in the kill chain. Realistically, there are a few that may even affect all phases in the kill chain, like implementation of a true security awareness and training program, and an effective threat intelligence plan. But, in the end, all controls serve components of a unified security program intended to protect the organization's information assets.

Cyber Kill Chain Phase 1
Reconnaissance

Definition: As defined by Lockheed Martin, this phase in the Cyber Kill Chain consists of activities related to "Research, identification and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies.[7]"

Defender Objective: Limit Reconnaissance and reduce the attacker's ability to enumerate the target's footprint.

1 Reconnaissance — 2 Weaponization — 3 Delivery — 4 Exploitation — 5 Installation — 6 Command & Control — 7 Actions on Objective — E

Targeted and Disruptive Countermeasures:

- Determine focus of reconnaissance activity
- Use search engines to ensure private information has not been publicly disclosed
- Manage thresholds for source volume traffic and type
- Perform proactive penetration testing
- Identify internal reconnaissance

Standard Recommendations:

- Monitor external exposure
- Install, configure and manage host and network-based IDS/IPS
- Update and maintain proper ACLs

Critical Security Controls:

- CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
- CSC 9: Limitation and Controls of Network Ports, Protocols, and Services
- CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- CSC 12: Boundary Defense
- CSC 20: Penetration Tests and Red Team Exercises

[7] Lockheed Martin Resource: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Cyber Kill Chain Phase 1: Reconnaissance

Case Study Timeline, Observations and Impact

The chronology of events related to the Reconnaissance phase is provided in the following timeline.

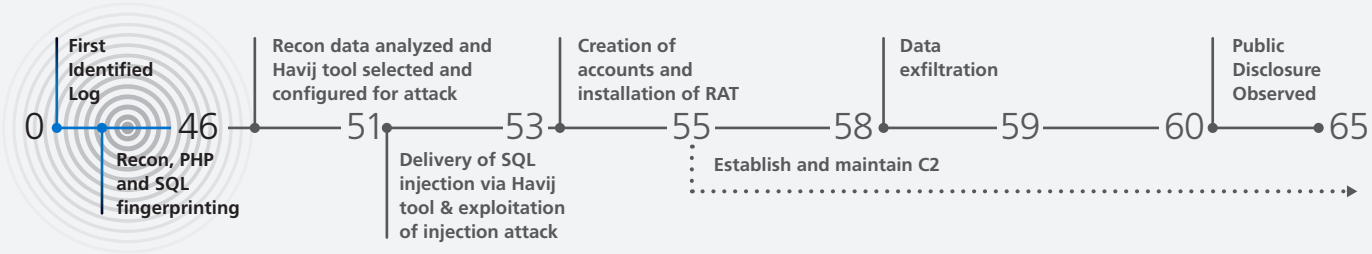


Figure 20: Timeline of events – Reconnaissance

The first signs of adversary activity at Peaceful Panda Financial Corporation[8] (PPFC) were reconnaissance activities taking place nearly two months before any intrusion occurred. The adversary scanned external systems to enumerate specific applications, systems and services in order to build a profile of the attack surface. This proved to be a critical phase in the CKC as the adversary was able to identify weaknesses in the organization's structure and technologies, providing the initial point of entry for the subsequent attacks.

Although PPFC was conscious of the need to log system, application and database events, their implementation was not designed to use those logs for defense. Some of the key challenges in spotting reconnaissance activity included:

- **The ability to identify the attack in real time** – Although PPFC was collecting information about malicious activity, it did not have a formal SIEM implementation performing aggregation, correlation or real time analysis of security events.
- **Existing log and event storage policies** – All systems were configured to log events on a centralized server; however, logs were overwritten after two months due to storage capacity limitations. This meant PPFC was unable to identify when reconnaissance activity started.
- **Selection of log types** – Only system, health and database performance logs were stored. Logs related to security events were not captured due to a lack of storage capacity, drastically reducing awareness of potential attacker activity.
- **Review of logs and event data** – The organization performed log and event analysis only when there was a noticeable decrease in network and application performance, further reducing the defensive value of the logs and the ability to detect attacker activity at early stages.

Cyber Kill Chain Considerations

The reconnaissance phase poses some unique challenges to defenders. Reconnaissance can include a broad range of activities, many of which are not inherently malicious (e.g., accessing press releases), and that can occur completely outside of the target's environment and control (e.g., search engines, social networks). Successfully identifying reconnaissance activity can improve your defensive posture by indicating what people, systems, or applications are likely to be targeted.

The sooner an organization can take actions to disrupt the attacker's progress through the kill chain, the better. Proper investment in detection capabilities that help identify and understand these early attack steps can be a significant advantage when trying to mitigate attacks before they reach their full potential. If the organization can understand what the attacker is targeting, it can take action to prevent success at later phases of the CKC through knowledge of the adversary's intent, capabilities and objectives.

[8] Not the actual company name

Reconnaissance activity observed by NTT Group accounted for nearly 89% of all log management volume and resulted in approximately 35% of escalated event activity.

In some cases, reconnaissance activity is only identified retroactively via post-incident analysis. Correlation of attack activity and preceding reconnaissance activity can help an organization understand where to strengthen its entire security program.

Targeted and Disruptive Countermeasures

These targeted and disruptive countermeasures have the potential to disrupt the attacker's activities during the current kill chain phase, hindering their ability to successfully move on to subsequent phases of the attack.

- **Determine focus of reconnaissance activity** – Is the activity observed across your entire IP space or just on one system? Is the activity targeting a specific set of ports (HTTP, SSH, etc.)? Evaluate reconnaissance activity, and focus mitigation directly against the areas undergoing reconnaissance. For example, if an attacker is conducting a brute force attack against your SFTP server, consider if that system needs to be available to the entire internet, or can controls be implemented to only allow connections from specific IP addresses? Is the SFTP server mission critical or can it be taken offline temporarily? Are there are other controls you can implement to directly protect the target of the reconnaissance?

- **Use search engines to ensure private information has not been publicly disclosed** – Disrupt any steps by the attacker to gain information by "passive" reconnaissance. This could include social engineering, exploring employee social media sites, gathering usernames and passwords, employee email addresses and much more. Attackers regularly leverage internal information dumped to sites like Pastebin by a disgruntled employee or previous threat actor. This information should be removed immediately, and credentials should be invalidated.

- **Manage thresholds for source volume traffic and type** – Reconnaissance and fingerprinting activities can be verbose and often originate from a limited number of IP addresses. Implementing thresholds in IDS/IPS, firewalls and SIEMs to identify potentially malicious activities or shun data-intensive attacks can reduce the attacker's ability to gather information in an automated manner. This can be an effective defense against high volume activity, but may have limited success against attackers using evasion techniques.

- **Perform proactive penetration testing** – Perform penetration testing to identify what an attacker could see using reconnaissance activities. Then, take action to hide or obfuscate information that was revealed to limit what can be gathered via reconnaissance.

- **Identify internal reconnaissance** – Not all reconnaissance is external. Attackers perform internal reconnaissance to expand attacks laterally through the infrastructure. Such reconnaissance may be harder to identify. Be aware of internal reconnaissance such as internal scans or probes. Organizations can leverage knowledge of their own environments by defining formal network segregation and hardening internal systems, and help prevent successful internal reconnaissance.

Cyber Kill Chain Phase 2
Weaponization

Definition: As defined by Lockheed Martin, this phase in the CKC consists of activities related to "coupling a remote access Trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Increasingly, client application data files such as Adobe Portable Document Format (PDF) or Microsoft Office documents serve as the weaponized deliverable.[9]"

Defender Objective: Interpret potential weaponization based on available information to disrupt future stages.

1 Reconnaissance · 2 **Weaponization** · 3 Delivery · 4 Exploitation · 5 Installation · 6 Command & Control · 7 Actions on Objective · E

Targeted and Disruptive Countermeasures:

- Application of threat intelligence
- Use honeypots for protection and detection signatures
- Train the incident response team to be prepared for the unexpected
- Determine what reconnaissance took place
- Identify weaponization characteristics

Standard Recommendations:

- Implement a configuration management program
- Perform formal risk assessments
- Implement robust log monitoring
- Actively enable internal communication

Critical Security Controls:

- CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers.
- CSC 9: Limitation and Controls of Network Ports, Protocols, and Services
- CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
- CSC 19: Incident Response and Management

[9] Lockheed Martin Resource: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Cyber Kill Chain Phase 2: Weaponization

Case Study Timeline, Observations and Impact

The chronology of events related to the Weaponization phase is provided in the following timeline.

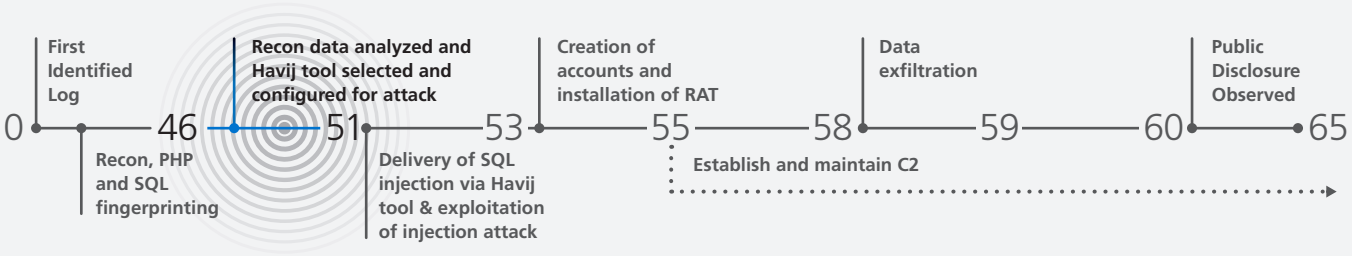


Figure 21: Timeline of events – Weaponization

Weaponization occurs outside of the defender's environment, so it is often impractical to detect the actual act of weaponization as it occurs. In our case study, the attacker reviewed the results of their reconnaissance, then selected and configured the Havij tool to conduct automated SQL injection attacks against PPFC.

At this point of the attack, PPFC could have been in position to identify the results of reconnaissance that had taken place, and could have used that information to identify potential targets. PPFC successfully logged scanning against Web applications, specifically PHP and SQL statements that were indicative of a future attack. If PPFC had identified SQL scans, for instance, they might have been able to determine that a potential attacker was targeting SQL injection weaknesses. This could have provided PPFC with the opportunity to take additional actions to protect themselves from this attack vector. Instead, PPFC did not detect that they were being scanned, and so did not take any defensive actions.

In later phases, PPFC may be able to identify indicators or "tool marks" left behind. Some of the key challenges in identifying weaponization activity included:

- PPFC was logging security events, but had no capacity to review them or to identify any activity that could have provided clues of the attacker's intent.
- Even if they had been reviewing logs and events, PPFC had no meaningful incident response process that could have helped focus their follow-on activity. Well-developed incident response procedures are critical, as discussed in the section titled Incident Response: Trend Shows Organizations Are Not Prepared.

Cyber Kill Chain Considerations

The act of weaponization is to adapt something for use as a weapon. During this phase, the attacker will use information collected during the Reconnaissance phase to identify their attack vector, then select and configure the weapon of choice. This may be packaging an exploit and malware with a benign PDF (accomplished using a "weaponizer"), but can also include other preparatory actions such as customizing tools and techniques to take advantage of weaknesses discovered during Reconnaissance, as it did in this case. Attackers will also employ countermeasures to evade detection and minimize the target's ability to trace the attacks back to the source.

Targeted and Disruptive Countermeasures

These targeted and disruptive countermeasures have the potential to disrupt the attacker's activities during the current kill chain phase, hindering their ability to successfully move on to subsequent phases of the attack.

- **Application of threat intelligence** – Gather and apply intelligence about potential adversaries, along with their tactics, techniques and procedures (TTP), and be prepared to track attack activity before it is generated. Identify trends that can enable other disruptive countermeasures. Without an effective means of tracking

information and threat intelligence, defense is considerably more difficult and becomes more reactive. By enabling defenders to track, correlate and better understand attacks, you are better able to proactively identify indications of adversary activity. This is a critical component of establishing a proactive defensive posture, as discussed in the section titled The Role of the Cyber Kill Chain in Threat Intelligence.

- **Use honeypots for protection and detection signatures** – Properly configured honeypots or honeynets can be an appealing target for attackers. Attackers may continue their intrusion efforts within the honeynet that is segmented from the true organizational environment. Attacks being used in the honeypot can reveal information about attacker TTPs, which can lead to additional detection and mitigation methods (e.g., HIPS, AV, IDS/IPS).

- **Train the incident response team to be prepared for the unexpected** – There is great value in preparing for the most likely attacks and ensuring a highly efficient response, but preparing to meet the unexpected is at least as valuable. Incident response teams must train continuously and ensure they include challenging situations as part of the training.

- **Determine what reconnaissance took place** – Understanding reconnaissance activities may give insight into what the attacker is planning. If the attacker scanned the DB, watch for DB activity like SQLi unauthorized access. If the attacker scanned for Cold Fusion, prepare for exploit attempts against Cold Fusion. Detecting the objectives of incoming reconnaissance can enable the organization to disrupt impending delivery efforts.

- **Identify weaponization characteristics** – Capitalize on opportunities to detect and mitigate threats based on weaponization characteristics to prevent attacks from reaching later phases. Understand the "tool marks" (artifacts, metadata, structures, attributes) which indicate that weaponization techniques were used. For instance, the word "Havij" is often found in the default user-agent text associated with Web requests generated by the tool. If the organization finds this text, it is a clear indicator the attacker is using the Havij tool.

Weaponization occurs outside of the defender's environment, so it is often impractical to detect the actual act of Weaponization as it occurs.

Cyber Kill Chain Phase 3
Delivery

Definition: As defined by Lockheed Martin, the Delivery phase in the Cyber Kill Chain consists of activities related to "Transmission of the weapon to the targeted environment. The three most prevalent delivery vectors for weaponized payloads by APT actors, as observed by the Lockheed Martin Computer Incident Response Team (LM-CIRT) for the years 2004-2010, are email attachments, websites, and USB removable media.[10]"

Defender Objective: Identify activity as hostile and interrupt the delivery of malicious content, forcing the attacker to change tactics.

1 Reconnaissance · 2 Weaponization · 3 Delivery · 4 Exploitation · 5 Installation · 6 Command & Control · 7 Actions on Objective · E

Targeted and Disruptive Countermeasures:

- Manage browser security
- Enable whitelist management
- In-line anti-virus
- Effective configuration and management of Web application firewall (WAF)
- Automatic device fingerprinting
- Implement a secure Web gateway (SWG)

Standard Recommendations:

- Enable verbose logging
- Manage peripheral security
- Assess physical security
- Implement professional security awareness and training
- Implement email filtering and sanitization
- Perform proper blacklist management
- Install in-line anti-virus
- Develop secure Web applications
- Implement and maintain sound identity access management

Critical Security Controls:

- CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers.
- CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
- CSC 7: Email and Web Browser Protections
- CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- CSC 13: Data Protection
- CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps

[10] Lockheed Martin Resource: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Cyber Kill Chain Phase 3: Delivery

Case Study Timeline, Observations and Impact

The chronology of events related to the Delivery phase is provided in the following timeline.

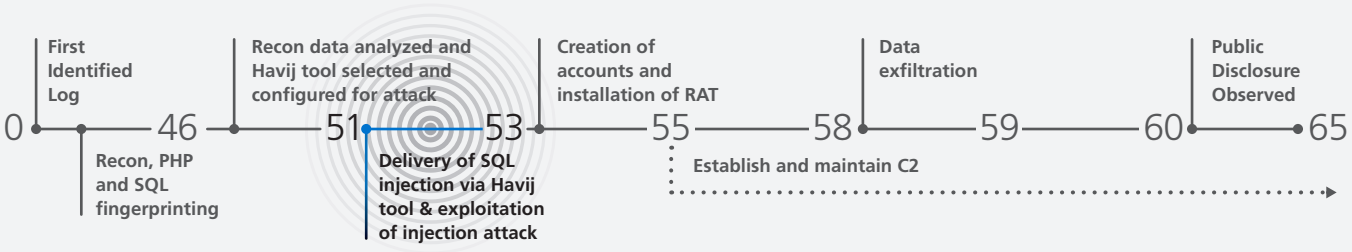


Figure 22: Timeline of events – Delivery

The attacker used the Havij tool to send Web requests designed to execute an SQL injection attack. These specially crafted payloads performed the Delivery phase in the form of Web application requests, advancing the attack. This activity appeared in PPFC Web and security logs, but since PPFC was not reviewing or processing security event logs, the attacks went undetected.

Delivery took place in a mostly automated manner, conducted by preconfiguring the Havij tool and pressing a button to launch the attack. The attacker then monitored the tool, watching for indications of success or failure of the delivered attacks, as commands executed on the target.

Cyber Kill Chain Considerations

The Delivery phase of the Cyber Kill Chain is the first chance an organization has to genuinely disrupt the attacker's progress.

Targeted and Disruptive Countermeasures:

These targeted and disruptive countermeasures have the potential to disrupt the attacker's activities during the current kill chain phase, hindering their ability to successfully move on to subsequent phases of the attack.

- **Manage browser security** – Enforce proper patch management and security settings on Web browsers. Typically, a victim is lured to a malicious website through redirection where a payload is delivered. Since these attacks exploit vulnerabilities in the victim's Web browser or applications, the attacks can be made ineffective if the Web browser and plug-ins are up-to-date and thus not vulnerable. Configuring a browser's security and privacy settings can also disrupt delivery of malicious payloads.

- **Enable whitelist management** – A common security control is blacklisting sites and applications that are known to be malicious. Blacklists enforce statements like, "don't go to these known bad websites" and "reject email from these known bad domains." Whitelisting would include sites that are "known good;" that is, sites that users would have valid business reasons to visit. If a site is not on the whitelist, it is automatically blocked. This is not a practical solution for every environment, but may be effective for sensitive environments where interactions are well defined.

- **In-line anti-virus** – Anti-virus/anti-malware products and real-time heuristics can be used to analyze emails or attachments and automatically block such objects. Hash values calculated by anti-virus services could be correlated to a threat intelligence database for validity, based on multiple open source resources to help inhibit the delivery of malicious objects. Organizations should develop the ability to deeply inspect objects as they enter the environment, enabling defenders to better understand the attacker's tools and further improve defenses.

- **Effective configuration and management of Web application firewall (WAF)** – WAFs analyze the traffic between Web-based devices, software and services. WAFs focus on Layer 7 (application) security, analyzing packets associated with Web traffic only. This can provide the ability to detect delivery of payloads against public-facing sites.

- **Automatic device fingerprinting** – Anyone with a mobile device – their own or one belonging to the company – could use it to deliver a malicious payload onto the organization's network. Mobile device connections can be denied with systems such as Cisco ISE by fingerprinting a device to identify its make, model and manufacturer. DHCP servers can also be used to block (or allow) smartphone MAC addresses. Without being able to control who has access to your employee devices outside the office, it is important to control who is connecting such devices to your corporate environment.

- **Implement a secure Web gateway (SWG)** – SWGs can help prevent end users from installing backdoor malware variants. These provide URL filtering, HTTP/S scanning, application control and much more. This can be important if end user Web browsing is necessary on the targeted systems. Flexible SWGs allow for easy administration and validation of email and data – email attachments are a common technique used to deliver backdoor malware variants.

Just under 5% of all verified events fell within the Delivery step of the Cyber Kill Chain, making it the step with the second fewest events.

Cyber Kill Chain Phase 4
Exploitation

Definition: Lockheed Martin defines the Exploitation phase of the Cyber Kill Chain as follows: "After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability, but it could also more simply exploit the users themselves or leverage an operating system feature which auto-executes code.[11]"

Defender Objective: Focus controls to minimize exploitation opportunities, reducing vulnerabilities, forcing the attacker into alternate or noisier attacks.

1 Reconnaissance · 2 Weaponization · 3 Delivery · **4 Exploitation** · 5 Installation · 6 Command & Control · 7 Actions on Objective · E

Targeted and Disruptive Countermeasures:

- Implement application/process sandboxing
- Perform proactive penetration testing
- Remove externally facing remote administration consoles for Web applications
- Use purpose-built tools such as the Enhanced Mitigation Experience Toolkit (EMET)
- Implement application whitelisting
- Implement Data Execution Prevention (DEP)
- Perform address space layout randomization

Standard Recommendations:

- Implement multifactor authentication
- Eliminate unneeded services and protocols
- Implement a patch management process
- Implement a vulnerability management program
- Use secure host baselines for system deployment
- Create and test incident response plans ahead of time
- Perform formal risk assessments

Critical Security Controls:

- CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers.
- CSC 4: Continuous Vulnerability Assessment and Remediation
- CSC 8: Malware Defense
- CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps

[11] Lockheed Martin Resource: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Cyber Kill Chain Phase 4: Exploitation

Case Study Timeline, Observations and Impact

The chronology of events related to the Exploitation phase is provided in the following timeline.

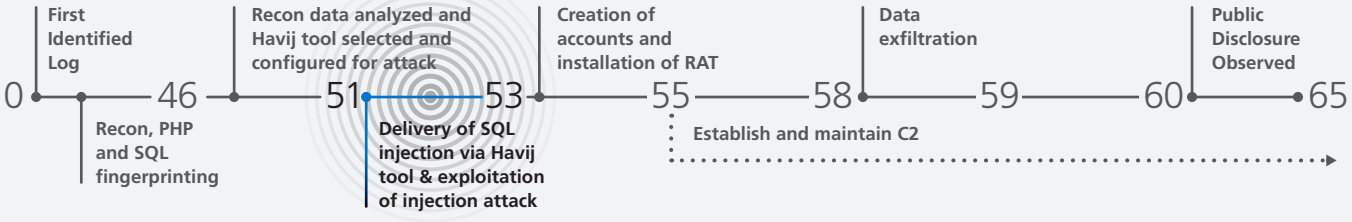


Figure 23: Timeline of events – Exploitation

Post incident investigation revealed the exploitation of vulnerabilities started approximately nine days prior to disclosure of PPFC customer information on a public "paste site." After information was made public, security analysts reviewed Web and security logs to identify successful Havij-based SQL injection attacks. The exploitation was not identified until after the attack was made public.

The attacks against PPFC took advantage of a vulnerability in the design of a PHP-driven website that failed to properly use parameterized queries within several Web forms. Post incident analysis identified the attacker's progress through multiple phases of exploitation, including steps taken to validate SQL server type, enumeration of users, databases, tables and information schema. The attacker was able to systematically export the entire customer database and perform additional steps to maintain persistence (discussed in more detail in the Installation and Command and Control phases of this case study).

Some of the key challenges in preventing successful exploitation activities include:

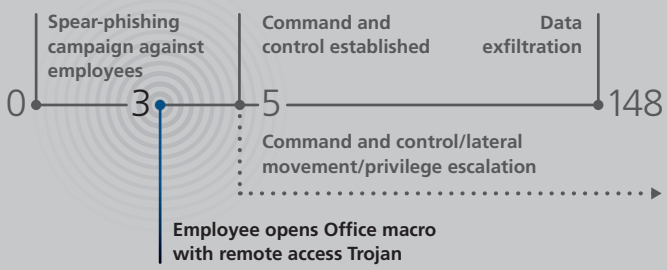
- **Application development and security practices** – Attacks such as SQL injection and cross site scripting are can be limited if organizations enforce secure coding practices. This attack may have been avoided if security testing had been part of the software development process

- **Web application attack detection and prevention capabilitie**s – PPFC conducts approximately 40 percent of its transactions online, during which many pieces of sensitive information are collected. Despite the significant portion of online business, no protection measures were

  taken to mitigate targeted attacks against the Web site, application or supporting database.

Advanced Threat – Phase 4 Exploitation

Other modern attacks work in a similar sequence, but with a different timescale. The timeline to the right is for a compromise that was the result of a successful spear-phishing attack of a customer. The victim opened the infected Office macro, and the exploit executed, infecting his machine with a remote access Trojan.



- **Vulnerability identification and remediation** – Although PPFC had conducted routine vulnerability tests of the Web application prior to compromise, the scan activity did not contain Web checks to identify common website vulnerabilities. Traditional vulnerability scanners do not provide robust identification of Web application vulnerabilities.

Cyber Kill Chain Considerations

Once the attacker has delivered their malicious payload (whether a weaponized attachment, a link to a weaponized Web page, or a specially crafted Web request), the next phase is Exploitation. The malicious payload, even if delivered, does not accomplish the attacker's objective if it is not able to execute or otherwise affect the target.

Traditionally, exploitation is thought of as vulnerabilities in applications and viewed in the context of vulnerability management. For many attacks and many environments, exploiting human behavior, and convincing a user to click a link or open an attachment, is the first (and sometimes only) exploitation needed.

Even after an attacker has successfully delivered his payload, defenders can still prevent the attack's success if they can interrupt the kill chain. Without exploitation, those payloads exist within the environment as a result of successful delivery but do not accomplish anything. Defenders have a tactical advantage if the delivery has been detected. At this point, the attacker has shown their hand and the organization should be able to analyze the attacker's capabilities and goals. The attacker only knows a binary value: did the attack advance to a later phase, or not?

Detection of both successful and failed exploit attempts is critical. Incident response teams can gain valuable information that may aid in determining where to focus analysis and forensic activities, as well as helping identify the scope of compromise.

Even after an attacker has successfully delivered his payload, defenders can still prevent the attack's success if they can interrupt the kill chain.

Targeted and Disruptive Countermeasures

These targeted and disruptive countermeasures have the potential to disrupt the attacker's activities during the current kill chain phase, hindering their ability to successfully move on to subsequent phases of the attack.

- **Implement application/process sandboxing** – Use a controlled host (sandbox) for analysis of potentially malicious programs. Running these programs in a sandbox allows analysis of network activity, program fingerprinting (hash), source code dissection and much more. Malicious payloads will cause no harm on the network if the sandbox is configured properly. For more details about sandboxes and the techniques attackers are using to evade them, see the Anti-sandbox Techniques section.

- **Perform proactive vulnerability testing** – Prior to an attack, an organization should perform its own penetration tests to determine the extent of their vulnerabilities. If the testing uncovers a vulnerability, there is a chance to take proactive actions by revising the network or applying appropriate patches, updates, and mitigating controls.

- **Remove externally facing remote administration consoles for Web applications** – Web platforms like PHP, and application platforms like WordPress or Joomla, often contain remote administration capabilities. These are used to manage the platform, but if exposed externally they can easily be exploited by attackers. These often provide the ability to upload files, giving attackers an easy path to installing webshells and backdoors.

- **Use purpose-built tools such as the Enhanced Mitigation Experience Toolkit (EMET)** – Currently supporting all Windows platforms, EMET is a free security tool that uses specific mitigation techniques to prevent exploits against memory corruption and buffer overflows.

- **Implement application whitelisting** – Whitelisting authorized software can help prevent tampered or customized programs from executing on a targeted system even if those programs appear to be legitimate. Organizations can implement integrity checks of applications or integrate program hashes, creating an additional layer of authorization.

- **Enable Data Execution Prevention (DEP)** – Data Execution Prevention is a security feature in most modern operating systems used to define whether certain areas of memory are executable or nonexecutable. This can disrupt certain exploits, buffer overflow attempts, and malicious code. Think of it as a firewall specifically for executable code that will deny or allow execution based on the area of memory.

- **Enable Address Space Layout Randomization** – Available on both Windows and UNIX platforms, ASLR can disrupt malicious payloads targeting buffer overflow vulnerabilities. This is achieved by using random memory address spaces for applications to run in and can make it difficult for exploits using a predetermined memory address.

Cyber Kill Chain Phase 5
Installation

Definition: Lockheed Martin defines the Installation phase of the Cyber Kill Chain as "Installation of a remote access Trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.[12]"

Defender Objective: Inhibit the installation of malware and other actions, interfering with the attacker's ability to establish and maintain persistent access.

1 Reconnaissance · 2 Weaponization · 3 Delivery · 4 Exploitation · **5 Installation** · 6 Command & Control · 7 Actions on Objective · E

Targeted and Disruptive Countermeasures:

- Only enable command-line based tools and features when necessary
- Implement user behavior monitoring and behavioral detection/prevention capabilities
- Implement file execution restrictions
- For Windows environments, configure User Account Controls (UAC)
- Configure and manage multi-layered firewalls (MLF)

Standard Recommendations:

- Enforce "least privilege" settings
- Ensure processes and batch jobs do not use hard coded credentials
- Assess system and database user account security

Critical Security Controls:

- CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers.
- CSC 4: Continuous Vulnerability Assessment and Remediation
- CSC 8: Malware Defense

[12] Lockheed Martin Resource: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Cyber Kill Chain Phase 5: Installation

Case Study Timeline, Observations and Impact

The chronology of events related to the Installation phase is provided in the following timeline.

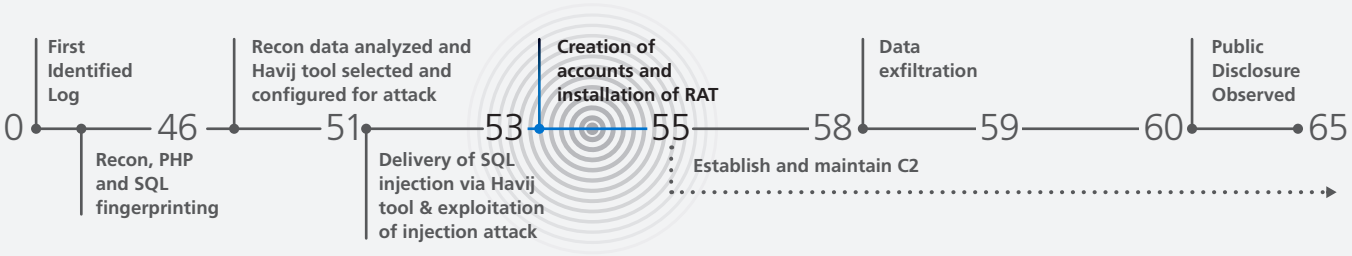


Figure 24: Timeline of events – Installation

The attacker used SQL injection to execute commands against the database, perform discovery on the database tables, and extract data. The attacker saw that the extracted data was valuable, so they used additional injected SQL commands to create a new database administrative user. That account was used to create a user account on the underlying operating system, which was then used to download and install a remote access Trojan (RAT). This provided the attacker with greater access to both the database and to the system on which the database ran, and persistent remote access through the RAT. Most of these actions were captured in logs, but were not identified as hostile until after the attack was made public.

Some of the key challenges in preventing successful installation activities include:

- **Active monitoring of the environment** – Active monitoring of the organizational environment can provide the organization the opportunity to identify and react to an attack in progress. In PPFC's case, the attacker made little effort to be stealthy, so it is likely any significant monitoring would have helped them detect this activity.

- **Modern malware is designed to evade detection** – Much of the advanced malware used by modern attackers includes a variety of stealth techniques that help avoid detection. While anti-malware solutions can help, organizations cannot solely rely on them to remain safe from an advanced attacker.

Cyber Kill Chain Considerations

The Installation phase of the kill chain is important for the attacker to continue an attack. If the attacker wants to establish access, investigate the target environment, extract information or use the victim's systems for additional attacks, it is crucial for the attacker to create a persistent presence. In some cases, persistence may consist of creating an account to facilitate later steps (e.g., access or export of data from the database).

It is important organizations plan security controls to disrupt an attacker's persistence before a breach occurs. This can help to defeat Installation activities, and to disrupt activities in other phases of the kill chain.

Targeted and Disruptive Countermeasures

These targeted and disruptive countermeasures have the potential to disrupt the attacker's activities during the current kill chain phase, hindering their ability to successfully move on to subsequent phases of the attack.

- **Only enable command-line based tools and features when necessary** – Upon delivery, a customized exploit does not necessarily have to be an executable binary payload, but could also be a customized script leveraging available command-line tools such as Windows PowerShell and Linux terminals. For most end users, these tools are not necessary and should be never be installed or enabled.

- **Implement user behavior monitoring and behavioral detection/prevention capabilities** – As attackers become better at avoiding detection defenders should consider more dynamic means of identifying

malicious activity. Behavioral monitoring uses multiple technical implementations ranging from anomaly detection, to machine learning, to identifying unexpected activity that can often be malicious.

- **Implement file execution restrictions** – File execution restrictions can be accomplished in a number of ways ranging from Group Policy Objects (GPO) to host intrusion prevention systems (HIPS). Regardless of the technical controls used, the objective for defenders is to prevent the installation and execution of malware. Preventing execution of applications from unapproved locations or from external origins (e.g., the Internet) can stop malware from being installed.

- **For Windows environments, configure User Account Controls (UAC)** – UACs can be leveraged to detect activity that requires higher privileges. During this detection, the user is prompted to enter the administrative password. Bots conducting malicious activity in real-time based on commands sent from the C2 server could be disrupted if credentials are needed before proceeding.

- **Configure and manage multi-layered firewalls (MLF**) – MLFs provide further verification of network traffic, typically via firewall ACLs and OSI layer 2 (data link), 3 (network) and 4 (transport) inspection. Such firewall architectures can process high-level policies provided by the administrator, as well as deep data analysis during packet inspection. Maintaining aggressive "deny or allow" rules, MLFs can disrupt backdoor setup or access attempts.

Installation activity observed by NTT Group accounted for less than 0.2% of all log volume and approximately 2% of all escalated event activity, making it one of the highest confidence types of event.

Cyber Kill Chain Phase 6
Command and Control (C2)

Definition: Lockheed Martin explains this phase as: "Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel. APT malware especially requires manual interaction rather than conduct activity automatically. Once the C2 channel establishes, intruders have 'hands on the keyboard' access inside the target environment.[13]"

Defender Objective: Disrupt the attacker's ability to retain long-term remote access, and end his hostile access.

1 Reconnaissance · 2 Weaponization · 3 Delivery · 4 Exploitation · 5 Installation · **6 Command & Control** · 7 Actions on Objective · E

Targeted and Disruptive Countermeasures:

- Ensure proper network segmentation
- Revert to disruptive tactics from reconnaissance
- Restrict peer-to-peer (P2P) traffic
- Set thresholds for DNS queries by a single machine
- Block communication to the external C2 server
- Use DNS sinkholes
- Implement aggressive domain categorization blocking

Standard Recommendations:

- Implement ingress and egress monitoring
- Implement auditing/traffic logging
- Implement log monitoring
- Implement authenticated proxies

Critical Security Controls:

- CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers.
- CSC 5: Controlled Use of Administrative Privileges
- CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
- CSC 9: Limitation and Controls of Network Ports, Protocols, and Services
- CSC 16: Account Monitoring and Control

[13] Lockheed Martin Resource: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Cyber Kill Chain Phase 6: Command and Control (C2)

Case Study Timeline, Observations and Impact

The chronology of events related to the Command and Control (C2) phase is provided in the following timeline.

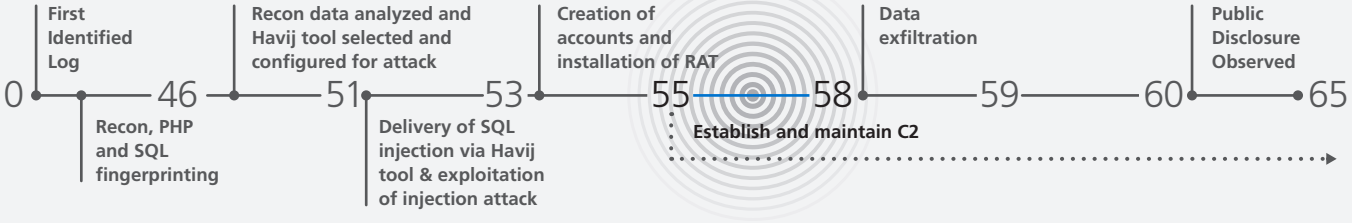


Figure 25: Timeline of events – Command and Control

Up to this point in the attack, the attacker was able to establish persistence and set up connectivity to a command and control infrastructure via installation of the RAT. During the C2 phase, the RAT communicated with a remote IRC server and obtained instructions from attacker-controlled profiles on a popular social media site. The RAT periodically queried content posted on the profile and interpreted the content as instructions for further malicious activity. Some of these communications were recorded in logs, but at PPFC only identified them as "hostile" once analysts started looking for anomalous behavior.

The attacker successfully established an ongoing presence in the PPFC environment using multiple C2 channels, and demonstrated an intent to further expand their access and continue exploitations within PPFC. A significant challenge in spotting such C2 activity is detecting it among all of the valid network activity.

Cyber Kill Chain Considerations

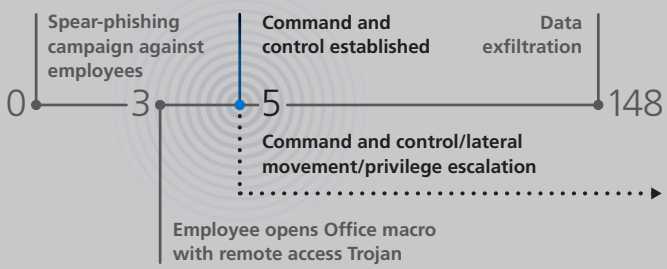
It is critical to realize that even in this late phase, defenders can still be successful if they can prevent C2 from occurring. The attacker cannot leverage the access they've gained until C2 has been successfully established. Even if the attacker has successfully installed a RAT on a host, if the attacker cannot interact with it, they will be unable to accomplish their objective.

Command and Control provides the attacker with direct control over target systems, and provides them the ability to return to the environment at leisure to take further action (e.g., data exfiltration, destruction, or manipulation). In many attacks, C2 continues for months before the attacker is able to access and extract targeted data from the victim's environment. C2 also allows the attacker to pivot from the initially compromised systems to different systems within the target's environment.

None of these outcomes are possible if the defender identifies and blocks C2 communications, and remediates compromised internal systems. Organizations should be aware that many C2

Advanced Threat – Phase 6 Command and Control

In the alternate example, the hostile attachment was executed and the attacker spread their compromise laterally through the environment. In the case of this attack, the C2 phase lasted 143 days, during which the attacker demonstrated extended and persistent access to systems within the targeted environment.



systems have alternate means of communicating. Blocking one channel while leaving others open not only fails to stop the attack, it also creates a false sense of security which can buy the attacker time to entrench themselves further.

Targeted and Disruptive Countermeasures

These targeted and disruptive countermeasures have the potential to disrupt the attacker's activities within the current kill chain phase, and will interfere with their ability to successfully move on to subsequent phases of the attack.

- **Ensure proper network segmentation** – Integrating network segmentation with detection and alerting could stop further activity by a compromised host. Proper segmentation includes ACLs and internal firewalls which support approved communications and help block unauthorized activity, in a cohesive network architecture. Identification of unauthorized internal communication can help reduce the chances of lateral compromise.

- **Revert to disruptive tactics from reconnaissance** – Although the threat may be far into the intrusion process and the attacker may have successfully established command and control, it is common for an attacker to use compromised hosts to conduct further reconnaissance on internal systems. Such access essentially repeats the kill chain phases for each successive extension of the breach, starting with internal reconnaissance. Organizations should monitor for internal to enable detection and blocking of this behavior.

- **Restrict peer-to-peer (P2P) traffic** – Organizations may support P2P tools such as Microsoft Skype, Cisco Jabber, and others. Bot masters often use P2P to send commands, tools, and additional resources to a compromised host. Disabling P2P where applicable will disrupt an attacker if their plan was to use a P2P-based C2 infrastructure.

- **Set thresholds for DNS queries by a single machine** – Bots will often use a domain-generation algorithm (DGA) to obfuscate the identity of their command and control server, making it difficult to block the server.

On average, over 14% of hostile traffic observed by clients was related to command and control. In clients for whom PCI is important, command and control accounted for less than 8% of their hostile traffic.

However, limiting the number of DNS queries coming from a single machine may disrupt these connection attempts.

- **Block communication to the external C2 server** – Responders often try to eradicate the infection first; however, any known or potential C2 traffic should receive attention first. This method of "cutting the head off the snake" will interfere with further communication. Identify the affected hosts and block all methods of C2. Remediation of the host can then occur once communication has been blocked and analysis has been completed.

- **Use DNS sinkholes** – Configure DNS sinkholes to disrupt communication with malicious domains. This is done by "spoofing" the authoritative DNS servers for those domains. When the attacker attempts to query these domains, DNS sinkholes return non-routable IP addresses, disrupting any further activity.

- **Implement aggressive domain categorization blocking** – Most organizations use proxy categorization to block known-bad domains. Attackers are aware of this and often create domains just-in-time to prevent categorization blocking. Attackers may also use other services like dynamic DNS, online storage or messaging domains. By taking an aggressive stance and blocking these categories (and anything uncategorized), access to many potential C2 resources can be denied.

Cyber Kill Chain Phase 7
Actions on Objectives

Definition: As defined by Lockheed Martin, "only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically, this objective is data exfiltration which involves collecting, encrypting and extracting information from the victim environment; violations of data integrity or availability are potential objectives as well. Alternatively, the intruders may only desire access to the initial victim box for use as a hop point to compromise additional systems and move laterally inside the network.[14]"

Defender Objective: Disrupt the attacker's ability to locate, access and extract sensitive information.

1 Reconnaissance · 2 Weaponization · 3 Delivery · 4 Exploitation · 5 Installation · 6 Command & Control · 7 Actions on Objective · E

Targeted and Disruptive Countermeasures:

- Restrict access to shared folders containing sensitive information
- Enforce Identity Management
- Implement Data Access Controls
- Implement controls to detect and mitigate unauthorized lateral movement

Standard Recommendations:

- Update the organization's risk profile
- Ensure proper network segmentation
- Perform regular data and system backups
- Maintain layers of security for all databases
- If a DDoS occurs be aware of other malicious activity
- Password protect Web application directories
- Implement diverse log monitoring

Critical Security Controls:

- CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- CSC 13: Data Protection
- CSC 14: Controlled Access Based on the Need to Know
- CSC 19: Incident Response and Management

[14] Lockheed Martin Resource: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Cyber Kill Chain Phase 7: Actions on Objectives

Case Study Timeline, Observations and Impact

The chronology of events related to the Actions on Objectives phase is provided in the following timeline.

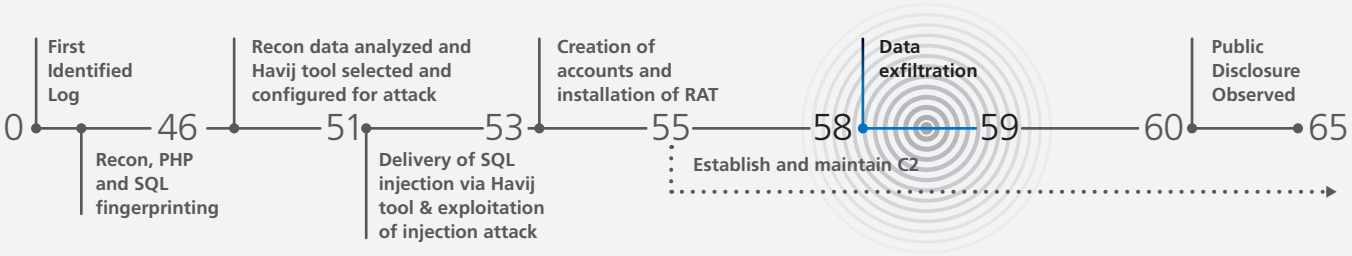


Figure 25: Timeline of events – Actions on Objectives

A third party contacted PPFC and informed them private PPFC information had been posted to a paste site. Before this contact, PPFC had not realized they had been compromised and attackers had extracted some of PPFC's most valuable information. Attackers had progressed through the entire CKC without being detected, found information of value, and dumped the contents of selected database tables.

After PPFC learned of the breach, they engaged incident response assistance. Analysts found evidence of most of the attack process in Web, system and security logs.

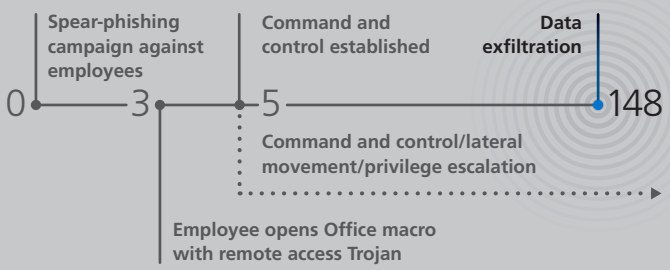
Some of the key challenges in preventing successful actions on objectives include:

- **Identification of the most valuable data** – To protect its most valuable data, an organization needs to identify that data and the critical systems, processes and staff that manage it. If an organization has not accurately identified its key data and systems, it will be difficult to adequately protect them.

- **Active management of key data** – Once identified, management of key data can still be difficult. Organizations typically define security around the systems and environment to be protected, and focus less on security controls designed to protect the actual data.

Advanced Threat – Phase 7 Action on Objectives

In the alternate example, the attacker spent nearly five months performing internal reconnaissance and moving laterally throughout the environment to meet their objective, which was to locate and access highly sensitive data. In the case of this attack, which started as a single hostile attachment, data exfiltration did not occur until day 148 of the attack.



Cyber Kill Chain Considerations

The Actions on Objectives phase of the kill chain is the goal of the attack (but not always the end of attacker activity). Every other phase is directed toward getting to this point: find a target, research it, uncover and exploit vulnerabilities, gain access, then accomplish the objective, such as extracting data to use or sell.

Once an attacker has access, the defender's goals are to limit lateral movement and detect data exfiltration. Organizations should be implementing controls to detected lateral movement and privilege escalation, especially on systems that house critical data.

Organizations can minimize the amount of time the attacker can stay in the target environment – keep the "time on target" low by logging and monitoring actions within their environment. Organizations can ensure that the attacker's "time on target" is noisy, giving the organization time to react to the attacker before they can take Actions on Objectives by including controls to limit access and protect data.

Targeted and Disruptive Countermeasures

These targeted and disruptive countermeasures have the potential to disrupt the attacker's activities within the current kill chain phase.

- **Restrict access to shared folders containing sensitive information** – Attackers often find shared folders with no measures taken to secure the sensitive information within them. These resources may allow attackers to identify usernames and passwords of higher privileged accounts. Access to this shared information should be restricted and require higher privileges than a standard user.

- **Enforce Identity Management** – Strong authentication, tied to a user population that is managed with effective group rights, can help control who has access to what assets. To improve organizational security, this can be combined with a well-defined need-to-know system and aggressive access monitoring. If data access is reviewed and approved through a rigorous process, it can reduce the chances of unauthorized access to key data. A strong identity management solution is also critical for additional controls such as an effective DLP solution and effective logging.

Actions on Objectives included the lowest volume of logs at 0.0003% of all logs, but included the highest confidence of all alert types.

- **Implement Data Access Controls** – Organizations should configure and test proper DLP solutions with information tagging, packet inspection, network monitoring and more to detect unauthorized use or movement of sensitive data. Improve the refinement of data access with database activity monitoring. Monitoring of data being accessed may allow an organization to take mitigation action while an attack is still in process.

- **Implement controls to detect and mitigate unauthorized lateral movement** – During the Actions on Objectives phase, attackers will often move slowly and cautiously as they attempt to extend their reach in the network. Implementing internal IDS, IPS and other controls within the network, not just at the border, can help identify unauthorized access attempts and prove to be valuable when performing incident response.

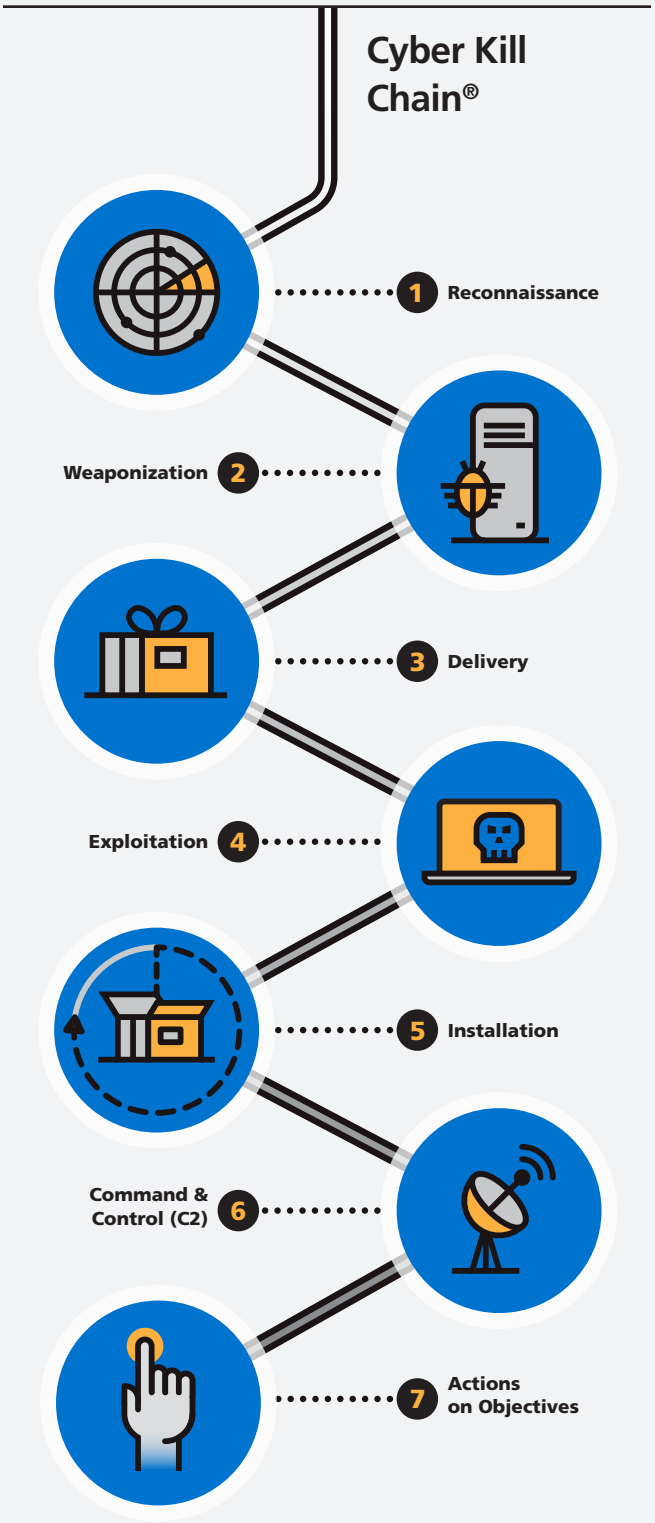
PPFC Case Study: Conclusion

Our case study has presented the events of an actual NTT Group security incident response. In this study, we described how an attacker invaded the PPFC environment without being detected.

The attacker moved through all seven phases of the Cyber Kill Chain. He performed:

- **Reconnaissance** to locate vulnerable targets
- **Weaponization** to select and configure software capable of exploiting the vulnerabilities
- **Delivery** to transmit his SQL injection attack
- **Exploitation** to obtain detailed information about the target database and underlying system
- **Installation** of a remote-access Trojan and attacker-controlled accounts, allowing persistent access
- **Command and Control** to continue the attack, still without being detected
- **Actions on Objectives** to export large amounts of PPFC data

With proper controls in place, PPFC might have interrupted the attack at any one of these phases. Instead, as NTT Group has seen in so many cases, PPFC implemented inconsistent controls that were inadequate to detect or prevent the attack. This led to valuable PPFC data being uploaded to a public website.



Incident Response: Trend Shows Organizations Are Not Prepared

As illustrated in the case study and the exploration of the Cyber Kill Chain, incidents do happen. And when they do, organizations must be prepared to respond. During 2015, NTT Group continued to participate in responses to cyber incidents affecting its clients. Throughout the year there were many media headlines due to confidential information being stolen, denial of service attacks and insider threats, yet the data collected by NTT Group in 2015 indicates organizations are not making focused efforts to prepare for such attacks.

A key requirement for being able to leverage concepts such as the CKC is to invest not only in detective and defensive controls, but also in the ability to take action when an attack is occurring.

This section of the 2015 GTIR report illustrates how prepared organizations are, the types of incidents observed by NTT Group, and basic steps that should be considered for an effective incident response.

Lack of Investment and Preparedness Continues to Prevail

During incident response engagements, NTT Group tracks metrics related not only to the impact of the incident, but also to how well organizations are prepared to respond. Unfortunately, many who engage NTT Group incident support do so because they have little investment in their own incident response capabilities, and thus do not have the technical knowledge to respond or the ability to attribute the attack back to its source.

Observing the trend of incidents supported since 2013, there has been little improvement in preparedness. In 2015 there was a slight increase in organizations that were unprepared and had no formal plan to respond to incidents. Over the last three years, an average of 77 percent of organizations fall into this category, leaving only 23 percent having some capability to effectively respond.

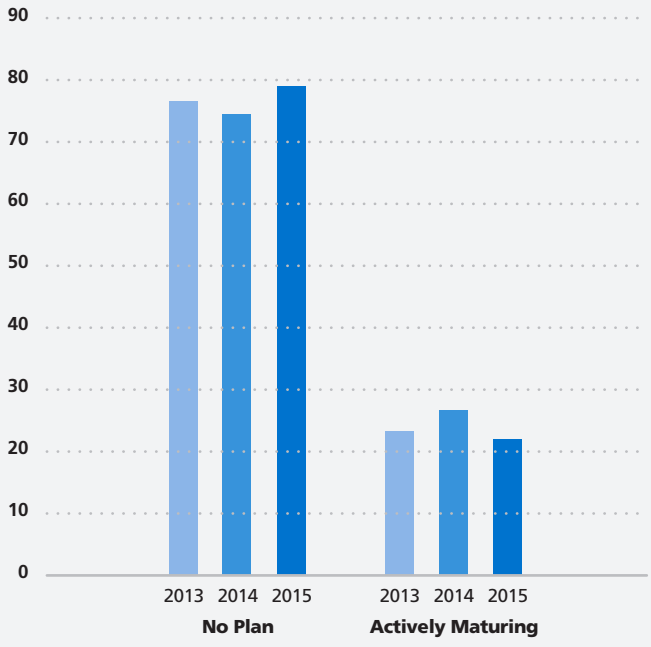


Figure 27: Percentage of organzations who are preparing response capabilities

Types of Incident Response

In 2015 NTT Group continued to provide client support focused on several core incident categories, including malware, DDoS and breach investigations, spear phishing and internal threats. Within these areas there were some notable changes from previous years, including a rise of breach investigations, internal threats and spear phishing, and a drop in malware and DDoS mitigation support. In cases where incidents spanned types, they were categorized according to their most significant threat vector.

NTT Group measured an increase in breach investigations, with 28 percent this year compared to 16 percent last year, and many of the activities focused on theft of data and intellectual property. Analysis indicated these were targeted and not opportunistic attacks.

Due to an increase in attacks related to internal threats, often involving employees and contractors, NTT Group created a new category for these types of attacks. In 2015, internal threats jumped to 19 percent of overall investigations compared to the previous year's two percent. Many of these investigations were the result of internal employees and contractors abusing information and computing assets, and were initiated by Human Resource departments.

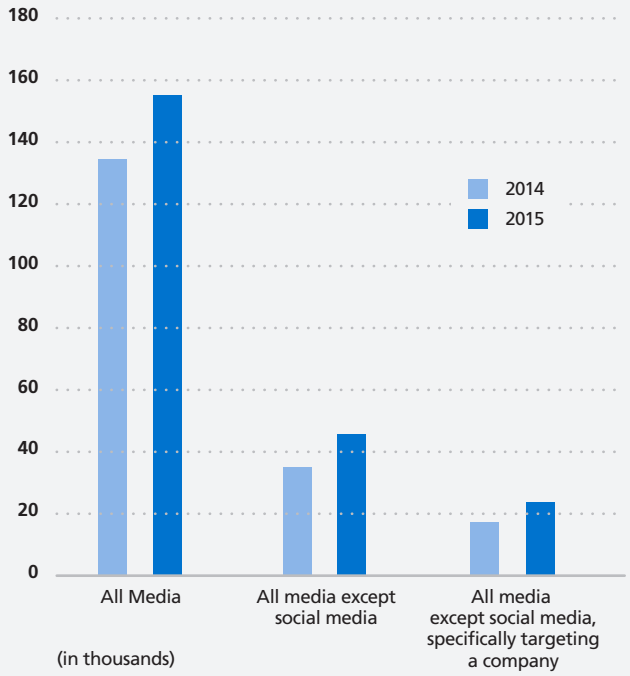


Figure 28: Recorded Future references for DDoS increases

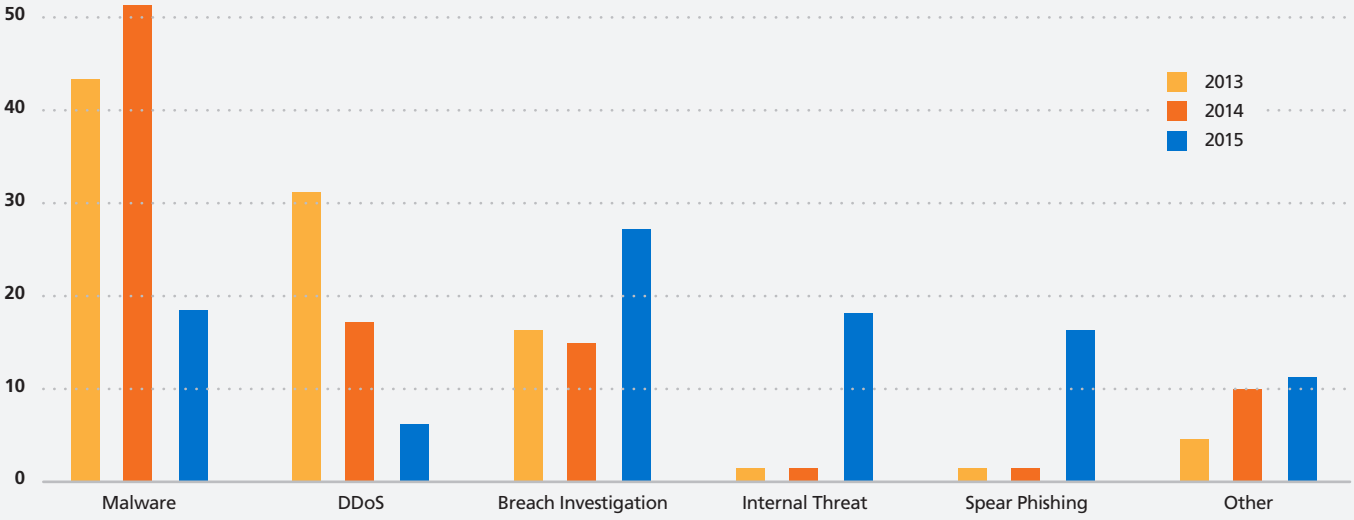


Figure 29: Percent of incidents across three years of data

Similar circumstances resulted in creation of a separate category for spear phishing attacks. Spear phishing attacks accounted for approximately 17 percent of incident response engagements, up from two percent the previous year. Many of the attacks were related to financial fraud targeting executives and finance department personnel in retail clients. Attackers often gained detailed knowledge of the organizational structure and performed well-crafted social engineering and spear phishing attacks. Several of these attacks were focused on duping organizations into paying phony invoices.

Although 2015 saw the rise of DDoS hacking groups like DD4BC and the Armada Collective, NTT Group again noticed a drop in DDoS related support compared to the previous two years. This drop is likely related to a continuing investment in defense against these types of threats. Adoption of the proper tools and services for DDoS mitigation is vital to surviving a well-coordinated attack. There has also been a decline in successful DDoS attacks observed by NTT Group, resulting in less support required during 2015.

Analysis of Recorded Future's data illustrates that while NTT Group incident data shows a decrease in DDoS attacks among its clients from 2014 to 2015, a review of DDoS references on the Web shows an increase in discussions about DoS/DDoS by 25%-35%.

Incidents by Vertical Market

Although finance was the leading sector for incident response in our previous annual reports, the retail sector took the lead in 2015 with 22 percent of all response engagements, up from 12 percent last year. This matches data that shows retail clients experienced the highest number of attacks per client, as shown in the Attacks by Sector section. The financial sector declined approximately 10 percent from last year's observations. Most of the spear phishing attacks previously discussed focused on the retail sector and help account for the increase in incident response in this area.

One independent cyber intelligence partner of NTT Group, Wapack Labs , reported the largest jump in 2015 activity was the global deployment of keyloggers. Wapack Labs reported over 12,000 unique infrastructures in over 85 countries were infiltrated by Nigerian actors selling compromised account details in Tor based forums. The activity, referred to as "Daily Show," seemed to be focused on a few geographical locations, primarily targeting the maritime community and those supporting it in the South China Sea, and maritime routes between Nigeria and the Black Sea, the Nordics and the Suez Canal.

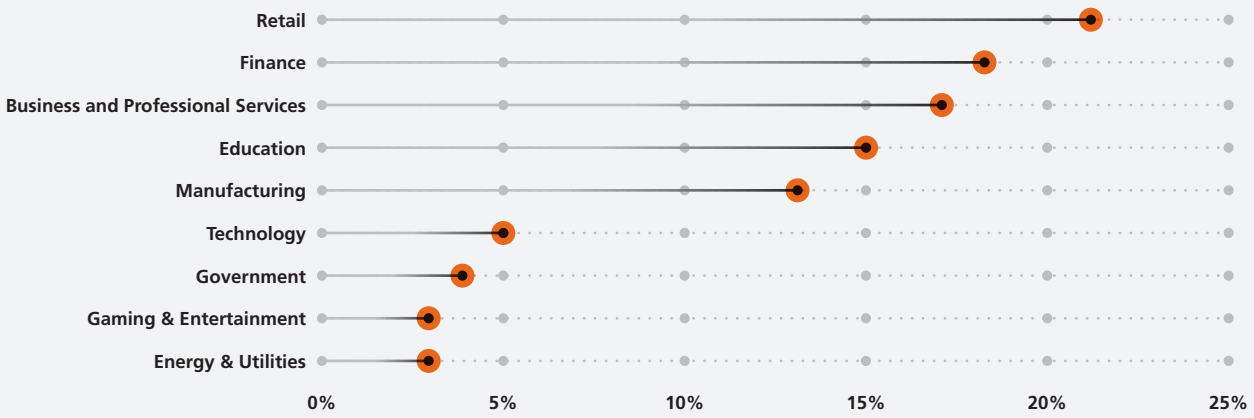


Figure 30: Percent of incident engagements by sector

Angler Exploit Kit was easily number two in the rise of threat activity observed. Wapack Labs published several technical reports related to this threat. Based on analysis, targeted organizations estimate Angler delivers roughly 90% of all malicious activity observed.

Wapack Labs detailed accounts of Russia's cyber actions in the conflict with Ukraine. The cyber underpinnings of the activity, in Wapack Labs' opinion, track closely with the Ivanov Doctrine – a plan for using cyber and other information warfare tools in conjunction with physical activities.

Iran moved into the top of the threat landscape starting with the stockpiling of tools and continuing with the building of associations with other cyber warfare related actors. Iran appears to have become the new China with one major difference: Iran isn't interested in espionage but is more focused on cyber warfare capabilities.

Wapack Labs reported 2015 attacks shifted from espionage and theft to focus more on integrity attacks, with documents manipulated to allow the movement of goods, services and money. Cyber security is moving quickly into the fraud and physical security spaces.

Why should you care? The majority of organizations discussed in this report lack security controls sufficient to stop these types of attacks. This report includes guidance designed to assist organizations in the identification of incremental controls that can make security programs more effective.

Incident Response Example: Emdivi

Among the many malware variants NTT Group observed during 2015 were several incidents related to the Emdivi malware. Emdivi was a key element in the APT attacks targeting a Japanese government agency, which contributed to a breach of the personal data of more than a million people.

Attackers targeted the agency and infected workstations with the Emdivi malware through an email attachment. As a result, attackers exposed approximately 1.25 million records of personal data. The agency is only one example, since they were not the only Emdivi attack. Analysis of Emdivi revealed the following consistent characteristics:

- Involved RAT (remote access Trojan)
- Focused on Japanese organizations
- Gathered information through workstation systems
- Used in targeted attacks and watering hole attacks, among others

Ultimately, the attack against the agency was successful. NTT Group observed several factors that contributed to the success of these attacks.

Factor	Details
Lack of information sharing	• Similar incidents using the same domain as the C2 server had happened before the incident, but the Japanese government had not shared information. These incidents occurred at the multiple other agencies within the Japanese government through April and May of 2015. • A May attack was prevented, but not enough details were shared so other offices could make significant, targeted improvements.
Lost focus on regulations	• Regulations had lost emphasis and enforcement. • Regulatory compliance was not prioritized. • The agency forced inoperable regulations on itself.
Improper monitoring	• The agency collected logs but did not audit them.
Inadequate initial response	• The delay in checking attached files allowed additional infection. • The agency detected and banned a single infected computer from the network. However, other infected but undetected computers were still connected.

Figure 31: Factors in breach

Malware infections such as Emdivi can have a significant impact, even when detected. In the case of this agency, a lack of formal response and communication allowed the infection to lead directly to a widespread breach of personal information.

Incident Response Recommendations

During 2015 NTT Group supported many different types of incident response activities affecting clients in diverse vertical markets. There are several places where organizations consistently fell short in their capabilities to respond effectively. The following recommendations represent only a fraction of what needs to go into a comprehensive program and is intended to highlight some of the common issues NTT Group observed.

- **Prepare incident management processes and "run books"** – Many organizations have limited guidelines describing how to declare and classify incidents even though these are critical to ensure a response can be initiated. Depending on the type of attack, potential impact and other factors, response activities will be very different for each. Common practices for incident response also suggest organizations should develop "run books" to address how common incidents should be handled in their environment. For instance, if DDoS activities are often used against your organization, it is a good investment to create a run book describing the procedures your response team can follow based on the tools and capabilities available.

- **Evaluate your response effectiveness** – We do not see a significant number of organizations testing the effectiveness of their plans. When incidents occur, the last thing you want is to lack an understanding of standard incident response operating procedures. Evaluation of preparedness should include regular test scenarios. Consider post-mortem reviews to document and build upon response activities that worked well, as well as areas needing improvement.

Threat Intelligence increases the ability to be proactive.

- **Update your escalation rosters** – As organizations grow and roles change, it is important to update documentation related to who is involved in incident response activities. Time is critical to incident response, and not being able to quickly involve the correct people can hamper your effectiveness. Updating contact information for vendors such as your ISP, external incident response support, and other providers is just as important.

- **Prepare technical documentation** – To make accurate decisions and identify impacted systems you must have comprehensive and accurate details about your network. This should include:
  - IP ranges and hostnames
  - DNS information
  - Software and operating system names, versions and patch levels
  - User and computer roles
  - Ingress and egress points between networks

Only when an organization is prepared to respond to incidents can they hope to effectively mitigate impact. These recommendations and others identified in the Cyber Kill Chain case study can help achieve a high level of threat preparedness.

The Role of the Cyber Kill Chain in Threat Intelligence

NTT Group recently joined the Lockheed Martin Cyber Security Alliance – a community formed to share best practices, gain insights and combine strengths. This edition of the GTIR focuses heavily on the CKC, and how threat intelligence (TI) and the CKC complement and strengthen each other.

In the 2015 edition of the *NTT Group Global Threat Intelligence Report*, we defined TI at its core as giving context to content.

This section describes how combining an effective TI program with the proven foundation of intelligence-driven defense, on which Lockheed Martin bases the CKC, is applicable to your organization. NTT Group security analysts discuss some of the benefits this combination provides, present the importance of attribution as a specific component of TI and share insights into validating the relevance and confidence of your intelligence sources.

The Threat Intelligence Debate

Throughout 2015, discussions concerning the usefulness of TI have been unrelenting, and the debate continues.

Is a TI program truly valuable? Challengers believe "threat intelligence" is an overused industry buzzword and is ambiguous at best. In the same vein, opponents believe vendors are selling "information" as opposed to "intelligence."

Properly defined and implemented, however, TI becomes an absolute necessity. With data and indicators of compromise (IOCs) changing in the blink of an eye, network defenders are simply unable to keep up with identification, tracking, logging and implementation of changes in their network environment. In fact, some IOCs (e.g., malicious payloads, URLs, IP addresses) are so ephemeral they may only be used once in a targeted attack.

TI increases the ability to be proactive, helping your organization identify the attackers who are focusing on you, as well as analyze their tactics, tools and procedures. TI can also help gain invaluable insight into vulnerabilities in your environment.

TI also adds insight into attackers' motivations and intentions. Consider how any stolen data would be used. Who wants your data and why? Are attackers just scanning the Internet

looking for vulnerable hosts, or are they specifically targeting your organization? Understanding an attacker's history, capabilities, intentions and methods will aid in determining if your organization may become a target, helping to prioritize your cyber defense spending.

The bottom line here is threat intelligence is incredibly valuable, especially when used with other tools in your cyber defense strategy.

As described in the *2015 NTT Group Global Threat Intelligence Report*, relevant and actionable intelligence is not a "one size fits all" solution, and defining those facets relevant to your specific organization is crucial to implementation of a successful TI program.

Threat Intelligence and the CKC Intertwined

Neither the Cyber Kill Chain nor Threat Intelligence are a panacea, but together they can add significant strength to a cyber defense strategy. The CKC is a well-known industry concept and proven model – a blueprint designed to help visualize the progression of a typical cyberattack, exposing points at which disruptive actions can be taken against an attacker. Use of this model in conjunction with a TI program provides an outstanding roadmap for addressing threats, allowing organizations to gain the upper hand and disrupt attackers' plans. In the Cyber Kill Chain Case Study, NTT Group uses the Center for Internet Security's Critical Security Controls to help build a framework to do exactly this.

The goal of the CKC is to interrupt the adversary at the earliest phase. A more ambitious goal is to stay ahead of the cyber kill chain altogether – to disrupt or identify the threat before attackers even begin phase 1 (Reconnaissance) of the CKC.

TI can be used throughout each phase of the CKC not only to identify your security gaps, but also to identify disruptive measures in other phases of the CKC. TI is best implemented, however, before the CKC even comes into play.

Prior to an adversary ever sitting down at the computer, he has motivations and intentions and is defining his target list. Knowledge of an attacker's intent, history, capabilities or supply chain increases the avenues by that an organization can defend itself and its clients. Security analysts can gather some of this information by viewing traffic logs (e.g., observing port scanning and other reconnaissance steps) to help identify tools, techniques and procedures, and potentially isolate specific attackers or attacker groups.

The CKC is also an excellent tool for outlining malware-based attacks. One attack vector that is highly involved in malware delivery is probably the most underestimated move in the attacker's playbook – social engineering, which is best addressed with a robust cyber awareness training program.

Effective threat intelligence can help build a profile of not only how an attacker may approach you directly, but indirectly, through a vendor or a partner.

But, you cannot just develop a training program based on some generic requirements. To create an effective security awareness and training program, you need to plan the content to focus on the threats and controls that are most important to your organization.

Beyond the assets organic to your organization, also consider other associations in your circle, such as third-party vendors or business partners. They may have vulnerabilities in their networks that may give an attacker an avenue into your business via shared infrastructure. You need to protect your data along with your clients' data. Knowing what information you have, who would want it and what an adversary might use it for, are imperative. Effective threat intelligence can help build a profile of how an attacker may approach you both directly and indirectly through a vendor or a partner.

Both the CKC and your TI program should be viewed as integral parts of your security system, as doing so will give your organization a greater capability to be proactive and resilient. Intelligence is an unending process, and the events

taking place in your environment, trends in your industry and geopolitical events are all critical factors impacting your TI program's success.

External Threat Intelligence Sources

By supplementing your internal data with external threat intelligence sources, you stop limiting yourself to internally generated threat intelligence that, by its very nature, is extremely limited. Gathering data from a variety of sources, piecing it all together, adding context and refining it over time are critical aspects to a robust TI solution.

Consider seeking out collaborative partnerships with organizations that have a 24/7 Security Operations Center (SOC), from which you can derive up-to-date IOCs. Your external TI service provider should have a variety of sources and include reports ranging from actionable emerging threat advisories, to reports for trending activity, to monthly or quarterly reports for more strategic considerations.

The Importance of Attribution

Over the last few years, the security industry has observed attribution (determining the actor behind a cyberattack or compromise) as playing a greater role in cyber defense. Standard methodologies such as blacklisting known bad IPs and domains are becoming an increasingly futile effort. Many IOCs are useless after the attack, as an actor may have changed his callback domain.

That being said, definitive attribution is quite difficult to achieve. Although forensic capabilities are essential toward this end, just the pursuit of attribution can bring about an enhanced understanding of the cyber defense challenges facing your organization. Adversaries are still only human, and analysis of adversary activity often reveals tangible artifacts. Adversaries have egos, intentions and motivations. Sometimes these intentions are made public, primarily by hacktivist-type groups such as Anonymous. Other times they are less obvious.

Adversaries have egos, intentions and motivations. Sometimes these intentions are made clear in the public arena, primarily by hacktivist-type groups such as Anonymous. Other times, though, these intentions are less obvious.

Analysis of adversary TTPs can be helpful in numerous ways:

- To identify adversary infrastructure you can proactively block
- To identify your priority infrastructure and assets (based on what attackers are targeting in your environment)
- To support red-teaming and vulnerability assessments against your environment based on adversary TTPs

Additionally, attribution can help your organization determine how to allocate funds based on cyber defense priorities. For example, if you can attribute a cyberattack to a particular advanced persistent threat (APT) your executives have heard about, it could encourage them to better fund cyber defense due to the group's notoriety.

Geopolitics also plays an increasingly important role, as more countries and hacktivists become cyber-savvy. Nation-state actors and hacktivists alike are progressing from infecting the systems that maintain machines, dams and power grids to influencing the mindset of a target (i.e., spreading propaganda). If a target perceives the adversary to have a capability or simply the intent to use it, this alone may affect the target's means of defending itself. For example, consider the intentional power outage for a large segment of the Ukrainian population during the continued strife with Russia. Although attribution is not yet definitive, the malware and TTPs used point to actors associated with Russia. This attribution, accurate or not, could affect the psyche of the populace of

Ukraine if they believe Russia has this capability and willingness to use it. The thought of Russia asserting this power in similar attacks could be a deciding factor in future Ukrainian action.

The essential goal of attribution and analysis of adversary TTPs should be part of a broader program to provide stakeholders with TI, supporting more proactive courses of action to prioritize your security resources.

Threat Intelligence: Summary

Traditional methods such as perimeter defense are becoming less effective in preventing attacks. Attackers are continuously becoming more sophisticated in their attack methods, developers are creating malware with anti-virus evasion capabilities and attackers are staying several steps ahead of defensive measures. All of these require a more proactive, resilient, adaptable approach to cyber defense.

The objective of a TI program should be to identify emerging threats before they can impact the business. Decreasing the number of direct threats can reduce risk, thereby maintaining or increasing profitability. To prioritize the identification and analysis of threat events and sources, TI teams must first gain an understanding of what an organization identifies as vulnerabilities.

Keep in mind that these tools – the CKC, TI, attribution, external sources – are integral pieces of helping your cyber defense program become more capable, agile and adaptable. You must also remain flexible in the development and implementation of your overall defense program, and increase the overall resiliency and survivability of your network.

Global Honeynet Analysis

NTT Group security researchers analyzed honeynet data from the NTT Group global honeynet to better understand the Reconnaissance phase of the CKC.

The data from 2015 consists of nearly 105 million attacks directed against honeynet sensors in over 100 different countries. The data included attacks from 206 countries and over 372,000 unique IP addresses. Researchers categorized the events into service-oriented categories, analyzing the data from a reconnaissance perspective.

Attack Categories

Security researchers observed a number of different attack categories throughout the year. The top five categories were: SMB/NetBios/Samba (Directory Services), SSH, HTTP, SQL and VoIP attacks.

May 1, 2015, was one of the noisiest days of the year, accounting for attacks to and from 101 countries, spanning 21 categories, over 3,100 IP addresses and more than 1,000 service providers, companies and other entities. SSH was the top attack method on that day, primarily originating from China.

Overall Rank	Category	Average Attacks per Day
1	Directory Services	128,000
2	HTTP	80,000
3	SSH	14,300
4	SQL	6,400
5	VoIP (SIP)	3,700

Figure 32: Ranking attack categories

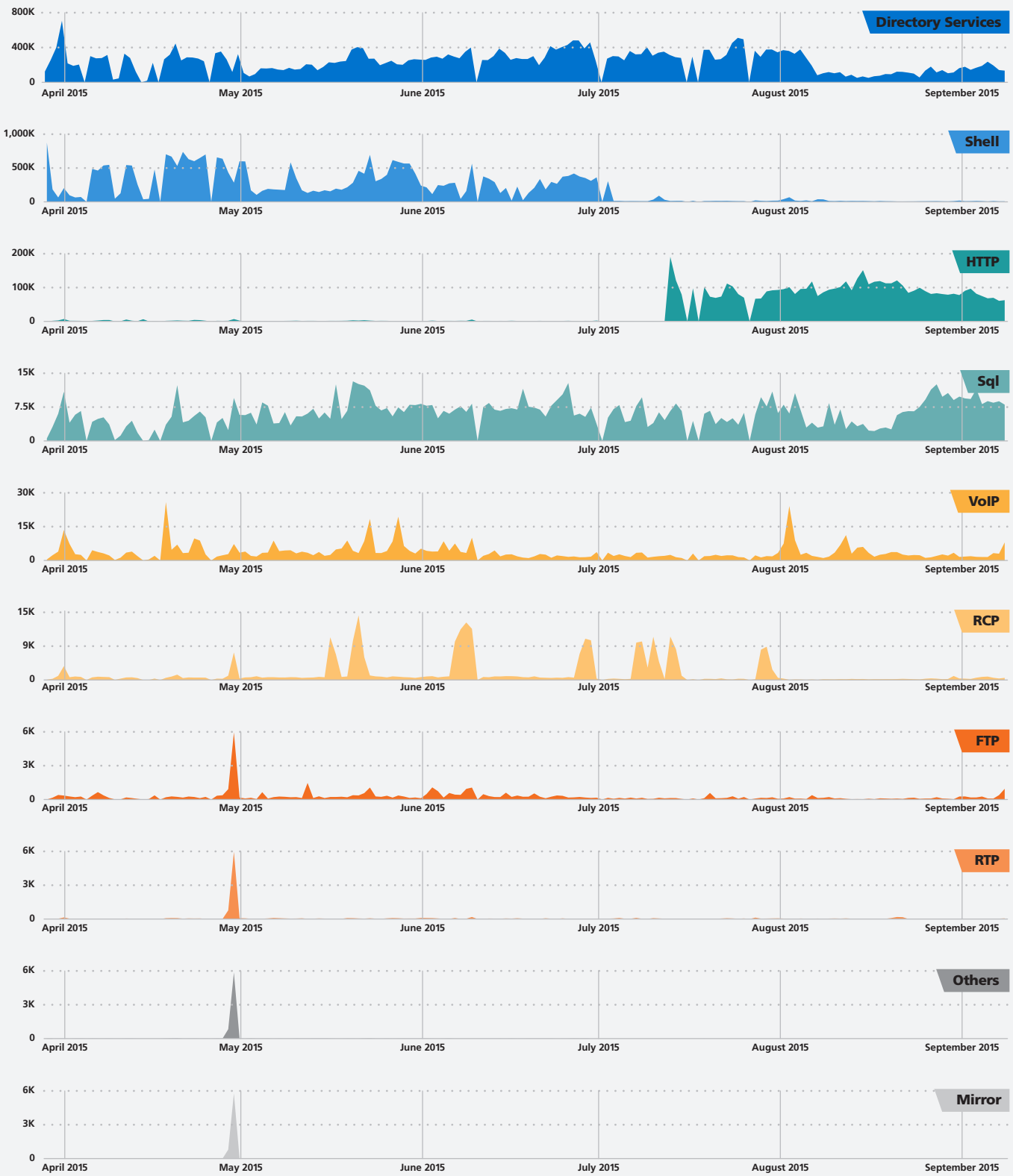


Figure 33: Attack categories from honeynet

Rank	Attack Origin	Total
1	Hong Kong	21,954,881
2	China	11,942,219
3	United States	9,398,814
4	Russia	9,153,213
5	Venezuela	7,286,212
6	Taiwan	5,044,451
7	India	4,004,119
8	Malaysia	3,219,336
9	Bulgaria	2,679,374
10	Romania	2,399,730

Rank	Attack Origin	Total
11	Ukraine	2,279,747
12	France	2,166,165
13	Brazil	1,813,481
14	Korea	1,389,191
15	Germany	1,380,097
16	Indonesia	1,345,938
17	Ireland	1,317,324
18	Japan	1,186,717
19	Hungary	1,017,004
20	Canada	916,258

Figure 34: Ranking honeynet attack source countries

Source Countries

Many of the countries on this list are no surprise. Firewalls, intrusion prevention systems (IPS) and other perimeter devices are accustomed to the constant attacks from both China and the Russian Federation. A majority of the companies whose infrastructure the attackers are using are Internet, telecommunications or hosting providers perpetually running outdated operating systems and services. This indicates that a significant amount of this traffic is likely originating from compromised networks and providers and not through hosting services that have been procured in a legal manner. The large amount of SSH and HTTP attack traffic reflects this, as these attack vectors still provide a reliable means of infiltrating a network.

This information is different from the source information observed during managed and monitored security services. First, the distribution of the honeypot network is different from the NTT Group client base. The honeypot network is a separate environment, segregated from all corporate and institutional networks. Second, honeynet traffic is primarily reconnaissance traffic.

Providers

The top five noisiest Internet providers accounted for nearly 31 percent of all the attack traffic observed throughout the year.

Rank	Provider	Primary Attack Vector
1	ISP Rainbow Network	SSH Brute Force
2	ChinaNet Jiangsu Province Network	SSH Brute Force
3	Cantv Servicios Venezuela	SMB/NetBios/Samba
4	Data Communication Business Group	SMB/NetBios/Samba
5	Shimizu Hang Road Causeway Bay Hong Kong International	SSH Brute Force

Figure 35: Top 5 noisiest ISPs

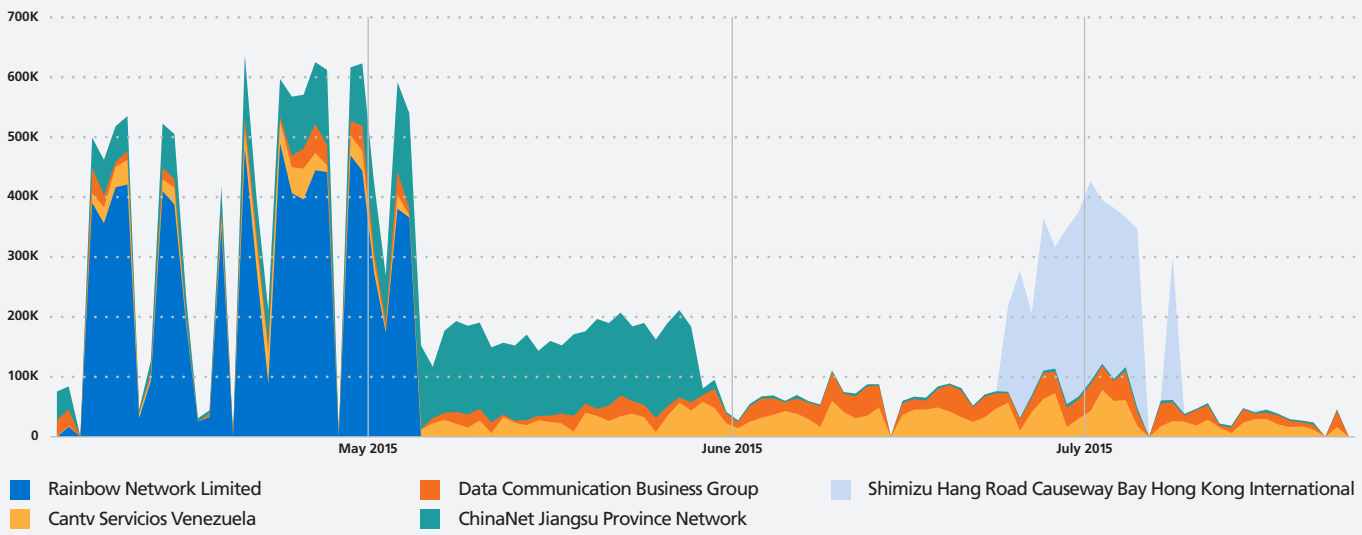


Figure 36: Top five providers from honeypot analysis

ASNs (Autonomous System Numbers)

ASNs are a group of external IP addresses and networks under the administrative control of one or more organizations. These are external IP allocations that communicate using a variety of network routing protocols. In conjunction with origin country examination, ASN analysis can pinpoint multinational operations that may be providing bulletproof hosting services or have a major problem on their network, both of which provide attackers with a distinct advantage in the Reconnaissance phase. NTT Group security researchers identified nearly 11,000 different ASNs across all unique IP addresses hitting the honeypot sensors. This totaled over 66,000 different prefixes and over 370,000 unique IP addresses. Below are the top 10 ASNs that averaged significant amounts of hostile traffic. *(Example: In a /24 prefix with 254 available IP addresses, this equates to 25 IP addresses.)*

Rank	ASN	Percent	ISP	Location
1	41578	60%	Level Next Ltd.	Gibraltar
2	57004	57%	VOLJAGLAS d.o.o.	Croatia
3	62540	44%	Drake Holdings LLC	United States
4	57063	41%	Klass Ltd.	Russian Federation
5	58182	41%	Kadroviy Reserv Ltd.	Russian Federation
6	58244	38%	ProektProfDevelopment Ltd.	Russian Federation
7	58061	35%	Trade House_BelRosResursu_Ltd.	Russian Federation
8	58137	33%	GazInvestProekt Ltd.	Russian Federation
9	3189	32%	Atlant-Stroy Ltd.	Russian Federation
10	58062	27%	Transport Company UGRA Ltd.	Russian Federation

Figure 37: Top 10 ASNs observed

Prefixes

In NTT Group efforts to determine which prefixes were involved in attack activity, researchers identified over 66,000 unique prefixes and their associated providers, ASNs and ASN owners. Following the thought process described above, there were nearly 8,900 prefixes where researchers observed nearly 220 prefixes averaging 10 percent or more of their available IP address space, while the top seven prefixes accounted for two-thirds or more of their available IP address space, as depicted below.

Prefix	Percent	ISP	ASN	Country
1.1.1.0/24	100%	Research Prefix for APNIC Labs	15169	Australia
104.128.66.0/24	84%	Vegasnap LLC	53340	United States
104.128.67.0/24	80%	Vegasnap LLC	53340	United States
192.92.196.0/24	80%	Drake Holdings LLC	62540	United States
104.128.65.0/24	78%	Vegasnap LLC	53340	United States
112.215.123.0/24	74%	PT Excelcomindo Pratama	24203	Indonesia
202.58.99.0/24	66%	Kingcorp KH	131178	Cambodia

Figure 38: Top seven prefixes observed

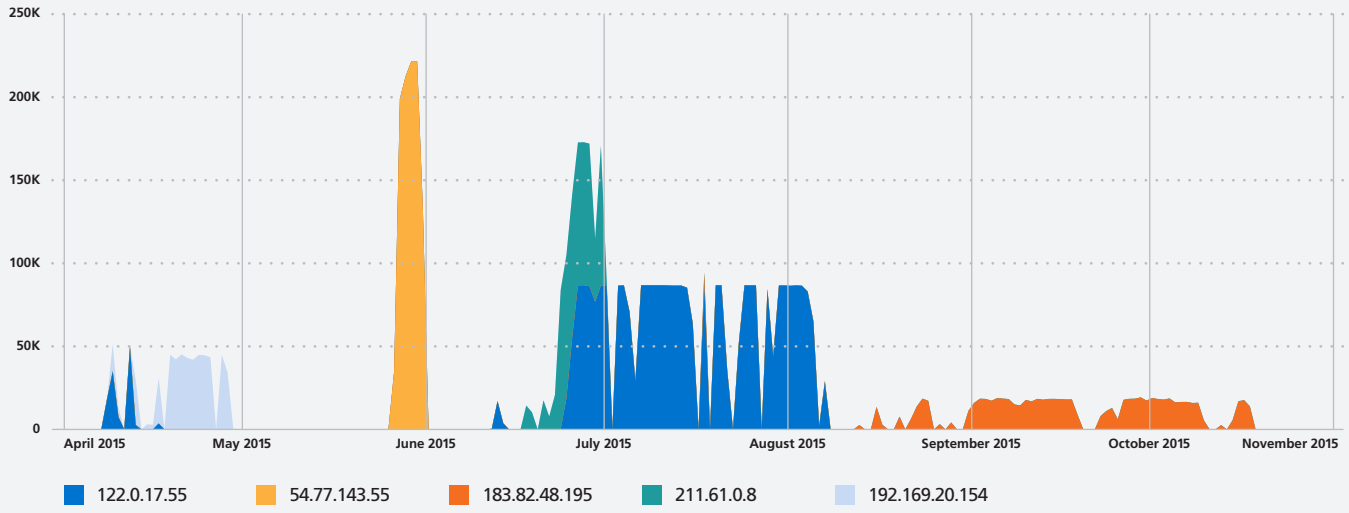


Figure 39: Top five IP address detections from honeynet

IP Addresses

Out of over 372,000 IP addresses, the top five IP addresses (0.00134 percent) generated over six percent of the total events the honeynet observed. Generally, the top actors did not engage in concurrent activity. Instead, researchers observed top actors attacking over specific periods throughout the year.

The table below lists the top five hostile IP addresses, along with the percent of total observed events.

Rank	IP Address	% of Total Events
1	122.0.17.55	3%
2	54.77.143.55	1%
3	183.82.48.195	< 1%
4	211.61.0.8	< 1%
5	192.169.20.154	< 1%

Figure 40: Top five most hostile IP addresses - honeynet

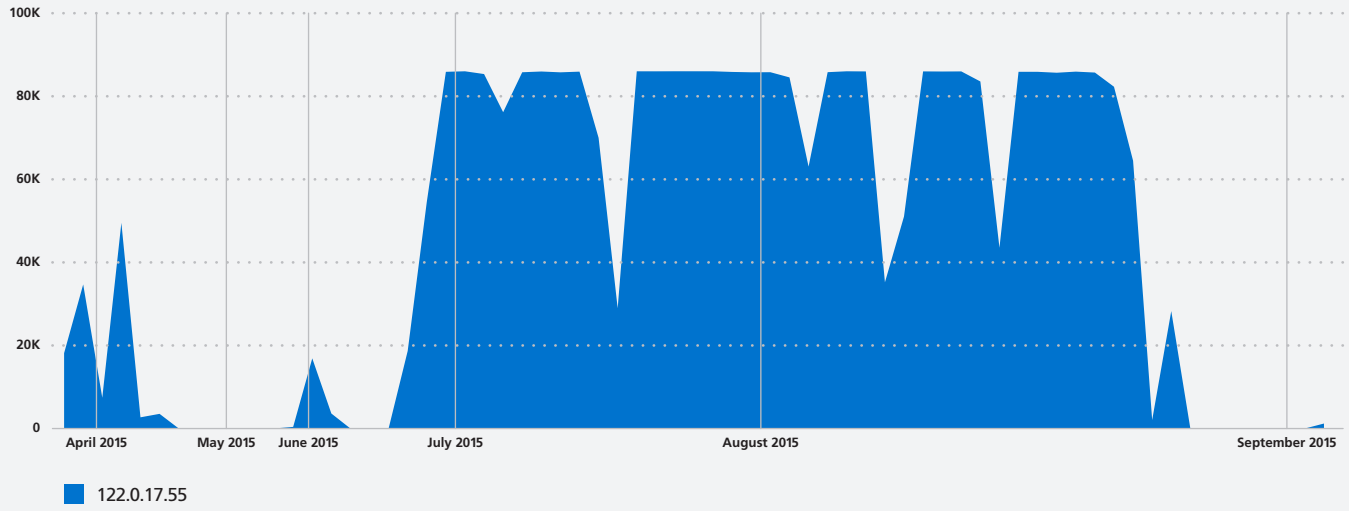


Figure 41: Detail for 122.0.17.55

Geopolitical Considerations

It is impossible to fully understand an attacker's motives behind certain reconnaissance activities without considering the geopolitical climate. NTT Group security researchers analyzed the data through the lens of geopolitical considerations, and in areas of political unrest, scrutinized the data to confirm or deny cyber activity correlation.

Unsurprisingly, attackers targeted Israel more than any other country in the Middle East region. Targeting outside of the region focused primarily on the United States, with Iran as the top attacker from the Middle East region.

Further east in Ukraine, the top four countries conducting attacks were those with the most vested interests in political developments in Ukraine. In order, these countries were:

Rank	Attack Country	Total Attacks
1	United States	320,014
2	China	240,917
3	Ukraine	224,216
4	Russian Federation	109,197

Figure 42: Top country sources of Ukraine attacks

Global Honeynet: Summary

Reconnaissance is the most benign phase of the CKC from an immediate damage perspective; but, for the attacker, it is arguably the most crucial. The longer an attacker is able to move about undetected in an organization's network, the more accurate his network mapping will be – and the greater the probability of success for subsequent phases of the campaign.

While new attacks are emerging daily, exploitation of old vulnerabilities affords attackers the most success. This is directly attributable to the reality that attackers exploiting out-of-date software continue to outpace organizations' abilities to repair or replace the same. The bottom line is that it is up to each organization to take the steps necessary to thwart attempts at network infiltration and subsequent attack.

Anti-sandbox Techniques – Why is your sandbox silent?

Sandboxes have become essential analysis systems for detecting malware and acquiring deep visibility into its behavior. Sandboxes execute suspicious code in a controlled environment, where they observe malware behaviors such as network related activities, file changes and registry operations. Although malware developers can easily evade signature-based and static analysis-based detection methods by using encryption or polymorphism, sandboxes are able to detect malware by observing known malicious activities. These evasion techniques are common to other attack capabilities as discussed in the Cyber Kill Chain case study.

Knowing that sandboxes are widely used for analysis, attackers have developed anti-sandbox techniques to evade detection. Some of these techniques detect the presence of a sandbox by inspecting specific artifacts related to the sandbox. These techniques then thwart malware analysis by terminating malware processes or showing fake behavior. Another common anti-sandbox technique uses the act of stalling execution or waiting for an event such as a reboot.

While security practitioners attempt to create sandboxes resistant to known anti-sandbox techniques, attackers create more sophisticated techniques to circumvent a sandbox's resistance. To ensure researchers can continue effectively using sandboxes for analysis, it is imperative to gain an understanding of anti-sandbox techniques attackers are currently using.

In 2015, NTT Group conducted extensive malware analysis while developing a sandbox intended to resist anti-sandbox techniques. NTT Group automatically analyzed thousands of malware samples daily, and manually analyzed the samples that did not show malicious activity in the sandbox. In the following sections, researchers explain sandbox characteristics, anti-sandbox technique taxonomy and details about the observed anti-sandbox techniques in the analyzed malware binaries.

Characteristics of sandboxes

Malware generally abuses several common sandbox characteristics to evade detection.

- **Limited analysis time** – Since sandboxes typically need to analyze many pieces of malware, they often end each discrete analysis within a predefined time (e.g., sandbox ceases analysis after one minute). If the malware has not exhibited any detectable behavior within that time window, sandboxes will frequently halt analysis even if the malware is still executing.

- **Automated and highly parallel processing** – For effective malware analysis, sandboxes need to achieve automated and highly parallel processing. To accomplish this, sandboxes commonly use virtual-machine technologies. These enable sandboxes to easily replicate and parallelize analysis environments, as well as to restore the environment after analysis and preventing interference with subsequent analysis.

- **Monitoring facilities** – Sandboxes have two analysis functions:
  - Monitoring malware's behavior
  - Defeating anti-sandbox techniques

Anti-sandbox Techniques – Why is your sandbox silent?

Malware uses the Windows API and Windows native system calls to perform malicious activities and inspect specific artifacts related to the sandbox. In order to monitor malware's behavior, sandboxes capture these calls to record the malware's arguments and return values. In addition, some sandboxes modify return values to bypass anti-sandbox techniques.

Anti-sandbox technique taxonomy

Malware developers routinely use a variety of anti-sandbox techniques. Figure 43 includes examples of the techniques taking advantage of the aforementioned sandbox characteristics.

Characteristics of sandbox	Anti-sandbox techniques
(A) Limited analysis time	**Time bomb:** Triggering malicious activity at designated time or date (Example 1) **Stalling execution:** Delaying execution of malicious activities until analysis times out
(B) Automated and highly parallel processing	**User interaction checking:** Detecting absence of user interaction such as mouse operations **Emulator detection:** Detecting virtual machine by examining differences between emulated hardware and real hardware **Service name/registry/file checking:** Detecting virtual machine on the basis of specific strings (e. g., VMware, vBox) **Hardware specification checking:** Detecting differences between common hardware specifications (e.g., CPU only has single core) **Environment fingerprint checking:** Distinguishing sandboxes from infected hosts on basis of fingerprints such as volume globally unique identifier (GUID) (Example 2)
(C) Monitoring facilities	**Hooking detection:** Detecting injected code for monitoring malware (e.g., code for API hooks) **Runtime overhead detection:** Detecting overhead caused by hooking and recording logs **Anti-anti-sandbox detection:** Detecting modification for bypassing anti-sandbox techniques (Case Study 3)

Figure 43: Anti-sandbox techniques

Anti-Sandbox Examples

Researchers and analysts have encountered several anti-sandbox techniques, including time bombs, volume GUID checking and sleep duration shortening detection.

Example 1: Time Bomb

A time bomb, which is a type of logic bomb, is an anti-sandbox technique that triggers malicious activities only on designated dates or hours. Because satisfying the condition is difficult, sandboxes will often fail to observe malicious activities. NTT Group confirmed the Emdivi malware used in attack campaigns targeting the Japanese public and private sectors uses this technique to make malware function only during business hours.

Figure 44 includes time bomb code as implemented in Emdivi. This program checks the current date and time, stalling execution unless the current time is a weekday between 9 a.m. and 6 p.m. This means sandboxes would never observe malicious activities during any analysis that starts outside of normal business hours.

Emdivi has multiple versions, most notably t17 and t20. For both of these versions, researchers confirmed multiple samples showed this functionality.

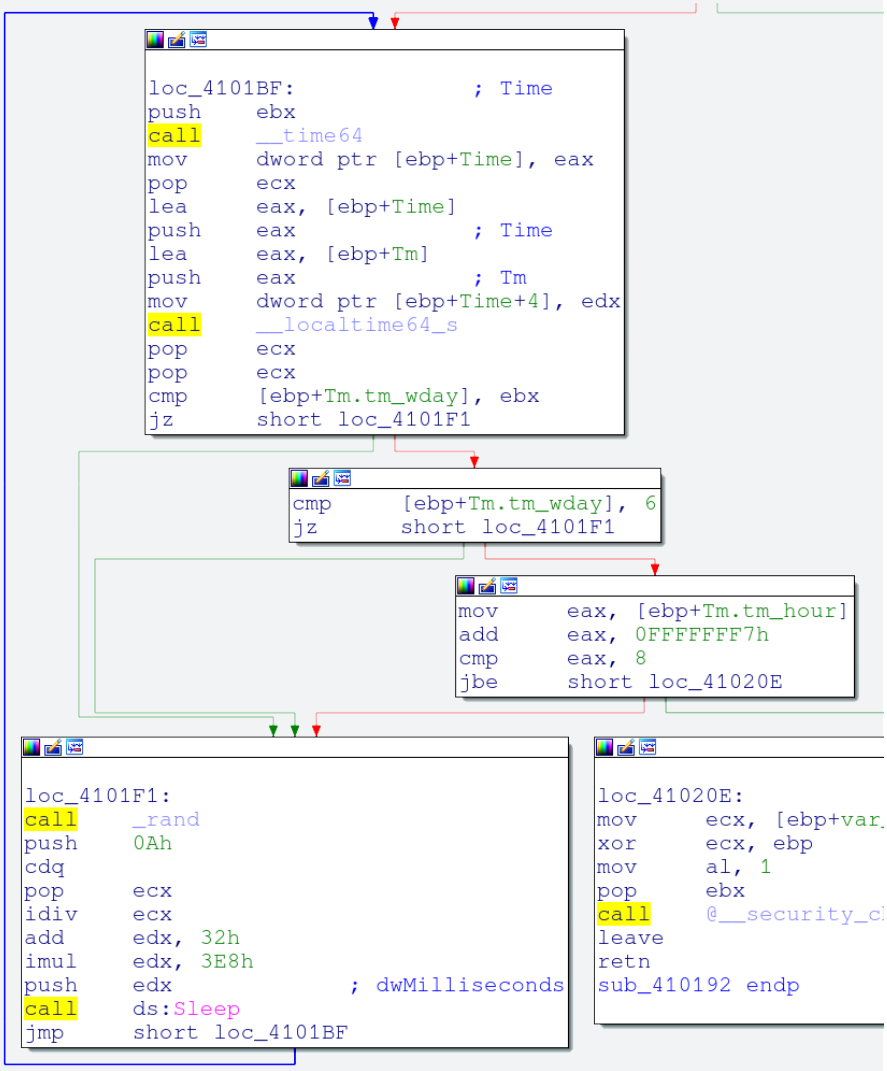


Figure 44: Time bomb implemented in Emdivi

Example 2: Volume GUID Checking

Researchers can also use a sandbox to analyze malware on an infected host. In which case, the malware in the sandbox may execute in an environment that differs from the infected host. Some malware takes fingerprints of an infected host during the infection phase so it can distinguish the analysis environment from that of the host.

One of the techniques for fingerprinting a host is volume GUID checking. Malware reads the volume GUID as a unique fingerprint of a host when it infects the host and embeds the GUID into itself as a part of its binary image. Subsequently, when the malware executes, it compares the volume GUID of the current environment with the embedded one. If the GUIDs differ, the malware stops execution. Zeus malware has used this technique and variants of it in the past.

NTT Group researched more than 5,000 malware samples, collected by employing NTT Group Web client honeypots from 2012 to 2015, and confirmed this is a common technique. During 2015, researchers identified 11 unique malware samples that used this technique.

Example 2: Volume GUID Checking

Researchers can also use a sandbox to analyze malware on an infected host. In which case, the malware in the sandbox may execute in an environment which differs from the infected host. Some malware takes fingerprints of an infected host during the infection phase so it can distinguish the analysis environment from that of the host.

One of the techniques for fingerprinting a host is volume GUID checking. Malware reads the volume GUID as a unique fingerprint of a host when it infects the host and embeds the GUID into itself as a part of its binary image. Subsequently, when the malware executes, it compares the volume GUID of the current environment with the embedded one. If the GUIDs differ, the malware stops execution. Zeus malware has used this technique and variants of it in the past.

NTT Group researched more than 5,000 malware samples, collected by employing NTT Group Web client honeypots from 2012 to 2015, and confirmed this is a common technique. During 2015, researchers identified 11 unique malware samples which used this technique.

Example 3: Sleep Duration Shortening Detection

Some sandboxes attempt to skip Sleep API calls by modifying the sleep duration. This countermeasure has proven to be less than effective because malware often uses anti-sandbox techniques to detect it.

Malware can detect the use of this countermeasure by checking the suspended time. To perform this check, malware uses the x86 read time stamp counter instruction (RDTSC) or the Windows API (e.g., GetTickCount) before and after calling the Sleep API. If the suspended time is shorter than the requested one, malware detects the presence of a sandbox. Researchers have confirmed the common ransomware, TeslaCrypt, uses this technique.

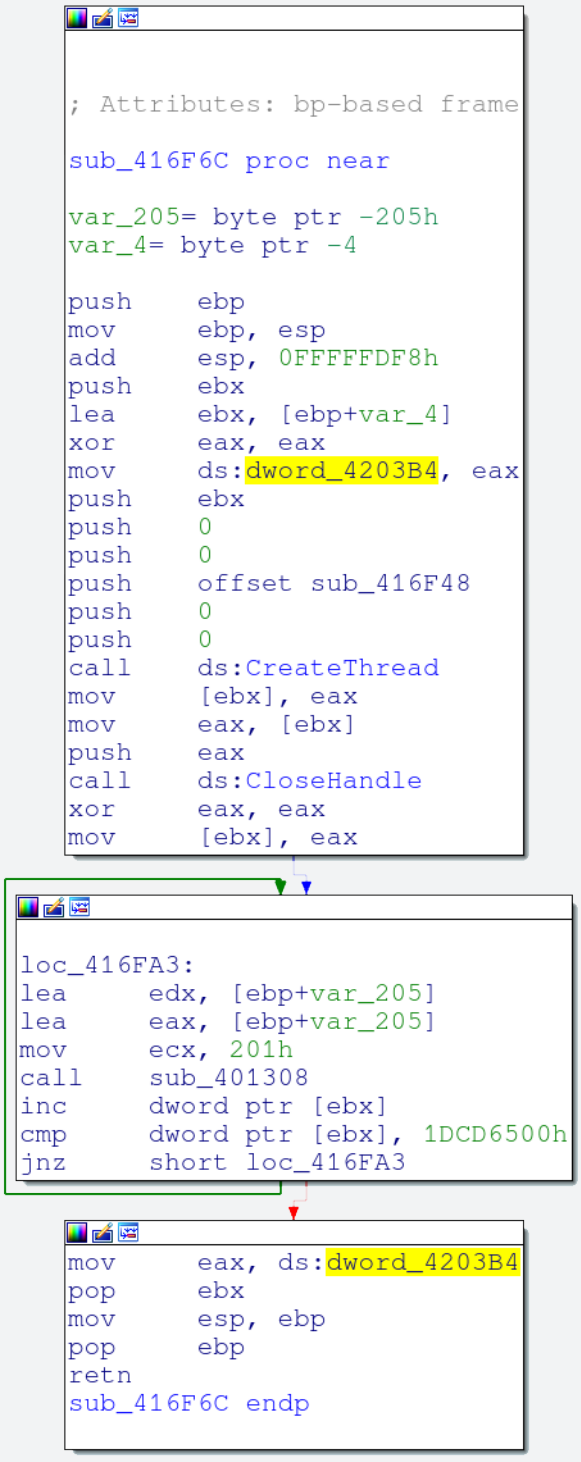


Figure 45: Anti-sandbox technique implemented in Shiotob to detect sleep duration shortening

Sandboxes can, however, easily defeat this technique by incrementing system time. NTT Group researchers confirmed the Shiotob spyware uses a more sophisticated technique that is difficult to bypass. Figure 45 shows the assembly code of Shiotob. Shiotob uses wasted loop execution instead of the Windows API or RDTSC instruction. The main thread creates a new thread and executes a wasted loop. The created thread stalls execution by using the Sleep API and modifies a global variable after calling the Sleep API. The main thread checks the global variable when the loop ends. If this variable has been modified, Shiotob detects the sleep duration shortening.

Recommendations – Sandbox Developers

Sandboxes can be an effective tool to help identify and analyze malware. But malware developers are well aware of sandboxes and have implemented anti-sandbox techniques. As a result, sandbox developers must advance their own techniques to help defeat the attackers and improve detection.

- First, it is important for researchers to understand the anti-sandbox techniques attackers use. It can be dangerous for researchers and analysts to rely on the results of a single sandbox technology and can be very helpful to compare results from different sandboxes. By comparing the results based on known techniques, analysts and researchers can potentially determine the evasion techniques attackers are using. For instance, altering behavior only in a specific sandbox is an evasion tactic that can be detected.

- Sandboxes should also provide options to customize their configurations. These configurations should include user environments as well as the analysis period. NTT Group researchers were able to mitigate the effect of the Emdivi time bomb using multiple sandboxes with different time zones.

  As another example, when researchers knew the volume GUID of an infected host, NTT Group sandboxes successfully bypassed the volume GUID checking by modifying the return value of the APIs to return the volume GUID of the infected host.

- When using sleep duration shortening detection, it is possible to analyze malware behavior in automatic fashion by extending the analysis period longer than the sleep duration. Researchers who have the capability to test with different sleep durations, or who have a customizable sleep duration, can often be successful in capturing malware that uses this evasion technique.

Tips for Sandbox Users

- Since sandbox developers continuously improve their sandboxes in order to bypass anti-sandbox techniques, users should regularly check and apply updates to ensure maximum sandbox effectiveness.

- Organizations should strongly consider sharing analysis results with sandbox developers in order for developers to improve sandboxes on a regular basis.

- Because each sandbox has particular characteristics, using multiple sandboxes (that use different anti-evasion techniques) can help reduce the risk of evasion.

NTT Group Resources Information

About Solutionary

Solutionary is the next generation managed security services provider (MSSP), focused on delivering managed security services, professional security services and global threat intelligence. Comprehensive Solutionary security monitoring and security device management services protect traditional and virtual IT infrastructures, cloud environments and mobile data. Solutionary clients are able to optimize current security programs, make informed security decisions, achieve regulatory compliance and reduce costs. The patented, cloud-based ActiveGuard® service platform uses multiple detection technologies and advanced analytics to protect against advanced threats. The Solutionary Security Engineering Research Team (SERT) researches the global threat landscape, providing actionable threat intelligence, enhanced threat detection and mitigating controls. Experienced, certified Solutionary security experts act as an extension of clients' internal teams, providing industry-leading client service to global enterprise and mid-market clients in a wide range of industries, including financial services, healthcare, retail and government. Services are delivered 24/7 through multiple state-of-the-art Security Operations Centers (SOCs). For more information, visit www.solutionary.com.

About Dimension Data

Dimension Data is a USD 7.5 billion ICT solutions and services provider with over 26,000 employees and with operations in 58 countries. Its security business delivers broad technical and integration expertise across a variety of IT disciplines, including networking, communications, data centers, and end-user computing. We service over 6,000 security clients across all industry sectors, including financial services, telecommunications, health care, manufacturing, government, and education. With our wide range of security capabilities, including consulting, systems integration, and a comprehensive suite of managed security services and threat intelligence capabilities, we assist organizations in planning for a full lifecycle of data security. For more information visit www.dimensiondata.com

About NTT Com Security

NTT Com Security, an NTT Group security company (NYSE: NTT), is in the business of information security and risk management. By choosing our WideAngle consulting, managed security and technology services, our clients are free to focus on business opportunities while we focus on managing risk.

The breadth of our Governance, Risk and Compliance (GRC) engagements, innovative managed security services and pragmatic technology implementations, means we can share a unique perspective with our clients – helping them to prioritize projects and drive standards. We want to give the right objective advice every time.

Our global approach is designed to drive out cost and complexity – recognizing the growing value of information security and risk management as a differentiator in high-performing businesses. Innovative and independent, NTT Com Security has offices spanning the Americas, Europe and APAC (Asia Pacific) and is part of the NTT Group, owned by NTT (Nippon Telegraph and Telephone Corporation), one of the largest telecommunications companies in the world.

To learn more about NTT Com Security and our unique WideAngle services for information security and risk management, visit www.nttcomsecurity.com.

NTT Group Resources Information

About NTT Innovation Institute

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

About NTT Secure Platform Laboratories

Part of the NTT Group, NTT Secure Platform Laboratories are tasked with improving security and intelligence-gathering technologies against ever-evolving security threats. The laboratories conduct research and development on leading-edge technologies such as cryptography, malware analysis, security log analysis, and IoT device/system security. To learn more about our R&D efforts, please visit www.ntt.co.jp/RD/e/.

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 Group. NTT-CERT generates original intelligence regarding cybersecurity threats, helping to enhance NTT Group companies' capabilities in the security services and secure network services fields. To learn more about NTT-CERT, please visit www.ntt-cert.org.

The NTT Global Data Analysis Methodology

The NTT Group 2016 Global Threat Intelligence Report contains global attack data gathered from NTT Group security companies from January 1, 2015, to December 31, 2015. The analysis is based on log, event, attack, incident and vulnerability data from clients. It also includes details from NTT Group research sources, including global honeypots and sandboxes that are located in over 100 different countries in environments independent from institutional infrastructures. The 2016 GTIR summarizes data from over 3.5 trillion logs and 6.2 billion attacks.

NTT Group gathers security log, alert, event and attack information, enriches it to provide context, and analyzes the contextualized data. This process enables real-time global threat intelligence and alerting. The size and diversity of our client base, with nearly 8,000 security customers, provides NTT Group with a set of security information that is representative of the threats encountered by most organizations.

The data is derived from worldwide log events identifying attacks based on types or quantities of events. The use of validated attack events, as opposed to the raw volume of log data or network traffic, more accurately represents actual attack counts. Without proper categorization of attack events, the disproportionately large volume of network reconnaissance traffic, false positives, authorized security scanning and large floods of DDoS monitored by Security Operations Centers (SOCs), would obscure the actual incidence of attacks.

The inclusion of data from the 24 SOCs and seven research and development centers of the NTT Group security companies provides a highly accurate representation of the global threat landscape.

NTT Partner Information

About Wapack Labs

WAPACK LABS
CYBER INTELLIGENCE SERVICE

Wapack Labs identifies cyber threats before they become attacks. Founded in 2013, Wapack Labs is a privately held cyber intelligence and threat analysis firm serving companies and organizations around the globe by providing early warning threat detection through Internet surveillance operations, data gathering, and in-depth analysis of economic, financial, and geopolitical issues. Intelligence information is shared with clients through an array of packages to meet both their cyber security needs and their bottom line. To learn more visit www.wapacklabs.com.

About Recorded Future

Recorded Future

We arm you with real-time threat intelligence so you can proactively defend your organization against cyber attacks. Indexing billions of facts, our patented Web Intelligence Engine continuously analyzes the entire Web, giving you unmatched insight into emerging threats. We help protect four of the top five companies in the world. To learn more visit www.recordedfuture.com.

About Lockheed Martin

LOCKHEED MARTIN

Lockheed Martin (LM) is a global provider of cybersecurity solutions focused on developing, implementing, maintaining, and securing critical infrastructures for Fortune 1000 and Global 1000 companies. LM engineers literally span the globe, overseeing more than 4,000 programs at 600 locations in all 50 states and in 75 countries. We employ over 3,000 cyber-security professionals and have robust IT and OT technology partnerships. Our lifecycle-focused products and programs enable both success and sustainability protecting networks across our commercial clients' infrastructures. Our approach is based on an Intelligence Driven Defense® philosophy that focuses on harnessing information from those who seek to attack and using it against them. To learn more visit www.lockheedmartin.com.

About the Center for Internet Security

Center for Internet Security®

The Center for Internet Security (CIS) is a 501(c)(3) organization dedicated to enhancing the cybersecurity readiness and response among public and private sector entities. Utilizing its strong industry and government partnerships, CIS combats evolving cybersecurity challenges on a global scale and helps organizations adopt key best practices to achieve immediate and effective defenses against cyber attacks. CIS is home to the Multi-State Information Sharing and Analysis Center (MS-ISAC), CIS Security Benchmarks, and CIS Critical Security Controls. To learn more please visit CISecurity.org or follow @CISecurity on Twitter.

Glossary

Glossary

0-day (zero-day) Attack, an attack that exploits a previously unknown vulnerability in software.

API (Application Program Interface), documented methods for software modules to communicate with each other or with the underlying operating system (e.g., the Windows API).

APT (Advanced Persistent Threat), an attacker with long-term goals who is highly skilled and well-funded, generally by a government or by organized crime. An APT is usually a complex attack using multiple techniques for maximum benefit.

ASN (Autonomous System Number), a number identifying a collection of IP routing prefixes under control of a single administrative entity such as a large ISP.

Backdoor, a method of providing unauthorized system access, typically with a password known only to the malicious actors who installed it.

Blacklist, a list of IP addresses or domain names believed to host malware. A security strategy may involve denying access to addresses on a blacklist, or only allowing access to those on a whitelist.

Botnet, multiple attacker-controlled systems capable of receiving instructions or commands at the same time. Botnets are often observed being used in DDoS and other types of cybercriminal activities.

Breach, a cyberattack in which an organization's data has been stolen or made public through compromise of networks or systems.

BYOD (Bring Your Own Device), the practice of enabling employees to use their personally owned mobile devices in the corporate work environment.

C&C (Command and Control or C2), communication infrastructure used by attackers to provide instructions or conduct administrative tasks to bots in a botnet.

CIA (Confidentiality, Integrity and Availability), the three cornerstones of information security. An attacker will attempt to undermine one or more of these.

Critical Security Controls, a set of recommendations for cyber defense activities, published by the Center for Internet Security.

CVE (Common Vulnerabilities and Exposures), a catalog of publicly known vulnerabilities.

CVSS, a method of scoring the severity of vulnerabilities. Scores range from 0 (least) to 10 (most severe).

Cyber Kill Chain®, a framework for analyzing and defending against cyber intrusions, first discussed in a 2011 paper by Lockheed Martin Corporation.

Cyberattack, an attempt by hackers to damage, disrupt or destroy a computer network system.

Cybercrime, the violation of laws involving a computer or network.

Cybercriminal, an individual or group who commits cybercrime using a computer as a tool or as a target, or both.

Cyberthreat, the possibility of a malicious attempt to disrupt a computer network or system.

Dark Web, private networks not accessible by the general public. These networks are often used for nefarious or illegal purposes.

Delivery, transmission of malware to a target environment.

DoS (Denial of Service) and **DDoS (Distributed Denial of Service)**, attacks that make a machine or network resource unavailable to intended users. A DDoS attack originates from many devices at once.

Glossary

Drive-by download, malware that is unintentionally downloaded by visiting a website or opening an email or attachment, without the user's knowledge.

Exfiltration, the unauthorized extraction of data from an organization.

Exploit Kit, a malicious toolkit often used in cybercrime to exploit vulnerabilities in software applications.

Exploitation, execution of malware code in a target machine.

Firewall, software or hardware designed to control incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed, based on a predetermined rule set.

Forensics (or forensic analysis), in-depth study of malware (or an infected system) to determine its design, source, actions and other characteristics.

GUID (Globally Unique Identifier), a lengthy number that unambiguously identifies a software component or hardware device. Two identically configured computers would still have different GUIDs.

Hacktivist, a hacker whose activity (hacktivism) is aimed at promoting a social or political cause.

Honeynet, a network containing honeypot systems.

Honeypot, decoy systems set up to gather information about an attack or attacker and to potentially deflect that attack from a corporate environment.

IDS (Intrusion Detection System), typically network based, relying on signatures or heuristics to detect potentially malicious network anomalies.

Incident Response Program, an organization's plan for reacting to, and managing the impact of a cyberattack.

Injection, an attack performed by inserting malicious code or data into what the receiving system sees as a valid command. Injection attacks often use the PHP or SQL programming languages.

Installation, malware becoming resident in the target environment to provide ongoing (persistent) access by the attacker.

IP Reputation, a database that classifies IP addresses according to whether they are believed to host malware.

IPS (Intrusion Prevention System), typically network based and similar to an IDS, except it takes the added step of blocking traffic identified as having potentially malicious characteristics.

IRC, Internet Relay Chat.

ISP, Internet Service Provider.

Malware, a general term for malicious software including viruses, worms, Trojans, and spyware.

Malvertising, malware that appears as a benign advertisement on a Web page, and is activated when a user clicks on the ad.

NTP (network time protocol), a protocol for exchanging time-of-day information to keep system clocks synchronized.

Obfuscation, encrypting or substituting text (in source code, domain names, etc.) in order to obscure its true meaning or activity.

OWASP, the Open Web Application Security Project.

Paste site, a public website where anonymous users can publish information, including information gathered illegally. Searching these sites is one way to tell if an organization's data has been compromised.

Glossary

Patch management, a systematic process for installing vendor-supplied software patches.

Penetration testing (or pen testing), an authorized, controlled attack deliberately performed against a network to check for vulnerabilities.

Perimeter, the interface systems that connect an organization to the Internet.

Persistence, the ability for an attacker to continue activity inside a target environment.

Phishing, attempting to acquire information such as usernames, passwords and credit card details (and indirectly, money) by masquerading as a trustworthy entity in an electronic communication such as email.

PHP, a programming language often used for Web application development.

Proxy, a server standing (typically) between other machines and the Internet. Proxies can implement filtering and additional safeguards, or validate requests against whitelists or blacklists.

Ransomware, malware that encrypts a victim's data and demands a ransom payment in exchange for a decryption key.

Reconnaissance, research performed by attackers to identify targets and their vulnerabilities.

Remote Access Trojan (RAT), a type of Trojan designed to give remote access to malicious users.

Sandbox, software that executes suspicious code in a highly protected environment and examines its activities.

Sanitizing, validation of Web form input to ensure accuracy and to eliminate possible malware injection.

Social Engineering, gaining unauthorized access through methods such as personal visits, telephone calls or social media websites. These attacks primarily target people and take advantage of human weaknesses associated with security.

Sleep, an API call requesting that a program suspend itself (delay) for a specific period of time.

Spear phishing, a highly targeted phishing attack, using knowledge about a specific person or organization.

Targeted Attack, an attack aimed at a specific user, company or organization.

Threat Intelligence, the collection and expert analysis of data related to cyberthreats, leading to actionable recommendations.

Tor (originally from The Onion Router), network software that attempts to hide the identity and location of website visitors.

Trojan, a type of malware that masquerades as a legitimate file or helpful program but has been designed for nefarious acts.

Vulnerability Lifecycle Management (VLM), a systematic process for discovering, documenting, tracking and repairing vulnerabilities.

WAF, Web Application Firewall.

Weaponization, creating a deliverable file that contains an exploit. The file often appears to be a benign file type such as a PDF document.

Web Application Attack, an attack targeting vulnerabilities in (typically public-facing) websites.

Whitelist, a list of IP addresses or domain names believed to be free from malware. See also **blacklist**. Can also apply to authorized application programs or other objects.

nttgroupsecurity.com

NTT Group Security