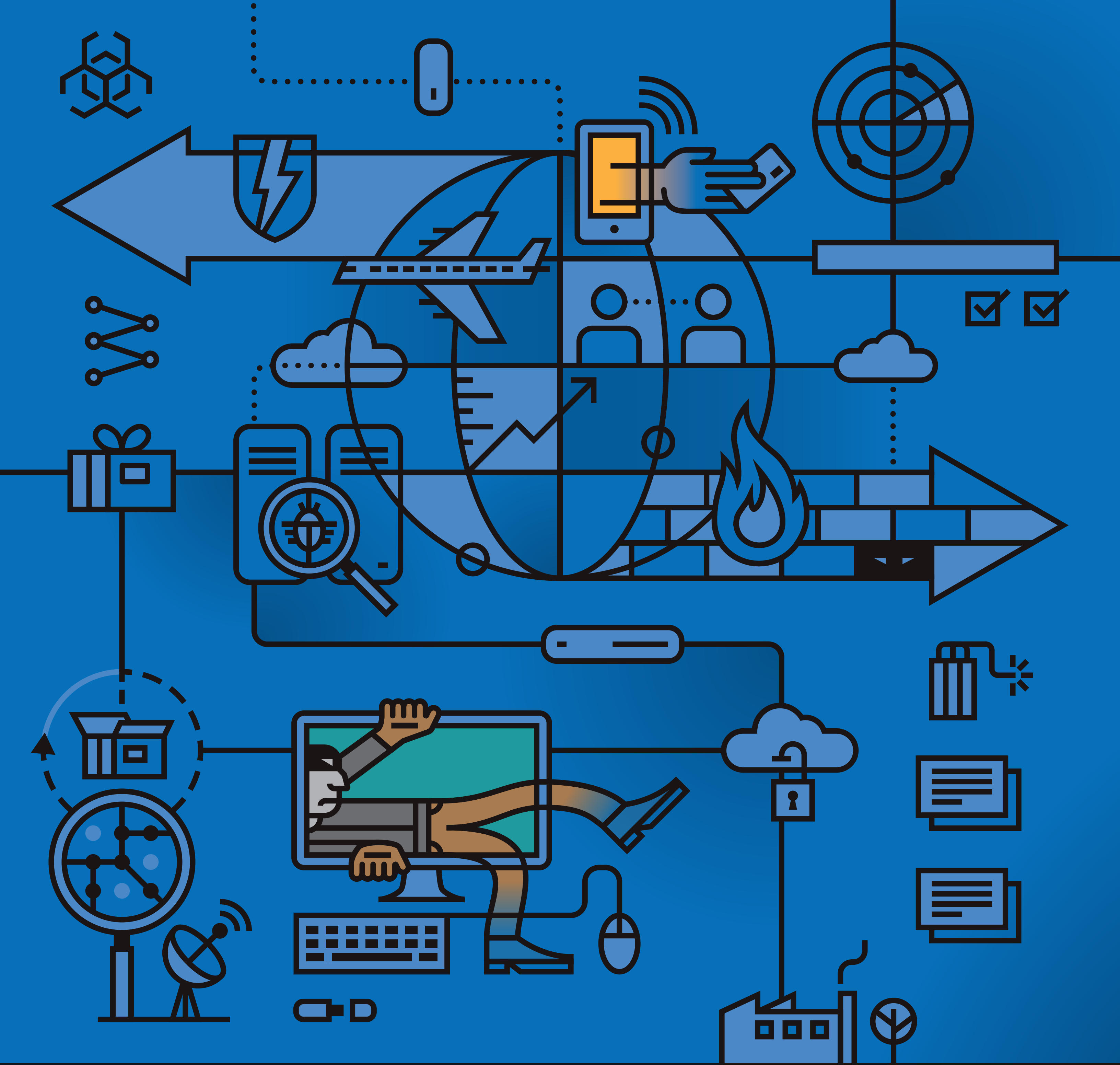


Security Engineering Research Team (SERT)

Quarterly Threat Intelligence Report Q2 2016

Table of Contents

Table of Contents – Continued

Introduction

Solutionary, an NTT Group security company, and its Security Engineering Research Team (SERT), focus on providing timely and actionable information allowing our clients to gain a better understanding of the threats facing their organizations today. This is accomplished through research and analysis of both current and emerging security threats affecting clients globally. Collaboration with the Solutionary Security Operations Center (SOC), Information Security Engineering Team (ISET), Professional Security Services (PSS) and Managed Device Team (MDT) allows Solutionary clients to benefit from our proactive approach to security research and the continuous evolution of ActiveGuard® detection capabilities.

The SERT Quarterly Threat Report provides a glimpse inside the research conducted by Solutionary researchers, security professionals and analysts, spanning the last three months and highlights the results of this research. In addition to a wide variety of open-source intelligence tools and honeypots, SERT also analyzes data from the Solutionary ActiveGuard® platform. The patented, cloud-based Solutionary ActiveGuard service platform collects, correlates and analyzes security events across systems for Solutionary clients globally, providing researchers with an even deeper understanding of the overall threat landscape.

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

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

Quarterly Highlights

During the second quarter of 2016 (Q2 '16), Solutionary security researchers and analysts uncovered information through the research of significant events identified through global visibility of the Solutionary client base. Some of the key findings based on this research include:

Global Threat Visibility

- Web application attacks, malware and application specific attacks comprised approximately 62 percent of all attacks during Q2 '16.
- The most common CVE detected during the quarter was CVE-2012-3373, a vulnerability in Apache Wicket. Solutionary detected both reconnaissance and attack activity throughout the quarter.
- The retail sector was the most targeted sector and was the focus of 18 percent of all attacks during Q2 '16.
- Attacks focusing on ActiveX or Adobe products accounted for nearly 48 percent of all attacks against the top five industries (retail, healthcare, education, finance and technology).
- The Neutrino, Magnitude and RIG exploit kits have replaced the faded Angler and Nuclear exploit kits as the most preferred kits.
- Germany was the number one source of all non-U.S. based attacks, with nearly 15 percent of attacks overall.
- The biggest increase in source of attacks was from Ukraine, which showed high volumes of reconnaissance and exploit attempts against Adobe Flash Player, Internet Explorer, Java and Joomla, mostly occurring after May 28, 2016.

Breaking Down Business Email Compromise (BEC)

- The FBI has reported a 1,300 percent increase in identified exposed losses due to BEC since January 2015.
- Since January 2015, BEC scams have hit over 22,000 victims worldwide and resulted in more than $3 billion in losses, an average of $135,000 per victim.
- The two most observed forms of BEC scams are fraudulent wire transfers and improper disclosure of employee W-2 information.

Ransomware in 2016

- With nearly 94 percent of detections, Cryptowall was the top ransomware Solutionary detected during Q2 '16.
- Ransomware detections decreased between January and February 2016 but have increased an average of 11 percent per month from March through May.

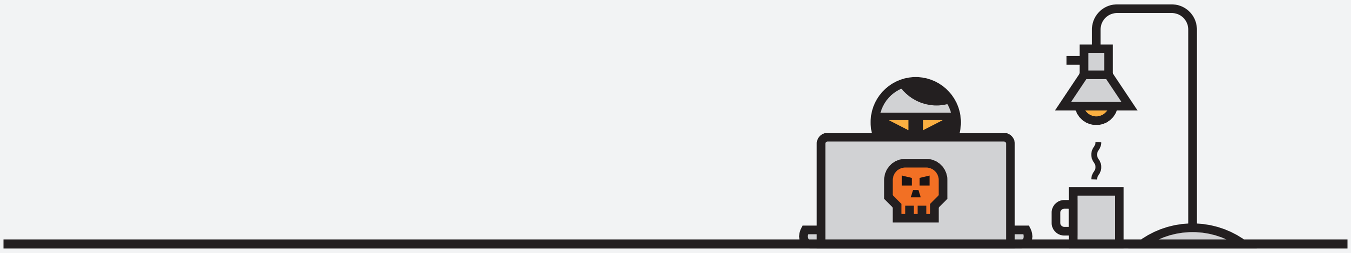
- The most targeted industry, healthcare, led with 88 percent of Solutionary detections. Affected industries also included education and finance, with all other industries combining for less than two percent.

China Five Year Plan

- In China's 12th Five Year Plan, covering 2011-2015, China identified healthcare, energy and government sectors as their top priorities. Many of the breaches experienced in Western nations within these industries over that time frame have been attributed to attackers affiliated with the Chinese government.
- The FBI reported a 53 percent increase in economic espionage, with losses estimated to be hundreds of billions of dollars. 95 percent of these cases were suspected to have been perpetrated by China.
- Based on their goals in China's recently released 13th Five Year Plan, the sectors most at risk of elevated attention from China are energy, the public sector, government and technology.
- China's 13th Five Year Plan includes goals to strengthen both offensive and defensive cybersecurity programs.

PCI 3.2 Highlights

- The Payment Card Industry (PCI) Security Standards Council (SSC) released version 3.2 of the PCI Data Security Standard (DSS) in April 2016.
- Assessments beginning after October 1, 2016 will be assessed against PCI DSS 3.2.
- New requirements are not effective until February 1, 2018, but Mitigation and Migration Plans should be in place for new requirements no later than October 1, 2016.
- The PCI SSC deliberately planned a long lead time for full compliance because they understood some of the required controls will require budget cycles and effort for implementation to be successful.
- Seven of the nine new requirements are for service providers only.



Global Threat Visibility – Observations and Trend Analysis

Attacks by Type

Solutionary researchers identified the top attack types from Q2 '16. Out of 11 categories, the top three – web application, malware and application specific attacks – accounted for roughly 62 percent of all attacks. Threat actors focused primarily on web applications, which saw nearly 24 percent of all attacks.

Researchers found threat actors used injection as their primary attack vector, as observed in over 45 percent of all web application attacks. Trailing behind were insecure direct object references and cross-site scripting (XSS). A majority of injection-based attacks included a collaboration of web server probing using Boolean expressions and targeted SQLi. These targeted attempts typically involved the use of a data manipulation language (DML), along with declarative and dynamic SQL statements. DML-based SQLi is common and often associated with opportunistic attackers attempting to retrieve sensitive data from or about the database. Attacks with dynamic and declarative statements are quite different and require more knowledge about the database, suggesting that attackers may have already completed some level of reconnaissance and have begun more advanced attacks.

Researchers also observed that a notable number of SQLi attacks leveraged DEALLOCATE statements, allowing attackers to remove any association between cursors and variables. Additionally, attackers used DECLARE statements to loop through multiple columns in various tables, select cursor variables and assign them a new value. This technique is typically used to bypass security measures or corrupt the database with malicious code. This tactic also suggests more advanced attack techniques.

Out of the top 10 most common SQLi techniques, researchers found the automated use of Havij to be number nine. Havij is an automatic SQLi tool with a user-friendly graphic user interface (GUI) for retrieving data from databases. Both low and high level attackers use Havij, which has the ability to perform SQLi vulnerability scanning as well, making it all the more attractive. Havij is clearly identified in the User-Agent header in HTTP requests as shown in Figure 2. Please note that the presence of the word "Havij" is a default tool setting which can be modified.

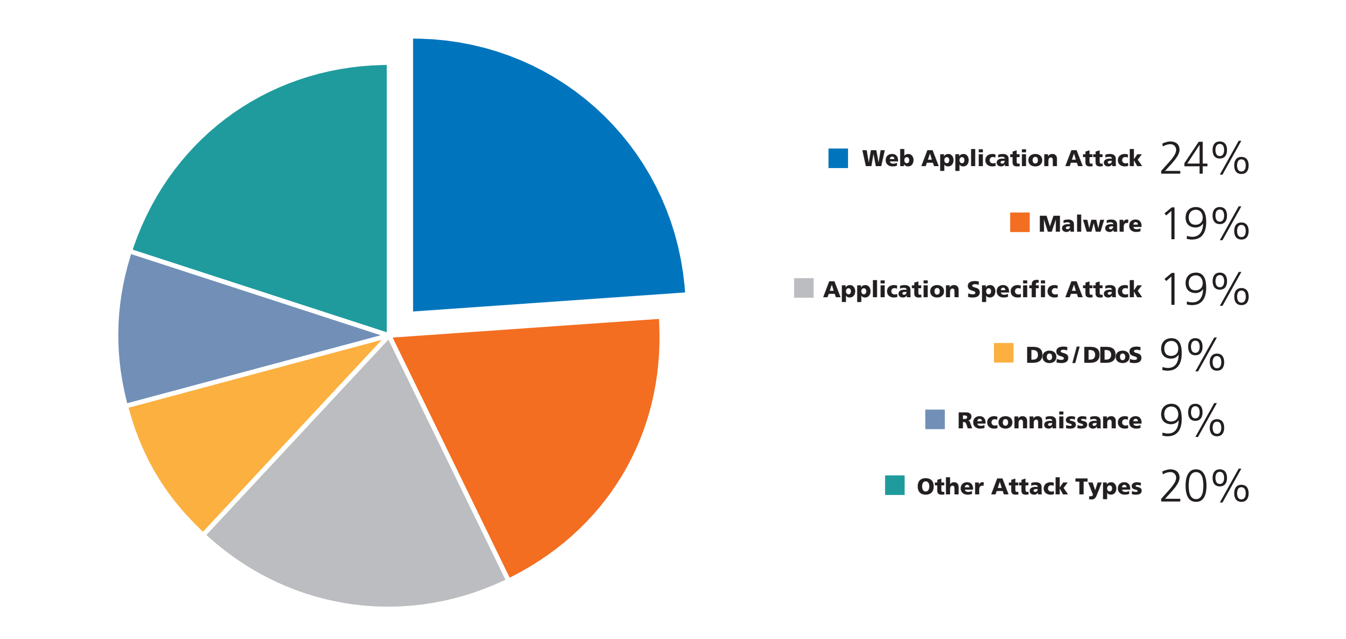
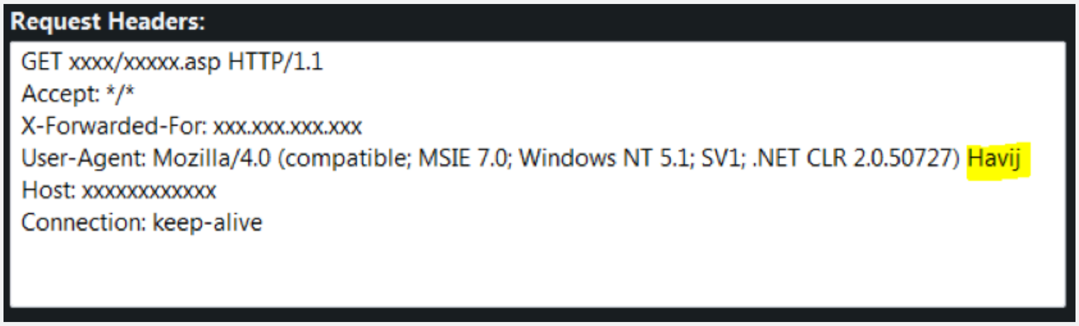


Figure 1. Attacks by type



```
Request Headers:
GET xxxx/xxxxx.asp HTTP/1.1
Accept: */*
X-Forwarded-For: xxx.xxx.xxx.xxx
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727) Havij
Host: xxxxxxxxxxxx
Connection: keep-alive
```

Figure 2. HTTP request from SQLi tool Havij

During injection based attacks, threat actors most commonly targeted PHP, IIS and Joomla. Attackers targeted server feature security flaws (e.g., Common Gateway Interfaces, CGI) in user input sanitation. These attacks lead to webshell installation, such as c99. From the beginning of April into May, Solutionary researchers observed a 13,000 percent increase in JBoss-based attacks, with attackers leveraging vulnerabilities from as far back as 2007. Attackers also used internet-wide scanning for JBoss webshells/backdoors such as Zecmd.

Figure 3 shows the web application vulnerabilities threat actors targeted most frequently throughout Q2 '16. Of these, CVE-2012-3373 was the primary target for attackers. Affecting Apache Wicket versions 1.4.3-1.5.7, this vulnerability allows web script or HTML injections by leveraging Ajax link URLs associated with Wicket. Solutionary researchers suspect threat actors perform Ajax fingerprinting to identify Ajax calls, allowing them to customize their HTTP requests so that the server cannot tell the difference between the local Ajax calls and attacker's requests. Requests are then embedded with scripts in HTTP query strings and headers and sent to the server. This attack vector could also be used to inject malicious code into pages on the Apache server. Since Apache Wicket is a Java framework, there are additional threats and vulnerabilities associated with it. Usage, if not configured correctly, may enhance vulnerable environments and increase risk.

Top Vulnerabilities	Type	Product	Patch
CVE-2012-3373	XSS	Apache Wicket	Link
CVE-2014-0160	Sensitive Data Exposure	SSL/TLS	Link
CVE-2015-5082	Injection	Endian Firewall	Link
CVE-2016-0482	Insecure Direct Object Ref	Oracle Application Testing Suite	Link
CVE-2015-6139	XSS	Internet Explorer, Edge	Link
CVE-2015-4031	Insecure Direct Object Ref	Visual Mining NetCharts	Link
CVE-2015-7297	Injection	Joomla	Link
CVE-2015-7808	Injection	vBulletin	Link
CVE-2016-0059	Insecure Direct Object Ref	Internet Explorer	Link

Figure 3. Top targeted web application vulnerabilities

Global Threat Visibility – Observations and Trend Analysis

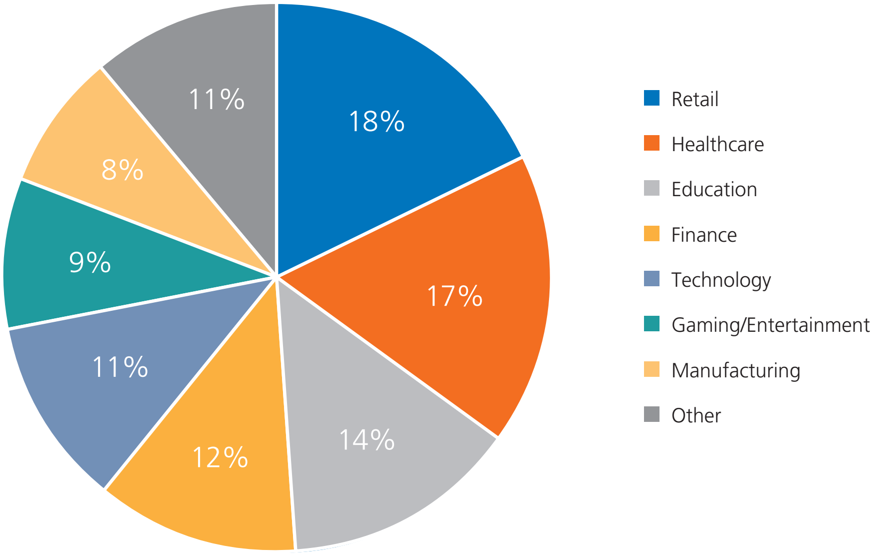


Figure 4. Targeted Industries

Below is a list of mitigation techniques for XSS and SQLi attacks.

- Perform input validation before writing to the database, and perform output validation for remote content.
- Sanitize user input against a formally-defined content specification.
- Establish and maintain an active patch management process to help reduce exposure from patched vulnerabilities.
- Use session tokens for specific hosts.
- Constrain privileges of applications, databases and users in the operational web environment (and any environment exposed to the internet) so scripts run in a limited authority mode.
- Leverage stored procedures at the database level to control user access permissions.
- Review OWASP's SQLi Prevention Cheat Sheet

Targeted Industries

Solutionary researchers analyzed the top targeted industries based on the number of attacks in sector divided by the number of clients per sector. The top five targeted industries were retail, healthcare, education, finance and technology. The retail sector was targeted the most with over 18 percent of attacks, but attacks across industries were widespread.

Researchers determined the common denominators for the top five industries were web application, application specific and malware-based attacks. Web application attacks resembled what had been previously mentioned in the Attacks by Type section of this report.

ActiveX and Adobe products were targeted in nearly 48 percent of all attacks for the top five industries. Of these, the majority of exploit attempts could have resulted in remote code execution (RCE). While ActiveX was designed by Microsoft and most ActiveX controls only run on Windows, ActiveX is not dependent on Windows operating systems. Both ActiveX and Adobe Flash Player are meant to enhance the end-user's experience while browsing the web, but both have inherent risks, typically leveraged in targeted attacks and compromised or illegitimate websites.

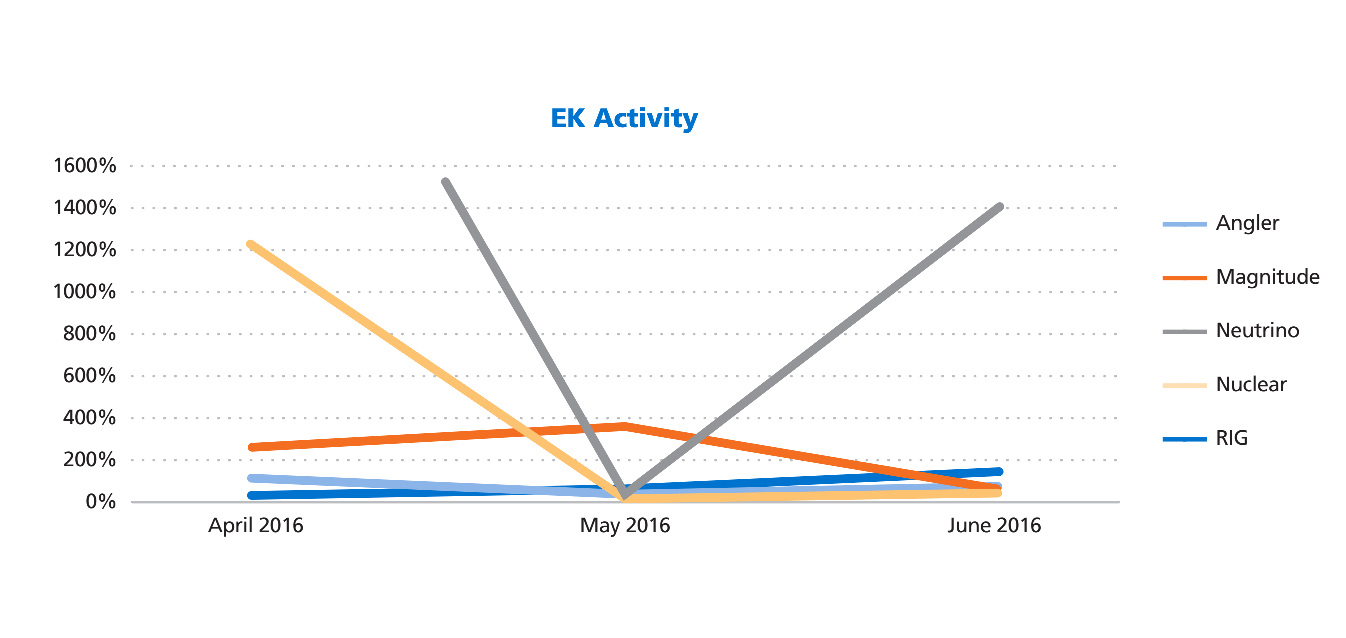


Figure 5. EK Detections

Internet Explorer (IE) has long been associated with ActiveX; however, as of January 2016, IE versions 10 and older are no longer supported by Microsoft, and IE 11 does not (by default) allow ActiveX controls to run. This suggests threat actors may be taking advantage of end-users who are running older, vulnerable versions. According to CVE Details, there have been 66 new IE vulnerabilities with no patches in IE version 10 and earlier. Additionally, 842 vulnerabilities exist in IE versions 9 and 10 alone. Microsoft has discontinued support for ActiveX controls in their new browser, Edge.

Adobe Reader and Flash Player showed a large attack surface with various vulnerabilities being attacked, most of which resulted in RCE or buffer overflows. While attack vectors vary, researchers determined threat actors were distributing Small Web Format (SWF), MP3, PDF, PNG and Dynamic Link Library (DLL) files with malicious code over the web and email. It is important to understand that exploit kits (EKs) are extremely popular for delivering Adobe exploit code to a victim's machine. Researchers analyzed the Adobe and EK attacks for Q2, determining 88 percent of clients experienced both EK activity and eventually Adobe exploits. Solutionary researchers identified less than a 12 percent difference between the total number of detections from Adobe products exploit attempts and the total exploits detected from exploit kits. This indicates a strong correlation between active exploit kits and their implementation of current exploits in Adobe products.

Researchers speculate Neutrino, Magnitude and RIG to be the primary threats in the future as Angler and Nuclear detections continue to dwindle, as explained in this article by Malware Don't Need Coffee researcher Kafeine. Although Angler is dead at the moment, a representative from InfoArmor stated that an Angler administrator stopped the sales of Angler, in order to "lay-low" following the arrests of a cybercriminal group in Russia. Figure 5 supports this statement by showing a 153 percent increase in Magnitude, 166 percent increase in Neutrino, 61 percent decrease in Angler and 93 percent decrease in Nuclear. These percentages represent the overall increase or decrease in number of detections between April and June. The latest version of Neutrino exploits CVE-2016-4117, a Flash Player vulnerability which allows the execution of arbitrary code, and distributes CryptXXX payloads.

Global Threat Visibility – Observations and Trend Analysis

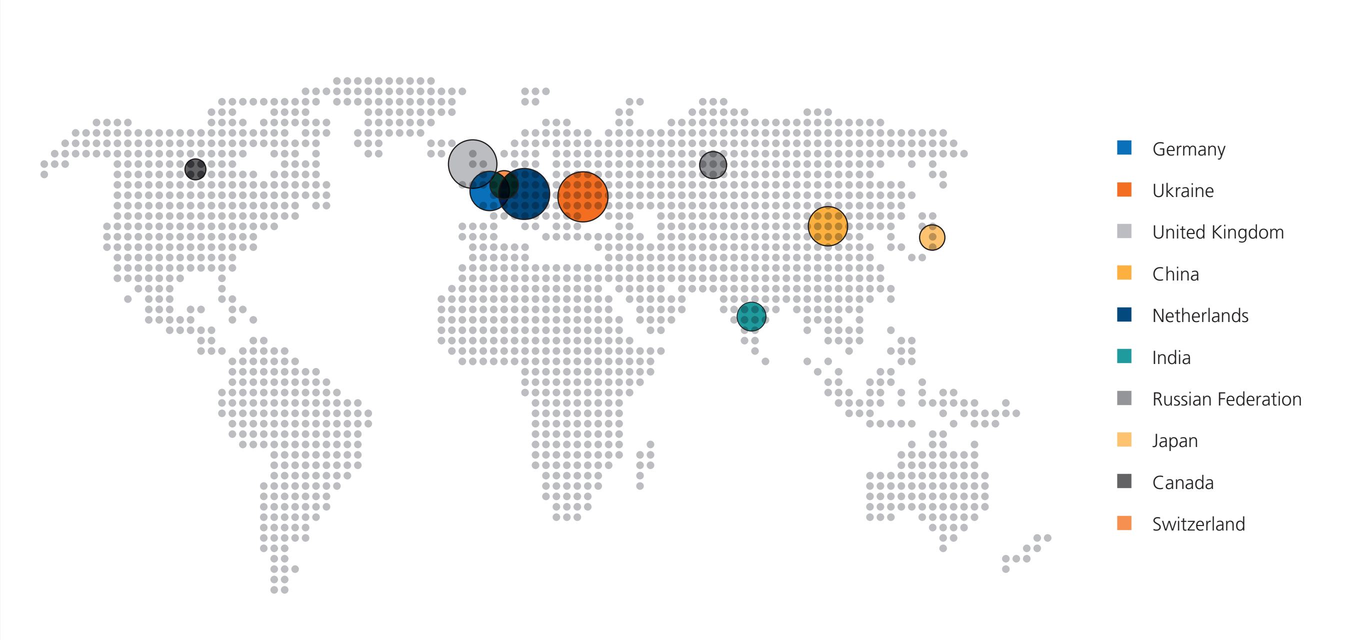


Figure 6. Attacks by source country

Top Foreign Attack Source Countries

The United States was once again the largest source of malicious activity, as the source of 68 percent of all attacks. As shown in Figure 6, Solutionary researchers trended the top 10 foreign attack countries throughout Q2, determining Germany to be the most hostile in regards to the number of malicious indicators across the Solutionary client base. Germany was the source of 15 percent of all malicious activity, while Ukraine, the United Kingdom and China trailed behind with roughly 10-13 percent each, showing a slight difference. As can be seen in Figure 7, Ukraine jumped back into the list after missing from the top 10 since Q2 '15. Activity from Ukraine included high volumes of exploit attempts against Adobe Flash, Internet Explorer, Java and Joomla, mostly occurring after May 28, 2016.

As a result, researchers focused more analysis on the sudden escalation in hostile activity from Ukraine. One of Ukraine's main focuses at the time of this report is its war with Russia, making motivations against United States based clients unclear. Solutionary does not directly provide services to Russian companies, which minimizes the potential that Solutionary was detecting hostile attacks directed at Russian clients.

While the cyberattack on the Ukrainian power grid is known in the security community, very few understand the cyber hurdles Ukraine currently faces. According to Ukraine Presidential Decree No. 96/2016, President Petro Poroshenko is heavily focused and invested in an approved strategy to deal with politically motivated cyberattacks, infrastructure vulnerabilities, cybercrime and Russian threats. Ukraine has about 80,000-100,000 IT specialists but has problems attracting qualified candidates to work in the public sector. Ukraine has stated they wish to increase the quality of their defensive and offensive cyber capabilities, but they have not yet been successful in attracting enough talent to build a state-sponsored Ukrainian cyber army, according to a blog by the Atlantic Council. The blog also notes severe cybersecurity legislation issues in Ukraine, contributing to a decrease in the effectiveness of efforts to address cybercrime in and from Ukraine. All things considered, it seems most likely that Ukraine is serving as a "cyber-haven" for attackers, whether abusing hosting services to obfuscate their identity and handicap attribution, or working directly from Ukrainian locations.

Change	Rank Q2 2016	Rank Q4 2015	Attack Source	% of Attacks
▲	1	5	Germany	15%
▲	2	>20	Ukraine	14%
▼	3	1	United Kingdom	13%
▼	4	2	China	10%
■	5	5	Netherlands	9%
▲	6	>20	India	8%
▼	7	3	Russian Federation	7%
▲	8	>20	Japan	7%
▲	9	>20	Canada	6%
▼	10	7	Switzerland	5%

Figure 7. Top foreign attack source countries

Researchers combed through Solutionary ActiveGuard data to discover the following points of interest from Ukrainian-based attacks.

- Adobe Flash Player, IE, Joomla, Java, SSL and outdated Windows systems are primary targets.
- The most significant reconnaissance efforts are against publicly facing servers using service enumeration and host discovery.
- 36 percent of malware variants detected are spyware/ keyloggers.
- 71 percent of all attacks are application specific or web-application based.

Given the types of reconnaissance and attacks being conducted, organizations should consider four recommendations to help manage the security of their environments:

1. It is more important than ever to aggressively patch the systems and capabilities being targeted (Flash, IE, Joomla, Java, SSL, outdated Windows, public facing systems and web applications) or consider removing them from organizational environments.
2. While anti-malware solutions are not 100 percent effective at identifying and defeating all malware, they can help reduce exposure.
3. Enhance web-application security by using security-aware coding techniques, and perform aggressive testing of web applications before they are fielded to isolate and fix vulnerabilities.
4. Perform configuration management by comparing baselines to current system states. This will aid in detecting anomalies which would suggest post-compromise or infection-related activity.

Breaking Down Business Email Compromise (BEC)

Business Email Compromise (BEC) may not be the biggest threat to businesses, but it is enough of a threat that the FBI has issued several warnings about how significant it is. Attackers are recognizing the success of such techniques as the attack has relatively high reward for comparatively low risk.

The FBI reports that there has been a 1,300 percent increase in identified exposed losses since January 2015. The FBI's latest numbers show that since October 2013, BEC scams resulted in over 22,000 victims and greater than $3 billion in losses – an average of over $135,000 per victim. The FBI states that BEC scams have targeted victims in all 50 states and 100 countries. The FBI bases their numbers at least in part on the information collected from their Internet Crime Complaint Center (IC3) and admits they would not be surprised if these numbers are actually underreported.

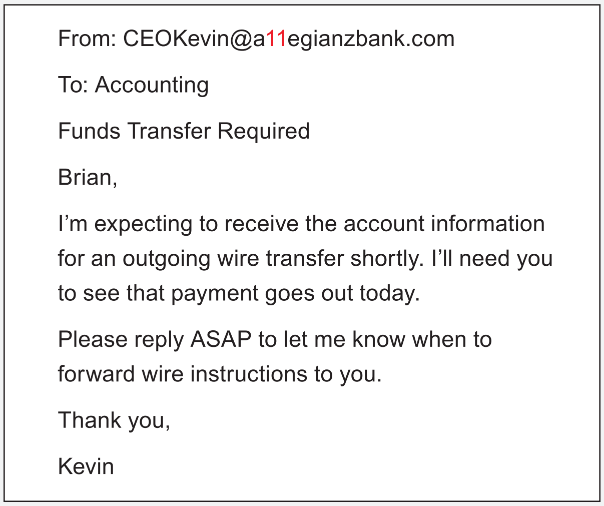
In comparison, Privacyrights.org includes records for nearly 4,900 breaches from all reported sources going back to 2005. While Privacyrights.org may not be a comprehensive source, it is generally respected as reasonably representative and reliable. Based on available information, BEC scams may very well be one of the most significant attack vectors businesses are currently experiencing.

What is BEC?

BEC is a phishing scam designed to take advantage of our reliance on email. An attacker pretends to be a person of authority and submits an email requesting some action. Internal staff responds to the email, taking that action as if it had been a valid request. BEC emails have also been called "CEO Fraud," since they most often appear to originate from the CEO (but can appear from anyone with authority to request such actions, like the CFO or other officer of the company). These emails come in a variety of forms, including the following:

1. An email from the CEO or CFO which includes an urgent request for a wire transfer. The details accompanying the request would be associated with an account to which the attacker has direct or indirect access.
2. An email from a vendor requesting payment for some service or product, including details for the attacker's account (but alleging it is the vendor's account). This often includes either a valid copy or an edited copy of a vendor invoice.
3. An internal email requesting wire transfers to one or more vendors to complete payments for invoices. The valid vendor account details would be replaced with details for accounts owned by the attacker. This often includes copies of vendor invoices.
4. The attacker may also not go after wire transfers. This same technique has been used to obtain employee W-2 information in many attacks. W-2 information includes salary details, along with social security number, full name and address details, potentially simplifying identity theft.

The email attack itself is relatively straightforward. That email is usually preceded by the attacker gaining some knowledge about the target organization. The attacker gathers intelligence about the organization via a variety of techniques, including public reconnaissance, social media reconnaissance, social engineering or compromise of internal systems (including the use of malware and keyloggers). Some of the victims have been successfully attacked so that the attacker can learn details about their internal operations and processes, including who the correct contact people are to get the W-2 or wire transfer request. For the BEC attack to work effectively, the attacker needs that internal information first. It is not as effective for an attacker to start with no knowledge of the target's internal processes.



From: CEOKevin@a11egianzbank.com

To: Accounting

Funds Transfer Required

Brian,

I'm expecting to receive the account information for an outgoing wire transfer shortly. I'll need you to see that payment goes out today.

Please reply ASAP to let me know when to forward wire instructions to you.

Thank you,

Kevin

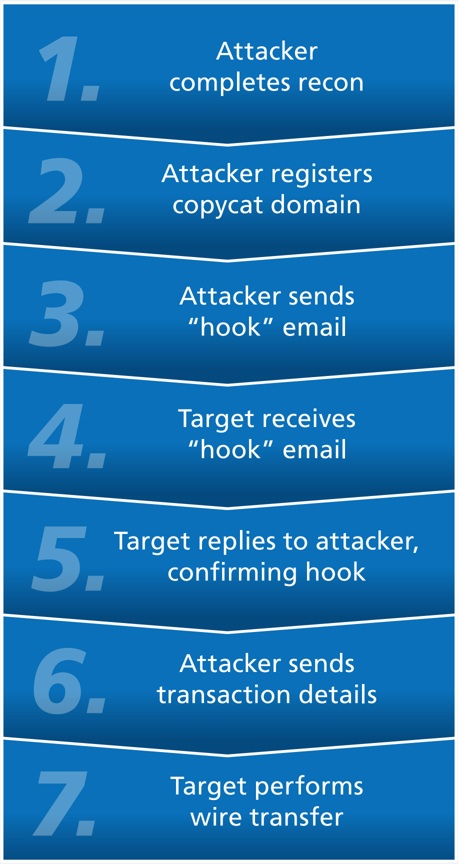
Figure 8. Example BEC hook email

Once the attacker has that information, sending an email is a relatively simple process. The attack is accomplished via a variety of related techniques. The most common technique Solutionary has identified is via the registration of a fake domain. For purposes of an example, let's assume the attacker is going to target AllegianzBank.com. The attacker completes enough reconnaissance to know Allegianz Bank's normal wire transfer process includes an email from Kevin, the CEO, to Brian, the person in Finance who actually completes the wire transfer. The attack proceeds as follows:

1. The attacker completes their target selection and reconnaissance.
2. The attacker registers the copycat domain A11egianzbank.com (using two ones instead of "L"), typically one to three days prior to the actual attack. The attacker will typically use a free registration service or pay for the service with a stolen credit card.
3. The attacker creates a "hook" email from a responsible authority within the target's organization. In this example, the attacker identified Kevin, the CEO. That user becomes "CEOKevin@a11egianzbank.com" (the fake domain), which is then used to send an email (Figure 8) from the fake domain to the real Brian@allegianzbank.com, the person who would conduct the wire transfer.
4. Brian receives the email, and believes it was sent by the real CEO, Kevin. The attack relies on Brian failing to recognize that the email came from a11egianzbank.com instead of allegianzbank.com. The email often includes a manufactured history of email conversations between CEO Kevin and other internal staff, designed to help support the validity of the email.
5. Brian replies to the email to ask Kevin for details of the wire transfer. Since the email was actually sent by the fake CEOKevin@a11egianzbank.com, the "reply" is successfully delivered to the fake account at the copycat domain.
6. The attacker, in turn, replies to the response from Brian with transaction information, including the amount and account number. This email is also generated from CEOKevin@a11egianzbank.com.
7. Once again, Brian does not recognize the copycat domain, and believes he has an email from the real CEO, Kevin. Brian performs the wire transfer using the information provided by fake Kevin.

Most BEC scams follow a process similar to the above process. In some cases, the attacker will compromise the email account of the appropriate requester (in the above example, CEOKevin) and send the hook email and transaction details from the genuine internal email address. In other cases, the attacker will simply spoof the email from CEOKevin and substitute a forged address (to which the attacker has access) for the "reply to" address. Sometimes the attacker does not use a hook email at all and leads with the wire transfer request, but the overall process is similar.

These emails are often delivered in timeframes during which the alleged source of the emails (the real CEO) is out of the office, and may not be easily reached for confirmation. These emails often include some sense of urgency (e.g., "must be completed before COB") and requests for secrecy (e.g., "don't discuss this with anyone else").


1. Attacker completes recon
2. Attacker registers copycat domain
3. Attacker sends "hook" email
4. Target receives "hook" email
5. Target replies to attacker, confirming hook
6. Attacker sends transaction details
7. Target performs wire transfer

How Does the Attacker Get the Money?

In the earlier days of BEC, the destination of the initial wire transfer was often a bank in China or Hong Kong. Banks in these countries have been known not to be especially cooperative when tracking down stolen funds, which has made it easier for organizations to recognize these attacks. If an organization never does business with China, and suddenly they are conducting a series of wire transfers to Chinese banks in a short time frame, it may be a strong indicator that they are being attacked via BEC. Many organizations and their banks recognized this trend, as have attackers. The FBI states that fraudulent transfers have now been sent to 79 different countries.

BEC attacks are more complicated than the attacker simply withdrawing funds from an account into which the funds have been transferred. Anti-money laundering rules help track transfers and withdrawals of $10,000 or more, but attackers get around these rules by making use of money mules and a variety of intermediate accounts which make tracking of the funds more difficult.

Romeo and Juliet

One technique which has become more common during the first half of 2016 is the use of a "Romeo and Juliet" scam. This has become especially attractive to scam artists from Eastern Europe. The attacker sets up an online dating profile and catfishes (an attacker pretends to be an attractive member of the opposite sex in an attempt to generate a romantic online relationship with the victim) an unsuspecting victim, pretending to develop a romance. As part of the romance, the victim is conned into opening an account so they can transfer funds to the attacker, who alleges to be someone who needs the money to escape some dire situation and visit the victim, often professing true love and a desire to date and even marry the victim. The BEC scam directs the wire transfer into the victim's account. The victim is then convinced to transfer the funds to a second account in the hope they will finally get to meet their young, Russian bride-to-be.

Almost needless to say, there is no "young, Russian bride-to-be," and the victim has just helped to enable theft via BEC.

Mule-Owned LLC

Attackers regularly send members of their organizations to the United States to serve as money mules. Typically, these money mules use fake identification to set up accounts soon after their arrival within the U.S. They often set up multiple accounts at several different financial institutions. Once the accounts have been established, the mule brings in referrals and opens other business accounts such as limited liability company (LLC) or doing business as (DBA) accounts. This action helps to establish these as valid business accounts. After the initial wire transfer from the target has been accomplished, the money mule makes several transfers to withdraw the funds, online or at multiple branches, and under the $10,000 per day limit to avoid detection from anti-money laundering systems.

Professional Cash Flow Manager

Individuals can be recruited via online help wanted ads to unwittingly help the criminals. The attackers list such jobs with titles like "Cash Flow Manager" and "Private Financial Processor," with promise of opportunities for high salaries while working from home. Individuals responding to these ads are counseled on how to set up business accounts capable of accepting wire transfers, as well as how to distribute any deposited funds. The "Cash Flow Manager" either takes a cut of the transfers as payment, or may be promised a commission after they have accomplished some number of transfers. That commission is often not paid.

Not Always Cash

Alternatively, funds may be exchanged for goods. Money mules, or scammed people (another fake job with a title like "shipment expediter") may buy large quantities of products and ship them to other locations, where the product will be resold for cash.

Sometimes, the money is converted to prepaid cards which are then redistributed for use and sale. These funds have also been transferred through wire-transfer agencies.

International Banking at its Best

When the money mule or innocent account owner (or sometimes not-so-innocent account owner) transfers money out of their account to other banks, the trails turn to dust fairly quickly. An initial $100,000 deposit can turn into 15 or more transfers of $4,900 to $9,900 to other accounts in other institutions. Unfortunately, there is no reliable way to identify any pattern in these transfers.

The FBI has indicated that fraudulent transfers have been sent to financial institutions in 79 different countries. Many of these countries are not especially cooperative with banks or law enforcement in the United States. These banks also follow local laws, which may effectively limit how much help they could be even if they wanted to. Combine this with different languages, diverse cultures and numerous time zones, and funds can disappear quickly. An efficient operation can move funds from a single initial bank in the United States to other banks based in the U.S. and Canada, then onward to banks in China, Hong Kong, the Republic of Moldova, Ukraine, Russia, Malaysia and Vietnam, or any other country in which the criminal has an account, in a matter of hours. For all practical matters, once the funds have been moved out of that initial account, the criminals can continue to move the money faster than banks can track the accounts and stop additional transfers, especially if the initial transaction happened late on a Friday or at the beginning of a holiday weekend.

What Can You do to Combat BEC?

An organization can reduce their exposure to BEC through a variety of both technical and procedural controls. These controls are not complicated, but they do require discipline, relying heavily on personal conformity with defined controls.

- Avoid the use of free, web-based email platforms, especially for high-dollar financial transaction business. If you are using such services, ensure you are employing multi-factor authentication options. Verify that forwarding and recovery options are appropriately controlled.
- Enable spoofed email protections so that external email for internal employees is flagged as being spoofed, perhaps even blocked. For instance, if the email server of allegianzbank.com receives an email from the internet with a "from" address of allegianzbank.com, the email server should know this email is an attempt to spoof the source of the email.
- Increase protection against impersonation attacks by using technologies such as sender policy framework (SPF), digital signatures, and Domain-based Message Authentication Reporting and Conformance (DMARC) in email accounts.
- Create intrusion detection system rules which flag emails with extensions similar to company email. For example, for the company allegianzbank.com, email originating from similar email domains (such as a11egianzbank.com, alleg1anzbank.com, or allegianzbank.biz) would be flagged as fraudulent email.
- Register all company domains which are logical variations of the actual company domain. If Allegianz Bank registers and takes ownership of domains like a11egianzbank.com, alleg1anzbank.com, allegiansbank.com and alegianzbank.com, it can make it harder for an attacker to register an effective copycat domain.
- Know the habits of your customers, including the details of, reasons behind and amount of payments. Organizations should pay special attention to requests which include an increase in the frequency of payments (like from once per month to twice in a week) or in amounts (like increasing from $30,000 payments to $130,000 payments).
- Carefully scrutinize all email requests for funds transfer to determine if the requests themselves are out of the ordinary. Organizations should scrutinize requests which carry a sense of urgency (e.g., "this should be completed ASAP!"), requests that specifically request secrecy (e.g., "this is of utmost sensitivity and should not be discussed outside of this email") or requests which occur while the originator is out of the office, or if the person who requests the wire transfer deviates from your organization's historical practice (e.g., if the CFO has always authorized the wire transfer, and suddenly the CEO is directing that a wire transfer take place).
- Be especially wary when such emails are delivered at the end of the day or the end of the week, especially before an extended holiday weekend. Attackers often use non-business hours to help give themselves time to disburse the stolen funds, since banks are often closed during such timeframes, which can make it harder for the victim to track down the funds before they are moved.
- Check with your insurance company to determine if your organization is covered for funds lost due to a BEC scam. Most cyber-risk policies do not cover such loss, which

means incorporating BEC scams into your incident response plan is critical.

- Perhaps most importantly, do not rely on email verification for sensitive processes such as approvals of wire transfers. Verify changes in vendor payments or wire transfers by adding two-factor authentication or having a secondary approval and sign-off which functions outside of email. Use a hardcopy sign-off process, or a process supported by a separate internal system, or at least have telephone contact with a known, registered phone number (not with any phone number in the hook email). Do not enable exceptions which can be exercised by attackers; consistently enforce the functional process.
- Don't try to track down the transferred funds yourself. Contact your bank. They will have better contacts and resources to maximize your chances of freezing and recovering any funds.
- Report any attempts at BEC. The FBI says that regardless of the size of the loss, they are hoping victims will file a complaint regarding the BEC at http://www.ic3.gov.
- Be aware that time is of the essence. If notified immediately (minutes or hours, not days), law enforcement and financial institutions can work with you to increase the chances of recovering some or all of the stolen funds.
- Conduct security awareness training exercises to increase employee knowledge of these scams. Include examples of BEC emails appropriate in your organization's environment – avoid generic examples.
- Test your organization by submitting your own fake email and observing how well your staff react to the "attack."
- The FBI includes additional guidance in their June 14, 2016 public service announcement.

References

https://www.consumeraffairs.com/news/fbi-reminds-companies-to-watch-out-for-business-email-compromise-scams-040816.html

https://www.fbi.gov/cleveland/press-releases/2016/fbi-warns-of-rise-in-schemes-targeting-businesses-and-online-fraud-of-financial-officers-and-individuals

https://www.ic3.gov/media/2016/160614.aspx

http://www.privacyrights.org/data-breach

Ransomware in 2016

In 2016, ransomware has already become one of the most popular security topics for the media, bloggers, forum discussions and conversations among professionals. Although ransomware dates back to 1989, threat actors have recently taken a particular interest in the return on investment (RoI) which ransomware promises and have increased their time, effort and money invested into developing and distributing both old and new strains.

Below is a timeline of the significant ransomware points so far in 2016, with a synopsis for further insight:

Synopsis

Starting in January, Ransom32 became the first ransomware variant to be written completely in JavaScript using Node.js. 7ev3n emerged soon thereafter, completely focused on denying recovery capabilities, subsequently destroying systems and demanding 13 bitcoin (BTC). 7ev3n-HONE$T was an update, which fixed the aftermath of infection and demanded a smaller ransom.

In February, TeslaCrypt infected numerous sites managed with WordPress, the number one content management system (CMS) platform. Locky soon emerged, spreading via Dridex's pre-existing P2P infrastructure, eventually causing numerous, well-publicized breaches, including a hospital in Hollywood, CA.

CTB-Locker received updates and started compromising websites. In March, SamSam became known as a result of threat actors conducting targeted intrusions and installing payloads manually, a step back from typical distribution efforts via exploit kits or spam.

Cerber, another new variant, showed authors leveraging crypters to pack and obfuscate source code. Developers added a "malware factory" feature for C2 servers to produce a new hash every 15 seconds.

KeRanger became the first Mac OS X based ransomware but was short lived.

Fully encrypting Master File Tables (MFT), Petya became a new but different strain. In April, authors invested greater time and resources into advanced variants, Maktub and CryptXXX.

JANUARY

Ransom32
7ev3n
Hidden Tear Source Code

FEBRUARY

Compromised WordPress
Locky
Hollywood Hospital
CTB-Locker for Websites

MARCH

Samsam (Samas)
Cerber
KeRanger
Petya

APRIL

Maktub
Jigsaw
CryptXXX

MAY

Zcryptor
TeslaCrypt Decryption Key
Kansas Heart Hospital

JUNE

FLocker
RAA
93% of Phishing

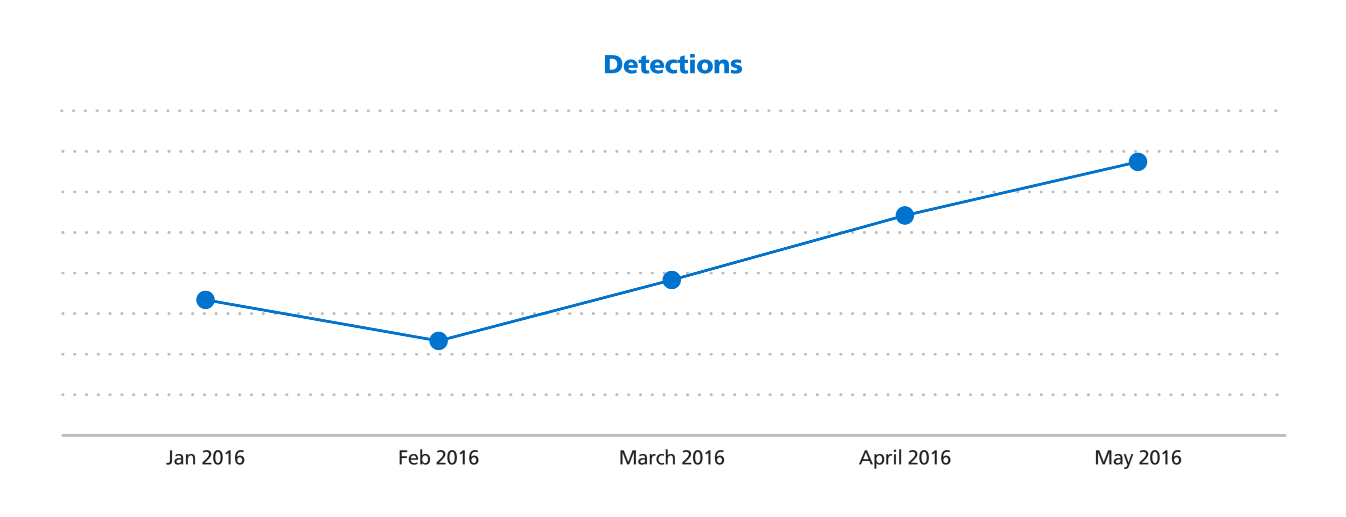


Figure 9. Ransomware detections

Maktub included sophisticated encryption, obfuscation and persistent techniques, coupled with a dynamic payment remission site hosted on .onion nodes. CryptXXX emerged, leading to version 3.2 and becoming a favorite among attackers.

In May, Microsoft announced the discovery of Zcryptor, a self-propagating strain, leveraging autorun.inf. Surprisingly, TeslaCrypt authors released a master decryption key leading to the creation of multiple tools. A hospital in Kansas became infected with SamSam and paid the ransom but did not receive decryption help as promised. In mid-June, researchers discovered FLocker, a "police" ransomware strain targeting mobile Android devices, including some smart TVs, which had been an unexplored target.

What We Know So Far

Based on the above Q1 and Q2 '16 recap, ransomware variants continue to emerge from authors who are both knowledgeable and skilled. The ability to develop strains based on programming packages like Node.js demonstrates a shift in authors' mentality to create strains compatible with various operating systems. Distribution via email, compromised websites and exploit kits remains prevalent, as successful infection rates provide no reason to change delivery method. As authors begin to reap the monetary benefits of ransomware campaigns and gain an understanding of which entities are paying ransoms, the motivation to create modular and robust strains becomes the norm, as evidenced with Cerber, CryptXXX and Maktub.

Continuous development cycles suggest Ransomware-as-a-Service (RaaS) and successful campaigns delivered via TeslaCrypt, Locky, Cerber and CryptXXX will not be abandoned after attaining their initial goal, money. As development continues, researchers are finding it more difficult to reverse-engineer variants and conduct cryptanalysis on encryption methods, thereby assisting victims with a decryption key. This escalation suggests ransomware authors are well aware of the battle between reverse-engineers, cryptanalysts and ransomware authors.

Solutionary Observations

Solutionary researchers trended ransomware data from January 1, 2016 through June 8, 2016. Analysis is based on the number of detections, which could multiply, as security appliances flag multiple stages of a successful ransomware infection.

Figure 9 shows that the number of ransomware detections began to decrease from January 2016 into February 2016. Shortly after, however, it began to steadily increase at an

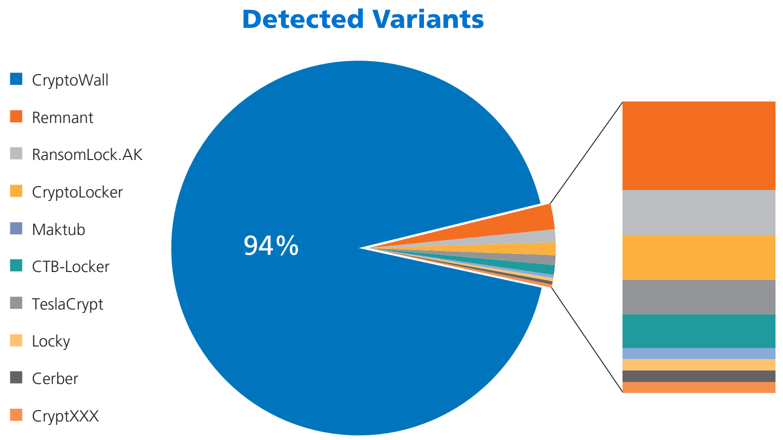


Figure 10. Detected ransomware variants

average of 11 percent per month from March through May. Researchers speculate this to be a combination of increased ransomware variants, accessibility and phishing. According to Bart Parys, a security researcher tracking ransomware variants, there are roughly 124 variants so far in 2016. Correlating this to a recent malware report, 93 percent of phishing emails now contain ransomware.

Figure 10 shows the ransomware variants Solutionary researchers detected. As shown, CryptoWall observations were nearly 94 percent of all detected ransomware. Researchers observed primarily outbound connections, C2 server check-ins and beacons, depending on CryptoWall's version. According to a recent blog, CryptoWall, Locky and Cerber were the top three observed ransomware variants recorded in Q2 '16.

Figure 11 shows the industries affected by ransomware, based on the Solutionary client base. Healthcare clients had the most, with 88 percent of all detections. Healthcare has recently become a primary target for ransomware campaigns,

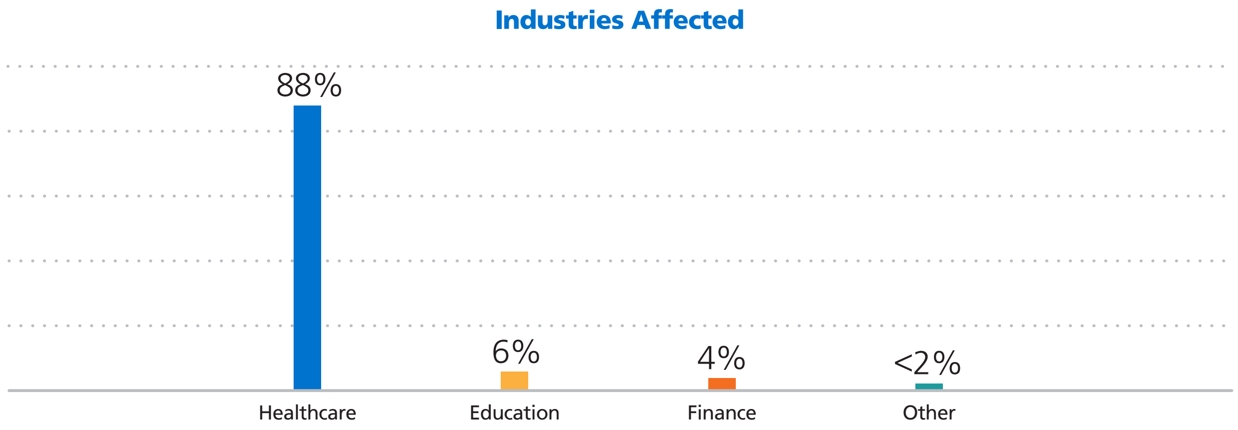


Figure 11. Industries affected

because the industry has often paid the ransom. When executing a disaster recovery plan (DRP), it is important to recover systems as quickly as possible for business continuity; however, when dealing with human lives whose treatment depends on those systems, paying a few thousand dollars is often the preferred choice. This tends to increase attackers' targeting of healthcare networks with ransomware.

The Future of Ransomware

Evasion

Evasion is critical to covering the attacker's footsteps during a successful intrusion. Ransomware developers have placed priority on the ability to evade popular "sandbox" environments and anti-virus engines. Recent strains which use FUD/crypters suggest that ransomware authors understand that researchers are reverse-engineering their strains. As a result, authors will continue to implement evasion techniques into ransomware variants, which in turn, limits the availability of decryption tools. The combination of FUD/crypters and executable packers like UPX will make research significantly more difficult.

Many new variants have the capability to encrypt files offline using system-specific tools like Windows CryptoAPI, thus reducing the ability to detect C2 communication and unexpected processes. Hashes will be unreliable as authors adopt "malware factories" to create hashes on the fly for each variant.

Persistence

In 2016, persistence has seemed an important priority for ransomware authors as they discovered specific locations within victim systems in which they would create undetected files, especially in Windows systems. Recently, authors have included features which allow ransomware to leverage Windows registry keys, autorun and autostart functions. Although Windows systems are the typical targets when developing ransomware strains, authors familiar with Linux will inevitably create similar strains which take advantage of features such as cron jobs, or other features possessing similar traits of Linux rootkits. These will adopt pre-existing process names, thereby avoiding detection.

Infrastructure

Over time, infrastructure setups have been crucial to widely popular ransomware strains and the success of their campaigns. CryptoLocker and Locky prove this assertion, as these ransomware variants were dependent on P2P setups from GameOver Zeus to Necurs. A solid infrastructure is valuable for anonymity (when using Tor) and resiliency (if a C2 server goes down). P2P protocols simply bounce back and use another host. Additionally, these infrastructures provide the ability to swiftly distribute ransomware strains on a massive scale. Leveraging infrastructures will only increase in the future as threat actors implement mass distribution and reap the rewards of multiple paying victims.

Self-Propagation

As depicted with Zcrypter, the use of crypto-worms is likely to grow rapidly, targeting a range of businesses and services. Threat actors using targeted selection are likely to distribute their strains to victims in an environment with multiple storage locations such as shared and network drives. This allows the crypto-worms to easily propagate not only to other drives, but to other systems as well, increasing the single-loss expectancy rate (SLE) and making incident containment more difficult. The arrival of improved propagation techniques is expected in the near future as threat actors attempt to determine new methods of increasing income, while simultaneously decreasing efforts.

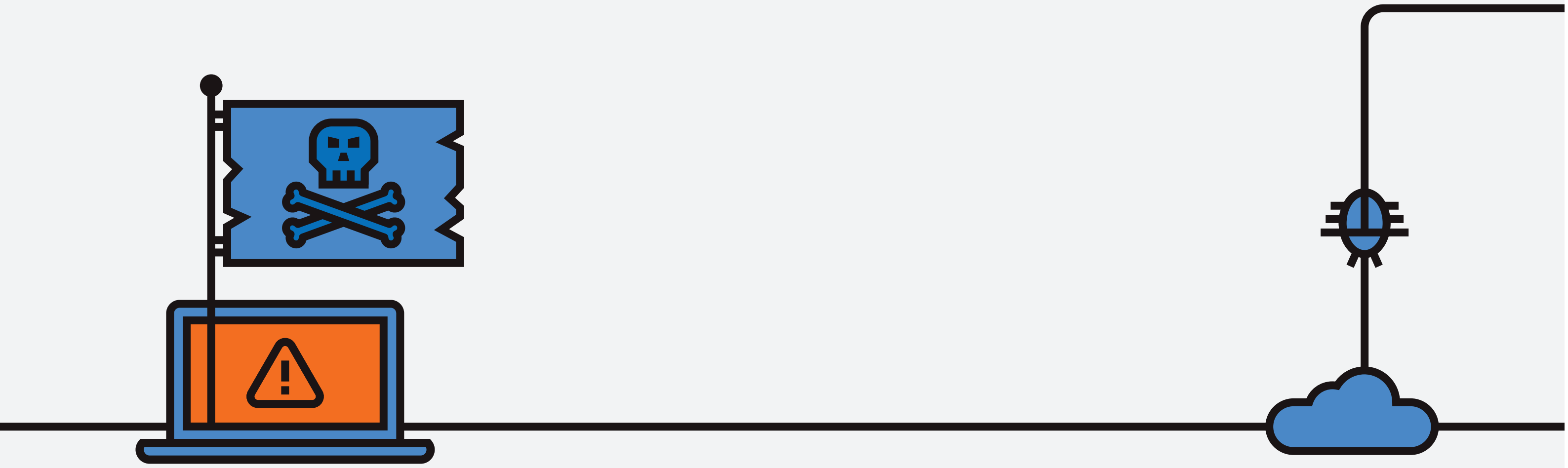
Targets

As healthcare and education sectors continue to be plagued with ransomware and often pay the demanded ransoms, the probability of more targeted attempts in these sectors will increase. Healthcare organizations use an abundance of systems and IoT devices which can become crucial pivot points for an attacker or can even be victims of ransomware themselves. As shown with FLocker, ransomware strains are common on mobile devices, servers, personal computers and more, but will inevitably become more common on IoT devices in homes. IoT disaster recovery plans are simply not created in these environments, so home users will be hit with the attack, and most will resort to paying the ransom or repairing or replacing the devices. Simply put, attackers will likely continue to focus on victims with diverse, complicated infrastructures who tend to reach the decision to pay the ransom more rapidly.

Recommendations

While a variant-based decryption tool or key can be a tool in your DRP, it is not dependable and should be the lowest priority when building a ransomware-specific mitigation strategy and DRP. KnowBe4 has completed a very helpful ransomware response manual which goes in depth about how to protect from ransomware, including a few checklists. Solutionary researchers also recommend the following:

- Security Awareness Training – Proper security awareness training will dramatically reduce the chances of an organization falling victim to ransomware. End users should be properly trained on email and web browsing policies. It may also prove beneficial to simulate different attacks, including a phishing email attempt.
- Backups – Using a combination of full and differential or incremental backup solutions is crucial when responding to ransomware incidents. Since ransomware targets shared drives, backups should be stored both off-site (at least off-line) and locally, providing minimal recovery time objective (RTO) if possible. It is important to test backup solutions and ensure they are planned and executed consistently.
- Anti-Virus Systems – Prevention is key, but detection is a must. AV systems should be used and regularly updated to ensure the latest signatures have been downloaded. This gives your security appliance the ability to detect the most recent variants.
- Defense-in-Depth – An “Information-Centric” defense strategy will include multiple layers of security at each level of the network, ultimately protecting data at the lowest level. This strategy ensures that security has been implemented at the perimeter, DMZ, internal network, host, application and data levels.
- Checklists – Solutionary has also prepared a checklist to help prepare organizations for ransomware attacks before they hit.



Decryption Tools/Keys

Below is a list of ransomware decryption tools made by cryptanalysis researchers who constantly reverse-engineer ransomware variants.

Variants	Decryption Tool or Key Link
TeslaCrypt	http://www.talosintel.com/teslacrypt_tool/
BadBlock	https://decrypter.emsisoft.com/
Xorist	https://decrypter.emsisoft.com/
Apocalypse	https://decrypter.emsisoft.com/
777	https://decrypter.emsisoft.com/
AutoLocky	https://decrypter.emsisoft.com/
Nemucod	https://decrypter.emsisoft.com/
DMALocker2	https://decrypter.emsisoft.com/
HydraCrypt	https://decrypter.emsisoft.com/
DMALocker	https://decrypter.emsisoft.com/
CrypBoss	https://decrypter.emsisoft.com/
Gomasom	https://decrypter.emsisoft.com/
LeChiffre	https://decrypter.emsisoft.com/
KeyBTC	https://decrypter.emsisoft.com/
Radamant	https://decrypter.emsisoft.com/
CryptInfinite	https://decrypter.emsisoft.com/
PClock	https://decrypter.emsisoft.com/
CryptoDefense	https://decrypter.emsisoft.com/
Harasom	https://decrypter.emsisoft.com/
Jigsaw	http://download.bleepingcomputer.com/demonslay335/JigSawDecrypter.zip
CryptXXX v1	http://media.kaspersky.com/utilities/VirusUtilities/RU/rannohdecryptor.exe
Petya - Process	http://www.bleepingcomputer.com/news/security/petya-ransomwares-encryption-defeated-and-password-generator-released/
CoinVault	https://noransom.kaspersky.com/
CryptoLocker	http://www.thewindowsclub.com/cryptolocker-decryption-tool

Figure 12. Decryption tools and keys

China's New Five Year Plan: Insight into Possible Cyber Targets

A cyber breach goes undetected for an average of 146 days. Granted, this is down from 205 days in 2014, but a sophisticated advanced persistent threat (APT) actor could do a significant amount of damage in five months' time. In some instances, APTs remained unnoticed for years. Sometimes, though, your organization gets an early warning that its data may be of high value and that it may become the victim of a breach. China's 13th Five Year Plan (FYP) may provide such a warning.

What is the Five Year Plan?

Initially implemented in China during 1953, many communist countries have adopted the practice of an FYP, reflecting the practice used by the Soviet Union since 1920. FYPs are a series of strategies which map out the government's vision of social, political and economic goals for the next five years, usually building on the goals and achievements in the previous FYP.

As China has transitioned to a more socialist market economy from a Soviet-style planned economy, the model for the FYP has evolved to a more modernized version designed to revitalize the Chinese nation. This evolution comes as a direct result of the information age.

While the information age has provided another avenue for China to leverage in their FYPs, this free flow of information is in direct contradiction to the Chinese government's rigorous attempts to control and manipulate online content available to its citizens.

Correlation between the FYP and Cyberattacks

Peter LaMontagne, former U.S. diplomat in Beijing during the 1990s, stated "there's a direct connection between the sectors highlighted in China's five year plans and the businesses that suffer breaches in the U.S.…and if it's a priority for China, it should be a priority for companies in the U.S. to protect themselves."

Intelligence agencies, along with some security researchers, assert that sectors identified for growth and the efforts outlined in China's FYPs will align with targets of cyberattacks. There is a direct connection between the two, as cyberattacks are used to enrich the industries deserving of focus in the FYP.

In its 12th FYP, covering 2011-2015, China identified the healthcare, energy and government sectors as some of the top priorities during those five years, and the U.S. and other Western nations saw enormous breaches in these sectors. While some of these breaches were coincidental, many are suspected to be the work of Chinese government-affiliated hackers. Along with attacks against many U.S. organizations in areas considered critical to the 12th FYP, high-level breaches occurred, also supporting guidelines set out during that timeframe:

- The U.S. Office of Personnel Management (OPM) lost 21.5 million sets of personally identifiable information (PII). This data included anyone who has applied for a security clearance, information on family members, SSNs, etc. Due to the sensitive nature of the data collected in this breach, it may be that this was a counterintelligence effort. More likely, though, is the potential for subsequent efforts in order to acquire additional information, especially since attackers acquired U.S. defense contractors' information. Follow-on efforts will likely include spear phishing or business email compromise (BEC) attempts to gain access to the networks of any major firm the United States Government works with for research and development, policies, procedures and best practices. Oddly, 25 percent of federal firms surveyed said they had not changed their security strategy after OPM was breached, and a majority of senior federal cyber officials said they don't think the U.S. can detect cyberattacks while they're occurring.
- Several major healthcare insurance providers saw extensive breaches as well, losing tens of millions of sets of PII. Researchers suspect China may be studying best practices for its aging population, which could be their reason for stealing such an extraordinary amount of PII during these massive breaches. Additionally, it may have been China's intention to prepare for providing healthcare to all citizens in the next several years, looking for the know-how to restructure its own healthcare system.

In July 2015, to highlight the growing threat to U.S. industries, the FBI launched a nationwide campaign warning industry leaders of the growing threat their networks and data faced from foreign actors. During the previous year, the FBI reported a 53 percent increase in economic espionage cases, which resulted in the loss of hundreds of billions of dollars from several large corporations in various industries. Economic espionage is defined as “theft or misappropriation of a trade secret with the intent or knowledge that the offense will benefit any foreign government, foreign instrumentality, or foreign agent.” China is suspected to have perpetrated 95 percent of these cases.

The 13th FYP — 2016–2020

Covering the years 2016 through 2020, analysts suggest that the newest FYP comes during a time of unprecedented slow growth for China. This could translate into more aggressive approaches to achieve the outlined objectives, including continued cyber espionage by state actors. The objectives and methods will likely expand on progress made in the 12th FYP.

The five principles which work in tandem to achieve the overall goal of “a moderately prosperous society” of the 13th FYP are:

- Innovation, to drive economic development
- Green, to protect the environment
- Openness, to engage in global markets
- Coordination, to ensure balanced development
- Inclusive, to ensure prosperity is shared by each citizen.

These tenets drive the overall goals of the 13th FYP. The primary goals are: reducing reliance on foreign technology and energy sources, developing green energy, reforming the military and providing healthcare coverage to each Chinese citizen by 2020. Much of the groundwork for these initiatives may have been laid during the massive breaches over the last several years during the 12th FYP.

As such, those industries mentioned should take special care in shoring up network defenses, though any industry may be susceptible.

- **Energy –** In its efforts to speed the transition from a coal-based to a clean-energy environment, China is expanding its efforts in developing renewable energy sources, to include solar, wind and nuclear power.
- **Public sector –** The extension of healthcare to all citizens by 2020, as well as changing the one-child limit to two children per couple, could raise government spending while it attempts to spur economic growth to 6.5 percent and double the GDP.
- **Technology –** As part of its focus, China wants to reduce the country’s dependence on foreign technology. China would like to grow its indigenous technological capability. This could pose a challenge to U.S. companies trying to gain a foothold in the Chinese market and could also potentially encourage intellectual property (IP) theft, thereby reducing development costs. In fact, it’s been reported that over the past two years, Beijing has cut a number of major foreign tech firms from its list of approved vendors.

Expect China to expand upon its advances from the last FYP. In fact, we may observe the use of previously stolen PII in subsequent spear phishing or business email compromise (BEC) campaigns, in further efforts to infiltrate pursued industries.

Latest Chinese Cyber Strategy

Released with the 13th FYP is China’s newest cyber strategy, another five year plan focusing primarily on improving software security and protecting state secrets and data. The policy, known as “Internet Plus,” is designed to increase internet control capabilities and “perfect cybersecurity laws and regulations.” The plan also states China will “strengthen

China’s “groovy” video explaining the 13th FYP, believed to be a propaganda piece for global consumption, suggests, “If you wanna know what China’s gonna do, best pay attention to the shi san wu (十三五, which translates to ‘China’s 13th FYP’).”

the struggle against enemies in online sovereign space and increase control of online public sentiment." The government is increasingly relying on the internet as a crucial domain to manipulate public opinion, squashing any anti-government sentiment. China also aspires to use the internet to bolster its slowing economy and envisions shaping itself into a global cyber power.

This policy comes on the heels of a significant anti-hacking deal between the U.S. and China in September 2015, which made it clear that neither country would conduct attacks against each other for financial gain.

It remains to be seen whether the anti-hacking deal is making a dent in combatting economic espionage against U.S. infrastructure. Although attack activity originating from China and targeting U.S. infrastructure showed no significant decline directly following the deal, researchers are now observing what appears to be an overall decrease in activity. Perhaps activity has declined, though it is interesting to consider other possibilities. Maybe they performed enough long-term analysis and penetrations that current efforts are simply more focused, and therefore, less visible. Perhaps with all the breaches recently observed, much of China's offensive cyber infrastructure has been revealed. There is a distinct possibility they have gone into "hiding" while they rebuild. Another possibility is that this is simply a period of transition as the new FYP is revealed. More frightening still is the possibility that Chinese hackers are so deeply embedded in any given network that their activity appears as normal traffic and may no longer be detected.

APTs and TTPs

Dozens of sophisticated APTs are suspected to be affiliated with Chinese government, military or intelligence agencies, each having specific areas of focus and both shared and individual tactics, techniques and procedures (TTPs), indicating a high degree of organization and discipline.

Unlike other nation-state actors who may have more malicious, destructive intents, including a "preparation of the battlefield," so to speak, Chinese APTs have traditionally appeared more interested in economic or business intelligence gathering for possible espionage purposes. For example, if a Chinese company is bidding on a contract against a U.S. firm, the knowledge gained from a successful cyberattack could give them a distinct advantage in negotiations. Chinese threat actors have also historically targeted information related to research and development, mergers and acquisitions and industry best practices.

That being said, Chinese APTs have more recently demonstrated their opportunism and adaptability, altering standard TTPs. Groups have been observed quickly taking advantage of zero-day vulnerabilities, as was observed with the exposure of the Hacking Team zero-days, and have recently been detected using ransomware, although the targets have not been identified.

This isn't the first time that suspected Chinese actors have gone outside of their "traditional" TTPs. In 2014, a group was observed using DDoS attacks after compromising poorly configured machines in a wide variety of sectors.

Although the motivations for the shift are unknown, these may be efforts to obfuscate other activity or may simply be more efficient means of accomplishing set goals.

Conclusions and Recommendations

75 percent of organizations are reported to be at significant risk of cyber incidents, while only 7 percent report having a mature cybersecurity capability.

As previously noted, we are only now beginning to see the fruits of the Chinese labor for the 12th FYP. Many of the targets of the last FYP are only now being discovered. TTPs will continue to evolve and IoCs will likely change. To determine the potential threat to your organization's networks and data, as well as to assist in identifying any possible breach attempts as quickly as possible, Solutionary recommends the following best practices:

- Conduct a business impact analysis (BIA) with the goal of identifying all of the organization's critical data and systems, and identify risk exposures for each.
- Conduct a risk-based assessment, designed to measure how likely the risk points in the BIA are to occur, as well as the impact they could have on your security and operations.

- Review your security program to ensure it is built on firm foundational security elements, including strong user identification and authorization, need to know and user education.
- Ensure your security plan supports effective defense-in-depth techniques, supporting data isolation and segregation.
- Consider a threat intelligence provider to enhance your understanding of foreign strategies and threat actors.

Regardless of the malicious actor or the attack vector, this is a good opportunity to remind users of operational security (OPSEC) measures, to review your insider threat program, and to take stock of what information users are sending, storing and destroying to ensure your critical business data is being protected.

Based on details in their 13th FYP, we should expect to see a drop in overall cyber activity from China against U.S. resources and organizations during the FYP transition. Additionally, expect to see the same actors, though perhaps with different infrastructure, since this FYP is a continuation of some of the same efforts as the last FYP.

Final Thoughts

As has been observed over the last year, China's economy can set the mood for the global economy, so much so that private and public industries alter their business models accordingly. The same should hold true for the cybersecurity model of each business. Since your potential adversaries are constantly adapting to their environment, it's not enough to rely on the security strategy you formed in 2010, and it is a good practice to continually update your security policies and strategy.

References

https://next.ft.com/content/40dc895a-92c6-11e5-94e6-c5413829caa5

http://www.zdnet.com/article/chinese-foreign-ministry-opposing-zte-trade-restrictions/#ftag=RSSbaffb68

http://thediplomat.com/2016/05/chinas-emerging-cyberspace-strategy/

https://www.nrdc.org/media/2016/160315-0

http://thehill.com/policy/cybersecurity/243296-china-set-to-issue-five-year-cyber-plan

http://www.cbichina.org.cn/cbichina/upload/fckeditor/Full Translation of the 12th Five-Year Plan.pdf

http://news.xinhuanet.com/english/china/2016-03/18/c_135202412.htm

http://www.bloomberg.com/news/articles/2016-05-19/u-s-can-t-detect-when-cyber-attacks-are-under-way-survey-finds

http://www.cnn.com/2015/07/24/politics/fbi-economic-espionage/

http://thehill.com/policy/cybersecurity/284235-security-firm-sees-sharp-decline-in-chinese-hacking

PCI 3.2 Highlights

The Payment Card Industry (PCI) Security Standards Council (SSC) has released version 3.2 of the PCI Data Security Standard (DSS), and this new version has both immediate and long term impacts. Michelle Stenner, an experienced QSA from the Solutionary Professional Security Services team, has reviewed the details and prepared this summary of impacts.

Summary of Immediate Impacts

- Assessments beginning after October 1, 2016 will be assessed against PCI DSS version 3.2.
  - PCI SSC clarified many requirements and modified the reporting templates.
  - New requirements are not effective until February 1, 2018; however, Mitigation and Migration Plans should be in place for new requirements no later than October 1, 2016.

Summary of Long Term Impacts

- New requirements in PCI DSS version 3.2 must be implemented on or before February 1, 2018.
  - Seven of the nine new requirements are for service providers only.
  - PCI DSS version 3.2 provides entities with time to design and budget for solutions.

Details of Immediate Impacts

The immediate impact is that all assessments beginning after October 1, 2016 will be assessed against version 3.2. New requirements, however, will not become effective until February 1, 2018. This allows organizations the time to design and implement new compliance measures, as some of them will cost money to implement, making budgeting critical to get these new standards successfully implemented.

There have been three types of changes made to the standards:

- **Clarification changes –** Changes designed to clarify the desired intent of the requirement.
- **Other changes –** Changes designed to offer additional guidance, explanation, definition or instructions to increase understanding of a particular topic.
- **Evolving Requirements –** New requirements designed to ensure the standards are up to date with emerging threats and changes in the market. Some of these apply to service providers only.

Details of Long Term Impacts (Evolving Requirements)

This section focuses on the 12 evolving requirements. Nine of the evolving requirements are new, and of those, seven pertain to service providers only.

Requirement 3.3

Requirement 3.3 is not a new requirement, but the requirement itself has changed somewhat. The requirement is:

> *Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.*

The requirement now specifies the maximum number of digits to be displayed when masked is 10 – the first six and last four. Additionally, this requirement makes it clear that the number of digits displayed should be based on business function. In other words, if a business function does not require the first six digits, those digits should not be displayed. Requirement 3.3 still requires a documented business need and list of roles requiring access to anything more than the first six and last four of the PAN.

Requirement 3.5.1

Requirement 3.5.1 is an additional requirement for **service providers only**. It is a best practice until January 31, 2018, after which it becomes a requirement. The requirement is:

> *Maintain a documented description of the cryptographic architecture that includes:*
>
> - *Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date*
> - *Description of the key usage for each key*
> - *Inventory of any HSMs and other SCDs used for key management.*

The intent of this requirement is to empower the service provider to understand the algorithms, protocols and cryptographic keys used to protect the cardholder data, as well as the devices that generate, use and protect the keys. Requirement 3.5.1 is designed to enable the service provider to detect missing keys or devices and identify unauthorized additions to their cryptographic architecture. Complying with this requirement will also enable service providers to keep pace with evolving threats to their architecture, enabling them to plan for updates.

Requirement 6.4.6

Requirement 6.4.6 is a best practice until January 31, 2018, after which it becomes a requirement. The requirement is:

> *Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.*

This requirement is predicated on the expectation that the organization's change management process be updated to indicate when a change is a significant change. PCI requirements being met, as well as applicable document updates, should both be included.

For example, when the change is adding a new server, some of the PCI requirements would include:

- Making updates to your network diagram
- Ensuring the server is included in the quarterly vulnerability scanning process
- Ensuring it is protected with anti-virus
- Ensuring audit logs are enabled and being saved to a central server
- Ensuring file integrity monitoring is configured
- Updating your asset inventory

Requirement 8.3

Requirement 8.3 has changed, and Requirement 8.3.2 is a rewritten version of Requirement 8.3. The requirements are:

> *8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.*
>
> *8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including [sic] third-party access for support or maintenance) originating from outside the entity's network.*

Requirement 8.3.1

Requirement 8.3.1 is a best practice until January 31, 2018, after which it becomes a requirement. The requirement is:

> *8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.*

This means that even if the system is inside your network, you must now use multi-factor authentication. Multi-factor authentication can be performed either upon authentication to the particular network or to the system component.

Requirement 10.8 and 10.8.1

Requirement 10.8 and 10.8.1 are for **service providers only**. Both requirements are best practices until January 31, 2018, after which they become requirements. The requirements are:

> *10.8 Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of:*
>
> - *Firewalls*
> - *IDS/IPS*
> - *FIM*
> - *Anti-virus*
> - *Physical access controls*

- *Logical access controls*
- *Audit logging mechanisms*
- *Segmentation controls (if used)*

10.8.1 Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include:

- *Restoring security functions*
- *Identifying and documenting the duration (date and time start to end) of the security failure*
- *Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause*
- *Identifying and addressing any security issues that arose during the failure*
- *Performing a risk assessment to determine whether further actions are required as a result of the security failure*
- *Implementing controls to prevent cause of failure from reoccurring*
- *Resuming monitoring of security controls*

The intent of this requirement is to ensure there is a formal process in place to detect and alert when critical security controls fail, and that there is a formal process in place to respond to such failures.

Requirement 11.3.4.1

Requirement 11.3.4.1 is for **service providers only**. It is a best practice until January 31, 2018, after which it becomes a requirement. The requirement is:

> *If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.*

The intent of this requirement is to validate the PCI DSS scope to ensure it is up to date and aligned with changing business objectives.

Requirement 12.4.1

Requirement 12.4.1 is for **service providers only**. It is a best practice until January 31, 2018, after which it becomes a requirement. The requirement is:

> *Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include:*
>
> - *Overall accountability for maintaining PCI DSS compliance*
> - *Defining a charter for a PCI DSS compliance program and communication to executive management*

The intent of this requirement is that Executive Management has visibility into the PCI compliance program, along with the ability to ask questions and drive the effectiveness of the program by influencing priorities.

Requirement 12.11 and 12.11.1

Requirements 12.11 and 12.11.1 are for **service providers only**. They are best practices until January 31 2018, after which they become requirements. The requirements are:

> *12.11 Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes:*
>
> - *Daily log reviews*
> - *Firewall rule-set reviews*
> - *Applying configuration standards to new systems*
> - *Responding to security alerts*
> - *Change management processes*
>
> *12.11.1 Maintain documentation of quarterly review process to include:*
>
> - *Documenting results of the reviews*
> - *Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program*

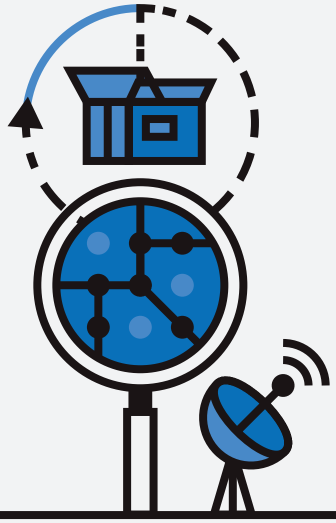
The intent of these requirements is for an independent party to confirm that procedures are being followed as expected, while also ensuring evidence is maintained to assist in the next PCI DSS assessment.

Next Steps

Getting your organization into compliance with PCI DSS version 3.2 may require adding hardware to an organization's environment, necessitating time to budget and purchase the additional equipment. After February 1, 2018, if an organization has not implemented the new requirements, they will be non-compliant.

Organizations should consider contacting their service provider to help ensure that compliance planning is conducted in a manner which maximizes the chances for success.

Solutionary recommends developing a formal plan and beginning work toward getting your organization into compliance with the updated requirements as soon as possible. Compliance with PCI DSS 3.2 is likely to require at least a full budget cycle and some advanced planning.



Summary

Solutionary observed an interesting “flattening” of attacks during Q2 ’16. First of all, the variety of attacks was compressed. In previous quarters, for instance, web application attacks made up as much as 42 percent of the observed attacks. In Q2 ’16, web application attacks made up 24 percent of such attacks, with other types of attacks filling in the gap. The result was that more types of attacks increased in percentage (i.e., attackers made better use of a wider variety of attacks).

Second, the variety of industries being attacked also showed less variability. While there has historically been one or two industries which were clearly more targeted, in Q2 ’16, the top four most attacked industries are all within four percent of each other. This indicates that attackers did not base target selection on industry as much as they have in most quarters.

Third, attack source countries showed more diversity. Again, history has suggested that attacks from a country or two (other than the United States) normally dominate the “source of attack”. In Q2 ’16, the top four attack sources each accounted for between 10 and 15 percent of attacks. It appears that attack sources were also more diverse, as the percentages of attacks from other countries also rose slightly.

The combination of these three observations suggests that during Q2 ’16, attacks may have been more about the technology and exploits than about targeting specific industries. Perhaps that also means more “targets of opportunity” than dedicated “campaigns”.

Along with the technical threat, one of the biggest threats faced by business in Q2 ’16 was related to Business Email Compromise, which is not a technical attack at all, and as such, is often difficult to detect. The attacker motivation for such an attack is clear – monetization of the attack – immediate RoI. Meeting that RoI, however, also requires the attacker to have previously established a significant infrastructure to distribute funds rapidly and effectively.

Ransomware also works best when it has a significant distribution and support infrastructure. Ransomware has evolved throughout the quarter and is expected to evolve and be a threat in the future, especially considering improvements in evasion and resilience techniques.

On a broader scale, analysis of the Chinese Five Year Plan shows strong correlation between Chinese goals and cyberattacks which have been attributed to Chinese resources. The new Five Year Plan most likely provides some insight into where future attacks and threats may lie.

This variety of threats businesses face today has contributed to the release of the new PCI DSS 3.2, which includes some significant updates. Businesses will likely require at least a full budget cycle and advanced planning to successfully implement effective compliance measures.

Ultimately, the changes observed in attack profiles, and what appears to be an emphasis on exploits, is likely simpler than it seems. BEC and ransomware attacks have dominated because they provide a more direct return on investment. There is limited information to sell, as the attacker ultimately gets funds from their victims – direct monetization. Solutionary fully expects this trend to continue. This does not mean, however, we will avoid a return of dedicated campaigns and targeted attacks – all built for long-term gain.

About SERT

The Solutionary Security Engineering Research Team (SERT) protects and informs Solutionary clients through security threat research, vulnerability analysis and the development of effective countermeasures. For more information, including vulnerability disclosures and threat reports, visit the research page on www.solutionary.com, the Solutionary Minds blog or download related whitepapers.

About Solutionary

Solutionary, an NTT Group security company, is the next generation managed security services provider (MSSP), focused on delivering managed 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® MSSP 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, email info@solutionary.com or call 866-333-2133.

ActiveGuard® U.S. Patent Numbers: 7,168,093; 7,424,743; 6,988,208; 7,370,359; 7,673,049; 7,954,159; 8,261,347. Canadian Patent No. 2,436,096. Solutionary, the Solutionary logo, ActiveGuard, the ActiveGuard logo, are registered trademarks or service marks of Solutionary, Inc. or its subsidiaries in the United States. Other marks and brands may be claimed as the property of others. The use of any third-party trademarks or service marks in this report is for reference purposes only, and does not imply any license or endorsement of any third-party products by Solutionary, Inc., nor any license or endorsement of Solutionary, Inc. products or services by any third parties.

The product plans, specifications, and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied.

SOLUTIONARY
AN NTT GROUP SECURITY COMPANY

solutionary.com