Deloitte.

Deloitte
Threat Intelligence
and Analytics

Ransomware
Holding Your Data Hostage

Threat Study

Issue Date: August 12, 2016 | TLP-WHITE[1] | Serial: W-TS-EN-16-00734 | Industry: All

Abstract

Ransomware — *Malware designed to prevent access to a system until a sum of money is paid.*

As cybersecurity threats continue to evolve, ransomware is fast becoming the number one menace. Financial gain is the primary motivation for computer intrusions. Unlike malware that allows criminals to steal valuable data and use it across the digital marketplace, ransomware directly targets the owners of data, holding their computer files hostage until a ransom is paid.

The alarming sophistication of ransomware marks a paradigm shift in the cybercrime ecosystem. Even the most advanced data theft malware has an inherent vulnerability — it must establish a communication channel with its controller to receive commands and exfiltrate the targeted data, and in the process, it generates a signature that can be detected on the network. Ransomware is more stealthy, with some recent variants completing their dirty work without making a single call to the Internet. Other variants attempt to eliminate data recovery options by encrypting additional connected drives and network shares, deleting files and system restoration points, or even remaining dormant until after a backup cycle.

This study will review the history of ransomware; describe common infection vectors and ransomware types; and propose strategies for detection, remediation, and recovery.

Table of Contents

History and Overview

Although ransomware infections have recently become commonplace, the origin of the scheme dates back to the late 1980s. The first ransomware was developed by Dr. Joseph Popp, a biologist with a PhD from Harvard, in 1989 and was dubbed the PC Cyborg Trojan, otherwise known as the AIDS Info Disk Trojan.

The original ransomware was manually distributed via a 5.25-inch floppy disk. Users of the infected computer subsequently became unwitting victims, saving their data to a floppy, along with the PC Cyborg Trojan. Each time users inserted an infected floppy into a new computer, the ransomware infiltrated that machine and the cycle of infection multiplied. Following installation and execution, the ransomware replaced the autoexec.bat file on the victim's computer and tracked each time the machine was booted. Once the boot count reached 90, the ransomware hid all directories and encrypted every file on the victim's C drive, thus rendering the computer completely unusable. To restore functionality, the ransomware demanded payment of $189 to PC Cyborg Corporation at a post office box in Panama (see Figure 1).[3]

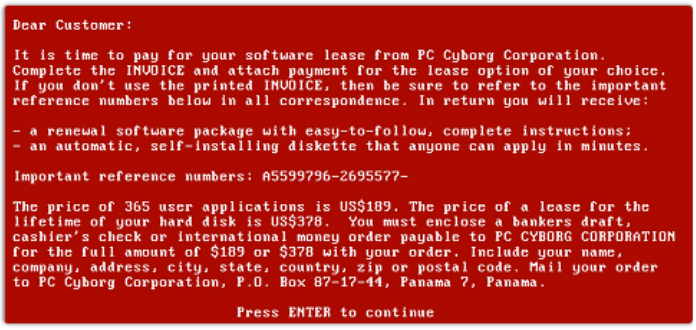
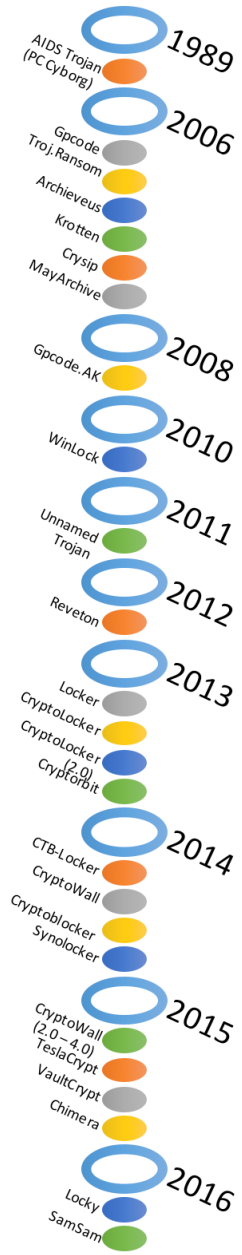


Figure 1. AIDS Info Disk Trojan ransom splash page[4]

Although the PC Cyborg Trojan seems primitive by today's standards, especially its methods of distribution and ransom payment, it generated significant revenue from its victims, thus spearheading the start of the ransomware era. A closer look at the evolution of ransomware is displayed in Figure 2, including the introduction of some notable variants.



1989 – AIDS Trojan (PC Cyborg) becomes the first known ransomware

2006 – Gpcode, TROJ.RANSOM.A, Archiveus, Krotten, Cryzip, and MayArchive. First to utilize RSA encryption algorithms.

2008 – Gpcode.AK. Utilized 1024-bit RSA keys

2010 – WinLock is discovered. Primarily seen in Russia, and would flash porn on the computer screen until the user would make a $10 phone call to a premium-rate telephone number.

2011 – This unnamed ransomware Trojan that was discovered that would lock up the user's computer, and direct the visitor to a fake list of phone numbers which they could call to reactivate their operating system.

2012 – The Reveton ransomware would let the user know their machine has been utilized to download either copyright material or child pornography and would demand the user to pay a fine. This was a form of scareware.

2013 – CryptoLocker, the most notorious ransomware. Had increased encryption, and was extremely difficult to prevent.

2013 – Locker is discovered and would demand a ransom payment of $150 in which the user had 72 hours to pay.

2013 –CryptoLocker 2.0 was released and utilized Tor to increase anonymity for payment.

2013 – Cryptorbit, another ransomware that utilized Tor and would encode the first 1.024 bits of every file it encoded. Cryptorbit would also install a Bitcoin miner on the victim's machine to create more profit.

2014 – CTB-Locker (Curve, Tor, Bitcoin), would leverage elliptical curve cryptography. Tor for anonymity, and Bitcoin for payment.

2014 – CryptoWall, another infamous CryptoLocker clone that was responsible for infecting billions of files worldwide utilizing infected emails.

2014 –Cryptoblocker did not encrypt Windows files that were over 100mb in size. Utilized AES for encryption.

2014 – SynoLocker targeted Synology NAS devices, and would encrypt all files.

2015 – CryptoWall 2.0 used Tor for anonymity and was delivered through multiple attack vectors.

2015 – TeslaCrypt and VaultCrypt originally targeted computers that had certain games installed. Newer variants targeted non-gaming machines.

2015 – CryptoWall 3.0 shared some of the same characteristics as its predecessor but added additional features such as Anti-VM check and was delivered via exploit kits.

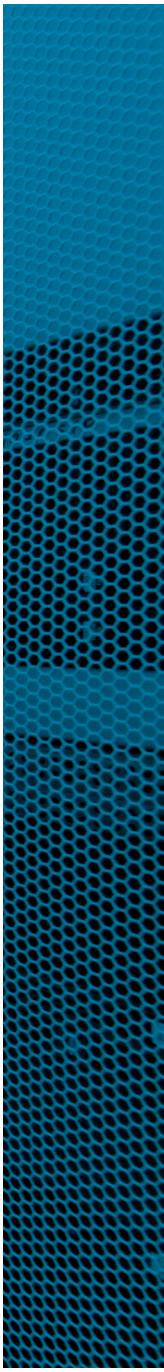
2015 – CryptoWall 4.0 would not only encrypt the data in the files but the file names as well. It also would disable any system restore functionality and shadow volume copies.

2015 –Chimera was more of a scareware ransomware that not only encrypt files but also threatened the user that it would publish them online when ransoms are not paid. Also known as doxing.

2016 – Locky is ransomware that would not only encrypt the user's files, but would first scramble the files and then rename your file extensions to .locky.

2016 – SamSam targets servers instead of end-users. The ransomware exploits vulnerabilities in JBoss application servers and compromises the server to gain shell access. SamSam then proceeds to spread to Windows machines and encrypts their files.

Figure 2. A chronology of notable ransomware development



The chronology in Figure 2 demonstrates the growing sophistication of ransomware, which poses a significant challenge to the enterprise. As complexity expands, the ability to protect and recover from infections diminishes. In 2013, ransomware began to surge from relatively few infections and variants to an exponential growth curve in the number of reported attacks. This trend shows no signs of slowing down. In the first quarter of 2016, an average of more than 4,000 attacks were observed per day — a 300% increase over the 1,000 ransomware attacks observed on average per day in 2015 (see Figure 3).[5]

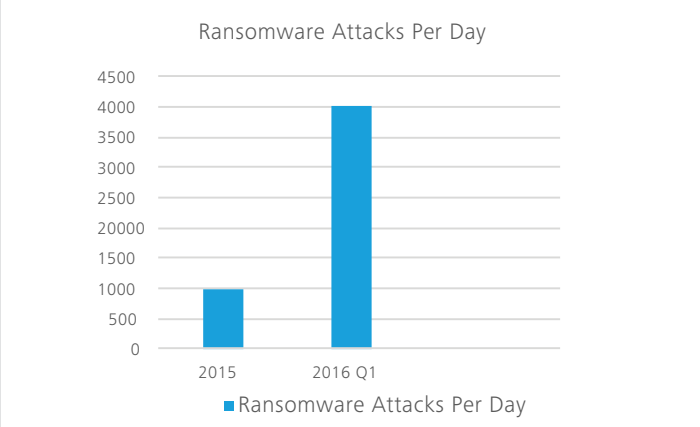


Figure 3. Average number of ransomware attacks per day in Q1 2015 and 2016)

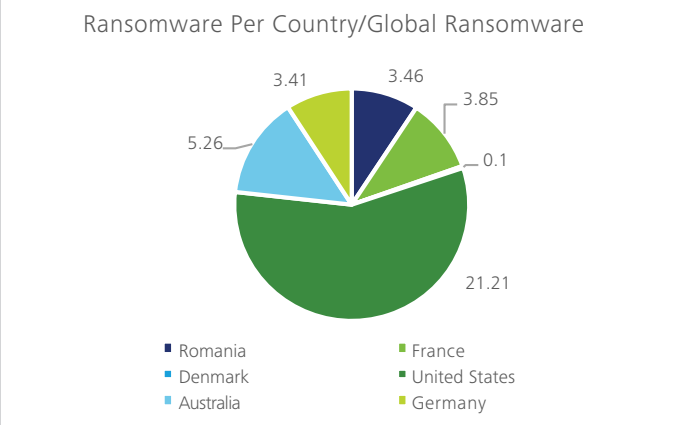


Figure 4 — Ransomware per country

As shown in Figure 4, the United States has the largest ransomware detection rates in the world, indicating criminals have made the United States their top priority, most likely because they consider the United States a highly profitable market. In 2015, creators of the CryptoWall ransomware managed to extort more than $325 million from US victims, according to reports.[6]

Ransomware Types

Ransomware is frequently divided into two different categories: Locker and Crypto.

Locker Ransomware — Locker ransomwar does not encrypt victims' files or data; instead, it is used in a scareware fashion to generate payment. Upon infection, the locker displays a message stating the computer has been commandeered by law enforcement in relation to some sort of crime committed by the user (e.g., viewing of child pornography or pirating of copyrighted materials), and demands the victim pay a fine (ransom) or face criminal charges, additional fines, and/or imprisonment. In many cases, as shown in Figure 5, the user's public IP address, Internet service provider, and geographic location are displayed in the threat and accompanying ransom demand, increasing the credibility of the message to trick the user into paying the ransom.

Figure 5. Example of a locker ransom screen[7]

Crypto Ransomware — Crypto ransomware encrypts victims' files or data using a variety of different cryptography methods, then notifies the victims that their files have been encrypted and demands a ransom to decrypt them (see Figure 6). Deloitte has observed that recent crypto ransomware variants, such as Locky, TeslaCrypt, and Cerber, encrypt the files, the contents within the files, as well as the file names, all without notification. Encryption makes it very difficult for victims to access their data, short of complying with the ransom demands.

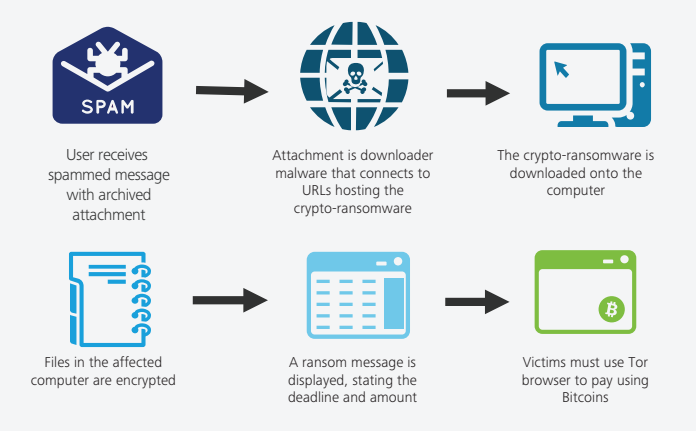


Figure 6. How crypto ransomware works

Motivation

Financial gain appears to be the primary motivation behind ransomware attacks. As attacks becomes more pervasive, the payoffs to criminals also increase, which encourages more criminals to exploit victims using ransomware. One theory behind the increase in attacks is the emergence of the Eurocard/Mastercard/Visa (EMV) payment standard in the United States in 2015, which is largely aimed at decreasing credit card fraud. As adoption of the EMV standard spreads, criminals are trying to find ways to replace the revenue formerly garnered through credit card fraud, and ransomware is one method to fill that void. Another possible theory is that criminals have realized the potential of ransomware as a relatively low risk and easy way to make fast money. In either case, the success of ransomware campaigns is staggering. According to the Federal Bureau of Investigation

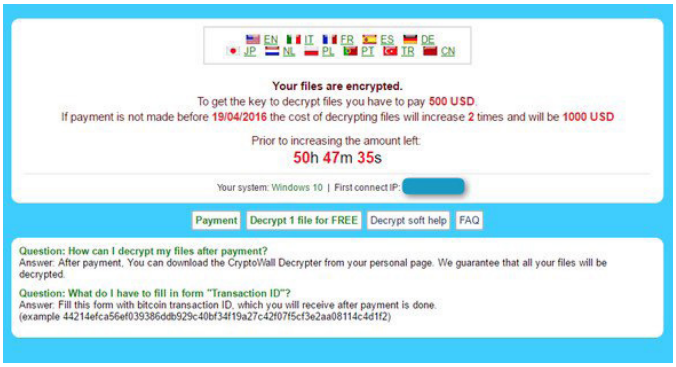


Figure 7. Ransom page with doubling threat[8]

(FBI) Internet Complaint Center (IC3), between April 2014 and June 2015, the IC3 received 992 CryptoWall-related complaints, with victims reporting losses totaling more than $18 million,[9] demonstrating the lucrative power of ransomware.

To maximize ransoms collected from victims, criminals often intimidate them with time-based payment deadlines threatening to double the ransom. In the past, criminals set timers on victims' computers to let them know the deadline on which their data would become unrecoverable. Now, the timer is often set to a deadline on which the ransom will double. This has been very effective for criminals. Victims either remit the ransom right away to avoid paying double or stall in hopes of obtaining some other form of recovery, and after failing to accomplish this, end up paying even more after the initial deadline has expired (see Figure 7).

In both time-based threat scenarios, the criminal's success hinges on the perception that once the ransom is paid the victim's date will be recoverable. The reliability of the payment and recovery mechanism must be perceived as positive, otherwise victims may not even attempt to pay the ransom.

Enablers

There are several enablers that, along with the rapid advancement in capabilities, allow criminals to go to market with a ransomware attack. These enablers are key to the success and growth of ransomware.

Pay-Per-Model Enablers

In the pay-per-install (PPI) business model, the buyer of the PPI service provides a malware stub (the decryptor) to the seller, while contracting him for x-number of ransomware installs. The service provider generates installs as he or she sees fit (e.g., exploit kit, spam). In this model, the buyer does not rent an Exploit Kit (EK) directly. A variation of this model is a pay-per-load service (PPL) in which the stub is cross-loaded onto already infected machines. Both models are advantageous to both criminal PPI buyers and sellers as both parties receive a cut. These models allow unskilled criminals to initiate campaigns because no coding skills are required and everything is already prepackaged for deployment.

Malware Enablers

One business model heavily leveraged by criminals is ransomware as a service (RaaS), which is a basic affiliate program in which the malware author rents or sells prebuilt ransomware for a fee to buyers who set certain paramaters such as ransom fee and payment deadline. The buyers then use whatever methods they desire to infect victims' machines. Any ransom collected from victims is split with the malware author, who gets a 5% to 20% cut, and the buyer who carried out the ransomware attack. This business model is gaining popularity since it keeps the original malware author anonymous and allows the buyer to carry out a ransomware attack with little to no coding skills.

Downloader Enablers

This business model primarily relies on malvertising, which delivers malware through multiple ad networks and exploits system vulnerabilities that are not yet patched. When the infected advertisements hit users, they redirect the page to servers hosting the malware, which includes an exploit kit that attempts to find a back door into the victim's computer where it can install ransomware.

Payment / Cashout Enablers

Payment anonymity is critical to the success of the ransomware scheme. In order to conceal their identities, criminals only accept payments via anonymous means, usually a crypto currency such as Bitcoins. Underground exchange marketplaces offer criminals a variety of ways to turn Bitcoins into cash. Since the life cycle of a Bitcoin payment can be traced through a blockchain ledger, making identification of the cashout node relatively trivial, criminals are starting to leverage tumblers (i.e., laundering) to interrupt the transaction chain and hide the ransom payment trail.

Tumblers, also known as mixers, exchange ransom payment Bitcoins for other Bitcoins with a different history in return for a small transaction fee. For example, Bitcoin A is sent to a tumbler service such as BitLaunder, which then returns Bitcoin B to the recipient in exchange for Bitcoin A, effectively air gapping the two payment chains. Before tumbling their Bitcoins, criminals ensure the mixing services they use operate in jurisdictions outside of reach of US and European law enforcement. Tumbler services are located worldwide and can be found on the Clearnet and deep and dark web (see Figure 8).

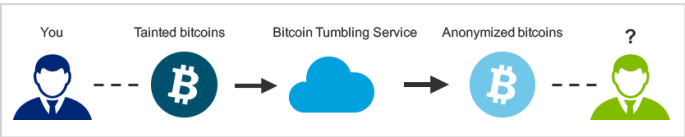


Figure 8. Workflow of a tumbler

To further increase the anonymity of ransom payments, criminals use their own Tor websites to deliver payment instructions, which allows them to control the payment page and stay hidden from law enforcement. A new method called Web-to-Tor is used by victims unable to install a Tor client. A Web-to-Tor gateway allows victims to access the payment server by going to a normal website that translates to the Tor payment site, thus not requiring victims to install a Tor client.

Ransomware Attack Vectors

Spam

Email is a main malware delivery mechanism. Billions[10] of spam emails are sent every day to millions of victims worldwide, and as many as one billion[11] of those spam emails are malicious. Spam is a basic malware delivery technique used by criminals to pass credential stealers, banking trojans, and ransomware on to unsuspecting victims. The goal of the criminals running the networks, botnets, and spam is to indiscriminately spread a threat to as many victims as possible. Using spam botnets such as Bruteres (responsible for delivering Dridex, a financial trojan) or Cutwail, criminals can expect a good rate of distribution for their malware.

Existing spam botnet infrastructures have been in place for several years and are set up to handle high volumes of spam. It is usually up to the spam botnet master to decide to distribute malware through the network or not. Deloitte received 5,340 malicious spam emails in March 2016 for 72 different malware campaigns (see Figure 9), which equates to the receipt of 2.88 different campaigns on average per day, except Saturdays and Sundays, with each campaign containing a different subject line and attachment.

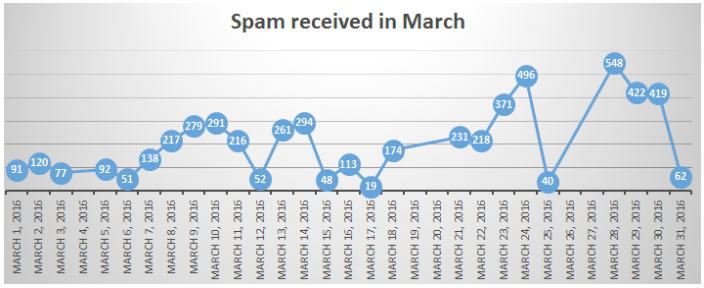


Figure 9. Spam volume received in March 2016[12]

Deloitte noticed that some of the thousands of infected machines used to send the malicious spam were reused, which indicates the strong foothold criminals have on certain networks and machines. It also demonstrates that criminals have so many infected computers standing by that they rarely need to reuse the same machines, which further allows them to evade detection and avoid being added to blacklists and reputation feeds.

Deloitte obtained some infrastructure information about the reused machines and found that each one was in a different country. Although the majority of the reused computers were in Europe, the findings illustrate the wide geographical coverage of the botnet.

Figure 10. Reused IP addresses of the spam botnet (original creation based on our data)

Deloitte's sensors began receiving significant amounts of spam in late November 2015. The spam delivered and installed the TeslaCrypt ransomware through a series of malicious JavaScript attachments that served as downloaders for the ransomware. The spam emails used social engineering techniques to lure victims into opening the attachments, including subject lines that said the victims owed money and/or had a late bill. An untrained eye could easily mistake the emails as legitimate and click on the malicious attachments, which come in a variety of formats, including Word documents, archived JavaScript, and executable files. Other attachments included multiple identical JavaScript, hta files (i.e., an html file with JavaScript code embedded). Spam with malicious attachments is the first stage of the infection chain. Figure 11 provides a screen capture of a spam email.

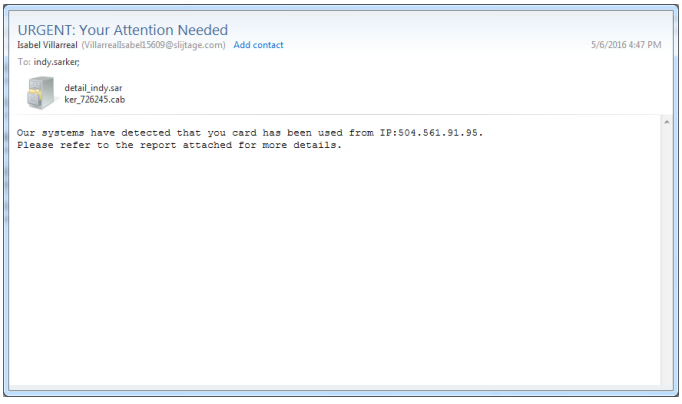


Figure 11. Email sample with zip file containing a JS file attached

Recently, criminals began changing tactics to gain more victims. The pam email illustrated in Figure 12 includes a cabinet file (.cab) attachment, which contains a library of compressed files. Cabinet files are commonly used to copy software programs onto a user's computer. Deloitte tested the cabinet file and discovered criminals used it to compress a malicious JavaScript that downloads Locky ransomware.

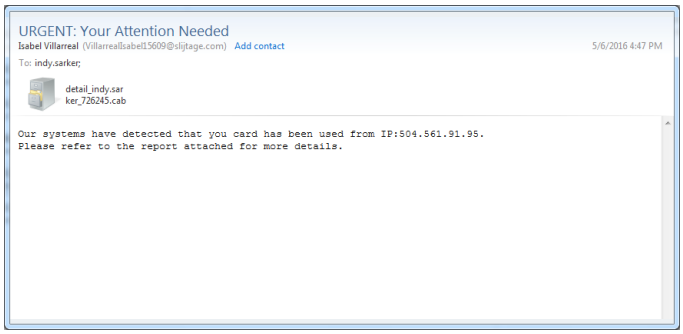


Figure 12. Spam cab file email

Details about the spam emails used to deliver the Locky and Cerber ransomware, including their subject lines, are as follows:

April 28, 2016	Doc0
	Document935
	Fw: Invoice
	Re: Outstanding Account
	Scan0
	file0
April 29, 2016	Attached Doc
	Attached Document
	Attached File
	Attached Image
	Attached Picture
	Re: Outstanding Account
	Second Reminder — Unpaid Invoice
	hi prnt
May 3, 2016	1 Unread Message of High Priority
	Third Reminder — Outstanding Account
	Your New Credit Card Has Been Shipped
	FINAL NOTICE — OUTSTANDING ACCOUNT
May 4, 2016	Alyssa Shields (subject is name in From field)
	Emailing: scan10001
	Re:

These attachments include a JavaScript trojan downloader called Nemucod specially crafted to call back URLs and Internet Protocol (IP) addresses for a malicious payload. The JavaScript in Figure 13 is one of many Deloitte received through spam. The earlier versions of Nemucod contained obfuscated code.

Figure 13. JavaScript file encoded

Once the JavaScript file is decoded, the download URLs are revealed as shown in Figure 14.

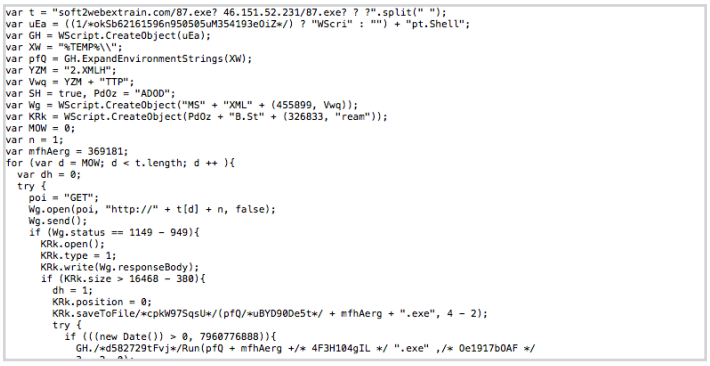


Figure 14. JavaScript file decoded

Criminals were finding the security industry could easily decode the obfuscated JavaScript, thereby discovering the C2 servers and quickly blocking them. The threat actor behind Necumod has updated to increase the level of obfuscation and make the malware a challenge to decode. Over time, Nemucod has become more obfuscated, making it very difficult to decode (see Figure 14)

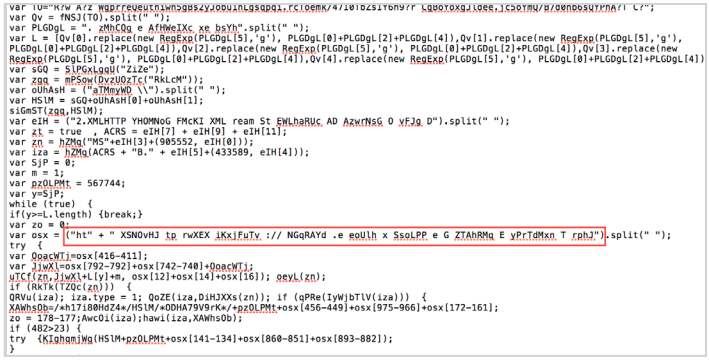
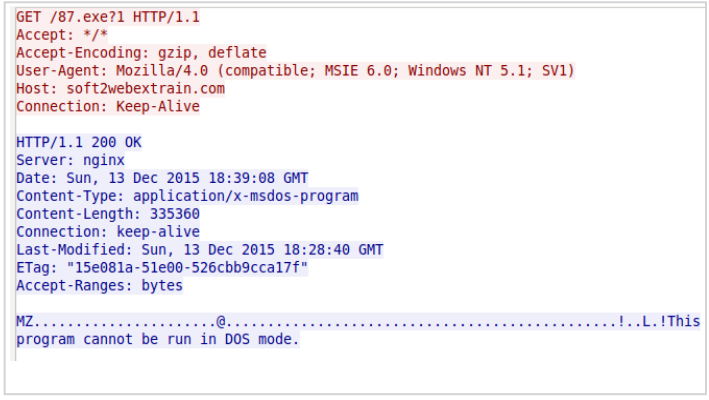


Figure 15

Once the JavaScript is executed, it makes an outbound connection to a remote server to download a malicious file. In this screenshot (see Figure 16), Nemucod downloads TeslaCrypt. The criminals didn't encrypt the network traffic.

Moreover, Deloitte researchers scouted different criminal forums and an advertisement for Nemucod, which is believed to be sold as a service for $20 a build by a threat actor using the handle JSman or Emmett. JSman advertised his services at approximately the same time we observed the first wave of malicious JavaScript spammed.



```
GET /87.exe?1 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: soft2webextrain.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Sun, 13 Dec 2015 18:39:08 GMT
Content-Type: application/x-msdos-program
Content-Length: 335360
Connection: keep-alive
Last-Modified: Sun, 13 Dec 2015 18:28:40 GMT
ETag: "15e081a-51e00-526cbb9cca17f"
Accept-Ranges: bytes

MZ.....................@.....................................!..L.!This
program cannot be run in DOS mode.
```

Figure 16. Nemucod screenshot

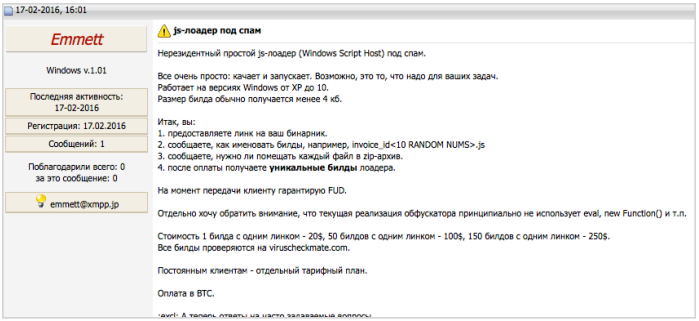


Figure 17. Post for Nemucod malware on criminal forum

Here is a rough translation of the forum post:

Nonresident simple js-loader (Microsoft Windows Script Host) under the spam.

It's very simple: shakes and runs. Perhaps this is what you need for your tasks.

It works on Microsoft Windows versions from XP to 10.

Build size is usually obtained less than four kb.

So you:

1. *Provide a link to your binary*
2. *Inform how to refer to builds, for example, invoice_id <10 RANDOM NUMS> .js*
3. *Inform whether to put each file in a zip file*
4. *After payment, receive unique builds loader*

At the time of transfer to the customer guarantee FUD.

I would also like to note that the current implementation does not use the principle obfuscator eval, new function (), etc.

- *Cost of one build, one link — $20*
- *Cost of 50 builds with one link — $100*
- *Cost of 150 builds with one link — $250.*
- *All builds are tested by viruscheckmate[.]com.*

Regular customers — A separate data plan

Payment in BTC.

Deloitte gathered information about JSman and his online footprint to create the map in Figure 18.

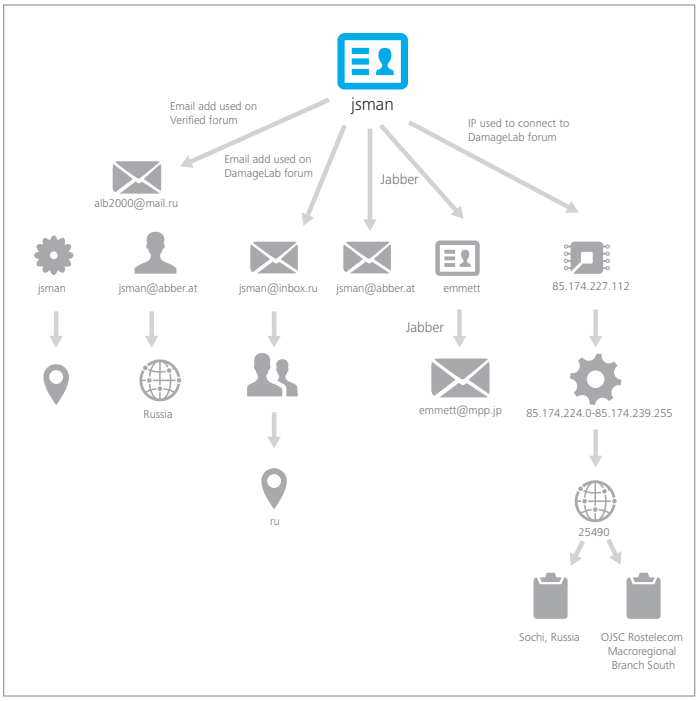


Figure 18. JSman information mapping

JSman used two different email addresses on two different criminal forums, DamageLab and Verified. To log onto DamageLab, he registered using the email address jsman@inbox.ru and the IP address 85.174.227.112, which is located in Russia. Additionally, he used the email address alb2000@mail.ru to register on Verified. The jabber account JSman was used to communicate with other criminals, including emmett@xmpp.jp and jsman@jabber.at. JSman also uses two different Skype linked to his email addresses. The first Skype account states that JSman is linked to the email address alb2000@mail.ru, and **Василий Злобин** (Vasiliy Zlobin) is linked to jsman@inbox.ru. A Facebook and a Mail.ru online profile are linked to the email address alb2000@mail.ru. In both profiles, JSman uses the same name **Альберт Базалеев** (Albert Bazaleev) and mentions that he lives in Sochi, Russia.

Loader

In the latest TeslaCrypt and Locky spam campaigns, criminals used loaders to download their ransomware. A loader is a small malicious program that has one simple task — to download another malware. In certain instances, the loader can have more than one task. Some loaders such as Pony, also known as Fareit, can steal credentials. Deloitte observed that a new loader called Rockloader was used to deliver Locky ransomware, while another loader called Onkonds was used to deliver TeslaCrypt. It is not uncommon for criminals to change their tactics over time.

Deloitte Advisory observed TeslaCrypt being delivered via a malicious Microsoft Word ("Word") file back in December 2015, then switched to the malicious JavaScript Nemucod in January 2016, and then switched to Onkonds in May 2016. Deloitte believes criminals keep the same tactics as long as they work well, but will change tactics when they observe a decrease in infection counts. Deloitte believes criminals have a ratio or threshold they strive to stay above or a golden number of infections. Criminal tactics include a malicious Word file, a malicious JavaScript in an archive file, and a malicious executable in an archive file. Criminals rinse and repeat their tactics.

For instance, Rockloader would first call home at:
Buhjolk[.]at/api/

Then downloads Locky ransomware afterwards at:
Buhjolk[.]at/files/dIseJh.exe

Exploit Kits (EKs)

Criminals not only use Nemucod or Rockloader to download malicious payloads, they also use a variety of techniques to deliver malware. In the case of TeslaCrypt, they often use a JavaScript file or a malicious word document. In some cases, criminals redirect the victims to an exploit kit such as Angler to broaden their attack surface. The Angler EK[13] (known as XXX in the criminal underground) has delivered variants of TeslaCrypt and Locky. Nuclear EK[14], also popular among criminals, has delivered Locky. Angler EK and Nuclear EK are offered as EKs as a service on criminal forums and can be leased for as little as $1,000 per month. These EKs are not only spreading ransomware, but whatever the buyer renting the EK wants, including the usual ransomware variants (e.g., TeslaCrypt, Locky), banking trojans (e.g., Vawtrak, Gozi, Dridex), information stealer and loaders (e.g., Andromeda, Gootkit). On May 3, 2016, Deloitte caught Angler EK spear phishing emails in a spam trap (see Figure 19). These emails appeared to be invoices that attempted to lure victims into clicking on the "view invoice" button. They did not contain any attachments, but rather HTML code.

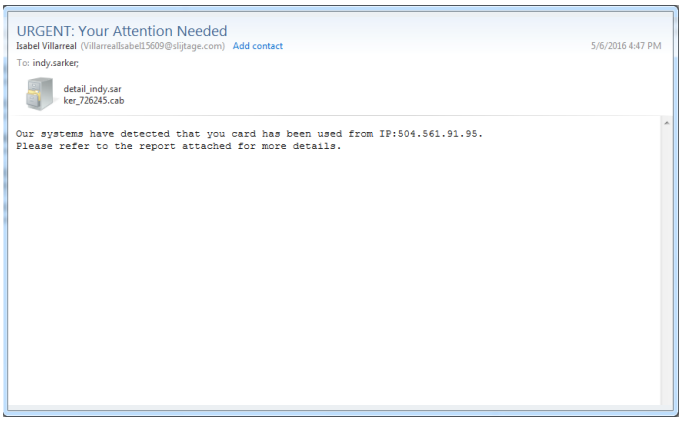


Figure 19

Urlquery[15] has reported the domain wpsupportgroup[.]com as an Angler EK landing page.

JBoss Vulnerabilities

JBoss is an open source application server program developed by RedHat. In March 2015, it was reported that criminals had leveraged vulnerabilities on old versions of JBoss to gain access to networks. Criminals used a tool called JexBoss to indiscriminately test and exploit vulnerable JBoss applications. Once they gained access to a network, they moved lateraly and started installing ransomware on multiple machines. The ransomware involved in these attacks was called Samas or SamSam[16].

Unlike other ransomware, Samas does not beacon to a command and control server. It is completely independent and able to perform encryption without external help. Once the machines are encrypted, a ransom of 1.5 Bitcoins is demanded for each affected computer, and upon payment, a key is sent to decrypt the machines. A hospital[17] in Maryland was recently a victim of this threat. Criminals demanded a ransom of 5 Bitcoins, equal to $18,500, to send the key to decrypt the affected machines.

Remote Desktop Protocol (RDP) Attacks

After criminals leveraged vulnerable JBoss servers, they decided to try another labor intensive attack to gain access to enterprise networks. Criminals spent time scanning servers looking for RDP open ports. RDP was developed by Microsoft to support the remote desktop application available on Microsoft Windows ("Windows"). This application enables users to remotely access another machine. It is often used by system administrators on a local network to perform different tasks on remote machines. RDP can work on a local network but also via the Internet, as long as the service is running. Anyone with the right credentials can gain access to a remote machine through the Internet via the RDP application.

Criminals realized they could perform an RDP brute force attack on servers that have the RDP application running and accessible via the Internet. Once they found a server with RDP running, they would start an RDP brute force attack on user names and passwords, trying multiple combinations until access was granted. Once inside the network, they moved laterally to install the ramsomware.

Targeting and Notable Attacks

Targeting

The typical infection vectors for most contemporary ransomware attacks — spam and EKs — are meant for opportunistic infections, rather than targeted attacks. Criminals behind these campaigns aim to infect as many computers as possible based on the assumption that only a small proportion of victims will pay the ransom. The only targeting in many ransomware campaigns is the tendency of criminals to focus on victims in wealthy, developed countries in general and English-speaking countries in particular. The frequent use of English in ransom notes underscores this focus on English-speaking countries, although many forms of ransomware can also display ransom notes and instructions in a variety of languages, based on victims' IP addresses or the language settings on their computers.

Many ransomware campaigns target certain geographic areas due to language differences or other localized social or cultural factors.[18] For example, a December 2015 CryptoWall spam campaign targeted Scandinavia,[19] while a March 2016 campaign brought the Android ransomware Lockdroid to Japan, its first and only Asian target at that time.[20] Beyond such geographically specific campaigns, many Russian-speaking criminals seek to avoid infecting victims in the former Soviet Union in order to avoid becoming targets of local law enforcement and thus focus on more lucrative Western victims instead. Russian speakers have nonetheless been victims of ransomware too. In fact, the BrLock ransomware family, which was first detected on April 18, 2016, appears to exclusively target Russian speakers.[21]

The list of file formats that ransomware variants encrypt suggests that some developers have envisioned the infection of victims in certain fields, areas, or niche demographics. For example, TeslaCrypt originally targeted online gaming communities when it initially emerged in 2015, and the list of file formats that it encrypted on victims' machines included file extensions specific to various online games.[22] More recently, during the 2016 US tax season, the list of file formats that the emerging PowerWare ransomware encrypted included files created by US tax filing programs, suggesting that the developer envisioned infecting the machines of US taxpayers.[23] Locky ransomware encrypts several file formats for MySQL databases, suggesting an interest in infecting enterprise systems, in addition to infecting the systems of individual users.[24]

Most ransomware families target Windows operating systems due to their enormous market share, although there are several variants that target other operating systems, particularly the widespread Android mobile operating system. For example, the newest Android ransomware family is Dogspectus, which spreads through malvertising redirections to EKs that exploit the Towelroot vulnerability (CVE 2014-3153) in older versions of the Linux kernel. Dogspectus demands a $200 ransom in the form of iTunes gift cards.[25] The choice of gift cards for an Apple platform as a payment mechanism for Android users is an unusual alternative to the more typical use of Bitcoins and remarkable, given the greater market share of Android mobile devices as a competitor to Apple's iPhones. It remains unclear if the Dogspectus developers were Apple enthusiasts or had some reason to direct Android users towards the Apple platform.

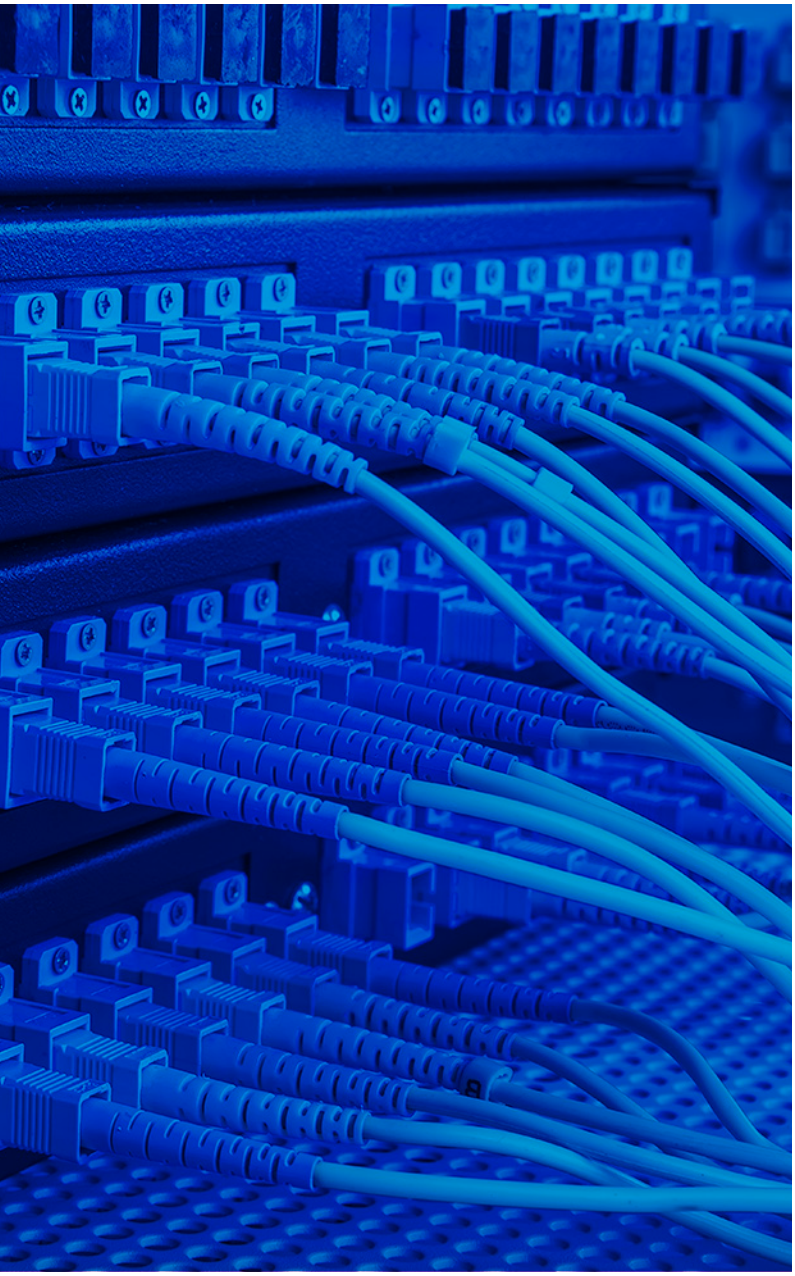
GinX, the first truly malicious crypto ransomware to target the Apple OS X (in addition to Windows) operating system, emerged as an RaaS offering on a dark web marketplace in February 2016. The only two previous ransomwares to target OS X were Mabouia, which a security researcher developed as a proof-of-concept for OS X crypto ransomware, and a law enforcement-themed JavaScript attack that merely interferes with browsers and does not encrypt files.[26] In March 2016, the KeRanger OS X crypto ransomware surfaced in attacks on Apple users. KeRanger can bypass Apple's Gatekeeper protection and bears a valid and signed Apple development certificate.[27]

Other crypto ransomware families have targeted websites and their servers. Linux.Encoder.1, the first ransomware family to target Linux web servers, came to light in November 2015.[28] It encrypted directories for Apache and Nginx web servers and many file formats typical of web applications.[29] A variant of the CTB locker ransomware family (AKA Critroni) emerged in February 2016 and shifted from that family's traditional targeting of personal computers to the targeting of websites. This variant's infection vector was a breach of the affected website. It was unclear what if any basis the criminals had for selecting websites to breach and hold for ransom.[30] Analysis of that variant's Bitcoin transaction history, however, suggests that it made very little money for its developers, perhaps due to the widespread availability of backup services at web hosting companies.[31]

Notable Attacks

Some organizations, such as schools or other local public sector bodies, may be more susceptible to ransomware than others due to limited security resources, substandard security practices, or obsolete infrastructure and software. Several hospitals in North America and Europe[32] were victims of a series of ransomware attacks in early 2016, most notably, the Locky ransomware infestation of the networks at the Hollywood Presbyterian Medical Center,[33] which reportedly paid $17,000 to regain access to its files. Another Locky infection occurred at Methodist Hospital in Henderson, Kentucky, in March 2016.[34] The number of publicly reported ransomware attacks on hospitals in such a short period of time has fueled fears that ransomware developers have targeted hospitals, perhaps in order to exploit the time-sensitivity and often life-or-death consequences of hospital operations as a way to pressure victims into paying the ransom.

The SamSam ransomware family, which originally came to light in connection with a series of health care ransomware incidents, provides the clearest example of ransomware targeted at attacking a specific industry — the health care vertical.[35] Its infection vector is the exploitation of vulnerable servers, instead of spam or EKs. The SamSam developers conducted lateral



movement, network reconnaissance, and other elements of the first reported SamSam attack manually, in contrast to the usual automation of most ransomware attacks.[36] Incidents involving SamSam have included the March 2016 attack on the MedStar Health network of hospitals in the Washington, DC, and Maryland areas.[37]

Additionally, a Canadian hospital may have been the target of a March 2016 watering hole attack or strategic web compromise. The website of the Norfolk General Hospital in Ontario, Canada, redirected visitors to the Angler EK, which tried to infect their computers with TeslaCrypt ransomware payloads. The criminals compromised the website by exploiting a vulnerability in an older version of the Joomla content management system (CMS)[38] in the hopes that an employee at the hospital would visit the website from a vulnerable computer on that hospital's network. The PowerWare ransomware also came to light in an unsuccessful March 2016 attack on a health care organization, although it is unclear to what, if any, extent the criminals may or may not have specifically targeted the health care vertical.[39] It is possible that the ransomware attacks on hospitals may reflect factors other than specific targeting of the health care vertical, such as the use of obsolete operating systems for medical devices and the preference of some health care practitioners for convenience over security.

The energy and utilities sector may also provide ransomware operators with attractive targets due to the critical infrastructure operated by companies in this industry and the potentially high physical impact of utility outages. On April 25, 2016, ransomware infected the corporate network of the Board of Water & Light (BWL) in Lansing, Michigan. It remains unclear what crypto ransomware family was involved, although the unspecified ransomware moved laterally throughout BWL's corporate network and into its customer call center and line outage map. BWL shut down its corporate network and phone services in response to this lateral movement. The ransomware did not spread further into BWL's water or electricity systems due to their separation. It is unclear whether this incident was a targeted attack, although the infection vector was a phishing email that a BWL employee opened.[40]

In January 2016, another unidentified form of crypto ransomware also displayed lateral movement capabilities when it infected the networks of the Israeli Electric Authority, a public sector body that regulates and oversees Israeli utilities. Similar to BWL, the Israeli Electric Authority also shut down its networks in response to the ransomware's lateral movement, and a phishing email was the infection vector for this incident as well.[41]

Prevention

Courses of Action and Remediation

Detection Is a Losing Proposition — Unlike other malware threats, detective controls may not be as effective in identifying and stopping ransomware before its effects are realized. This is due to the way ransomware works to achieve its aims. For example, trojans, remote-access toolkits, or other similar threats rely upon observable activity in order to facilitate their goals. This activity involves regular over-the-network communication to a command-and-control infrastructure in order to receive commands, execute infiltration tasks, or exfiltrate data. Much of the ransomware observed by Deloitte threat intelligence analysts, however, follows an entirely different playbook. In fact, many ransomware kits communicate only once, if at all, usually during or immediately after infection to obtain or transmit data necessary to carry out their encryption operations and present ransom demands.

Consequently, a detective measure such as an intrusion detection system (IDS) or other similar detective device that notifies a security operations team of a threat is not going to stop ransomware. At a minimum, a detective device would be superfluous as an Security Operations Center (SOC) would receive notification from the security controls, as well as from users complaining that they received a ransom popup on their computers. At this point, the damage has already been done (i.e., files encrypted on an endpoint, server, or network share). This is counterintuitive to everything the marketplace has said for years — that the proper cybersecurity focus should be on detective controls because it is not possible to stop every threat. In the case of ransomware (and other destructive malware kits), preventative controls are at least as important as detective capabilities.

So which preventative controls should an enterprise focus on in order to stop ransomware? To get the answer to this question, one has to look at the attack vectors.

Attack Vector #1 — Spam

As with so many other threats, the same old tired story applies here: one of the most prevalent vectors of attack for recent ransomware campaigns has been spam. As with other email threats, there is no single magic bullet to stop this threat. The most effective course of action to blocking inbound ransomware and its associated downloader components is going to be a cocktail or blend of approaches.

Attachment Scanning and Filtering — For attachment scanning and filtering to work effectively, email controls should be able to identify files based on their actual file type, not via a purported extension or other naming convention. Additionally, inbound emails containing attachments should be scanned and filtered as needed, at scale, on demand, and across all inbound email vectors.

- If the enterprise is not doing so already, it should drop natively executable file attachments such as .exe, .scr, and others prior to delivery to user inboxes.
- File archives (e.g., zip/rar and others) containing files such as JavaScript, visual basic scripts, and executable types (e.g., .exe, .src) should also be dropped prior to delivery to user inboxes.
  - In 2013, during the height of the Cryptolocker campaigns, this control approach reduced the infection rate for a top-five financial services company by more than 90% overnight.
- Mileage may vary when it comes to scanning attachments using an inline antivirus control due to regular changes introduced to attachments and malware that obfuscate their purpose.
  - It is strongly recommended that an antimalware behavioral control that sits inline in the email channel and can deliver or block based on the results of a behavioral analysis be used instead of or in conjunction with simple inline antivirus controls.
  - Sometimes this can be achieved by simply copying all suspect emails into a central location, stripping attachments off into a directory, running the attachments through a simple analysis (e.g., scripted file identification and email metadata cataloging), and then going back to users' inboxes and removing all offending emails; thus, expensive and elaborate hardware-based solutions are not always the answer and may be overkill.

Content Filtering — Deloitte Advisory has observed the unique features of spam-bots used to deliver various ransomware attacks, and an increase in spam filter thresholds is recommended too so that messages from suspected spamming hosts get dropped or quarantined appropriately.

- Third-party reputation services implementing DMARC, email filtering, spam-scoring, and other similar technologies can decrease the likelihood of spam delivery.
- Tuning keyword controls for spam may or may not be effective and are dependent on several variables in spam campaigns that deliver ransomware, which have been observed to change as many as two to three times per day. Effectiveness in this approach is completely dependent on early detection and identification of spam-run themes, the ability to rapidly adjust these controls (within minutes in some cases), and the human resources available to perform analysis.
  - Some identification rules should be developed and eventually turned into automation controls to aid analysts, such as whether email with the same subject line is being delivered to dozens of users or whether the attachment name present in <threshold #> emails can speed results and reduce the time between detection and implementation.
  - External threat data feeds containing this information can be leveraged as well using an Indicator of Compromise (IOC)-funnel approach to feed threat data directly into any email content filtering system

User Education and Training — Even after acquiring, deploying, tuning, analyzing, and blocking spam across communications channels, some spam will still leak through, which prevention is ultimately in the hands of end users; thus, user education to prevent the spread of ransomware via spam is essential.

- While most information security training programs contain guidance on the identification of spam, including how to spot and report it, this information should be reinforced in practice.
- Training programs that include highly customizable simulation and response components are more effective than simply walking users through slides and telling them what to do.

Attack Vector #2 — Drive-By Web Exploit

EKs are another popular vector used by criminals to distribute ransomware. Traffic redirection through malvertising, compromised Wordpress installs, and other means drive user web browsing toward EKs that deliver ransomware. Similar to email channel controls, there is no single control in an enterprise outbound web channel that will solve the ransomware threat; thus, a mix of controls is required.

Content Filtering — Whether deployed as a transparent proxy, via Domain Name Service (DNS) controls, or through an inline-proxy system, web reputation content filtering should be enhanced in several different ways:

- Addition of ransomware-specific threat data feeds into web-content filters through IOC-funnel mechanisms to not only block active infections, but prevent infections from obtaining the data needed to complete file encryption.
- Deployment of inline behavioral controls to detect and block EK activity by analyzing the results of web sessions, notifying security of suspicious activities, and blocking communications to EKs.

Intrusion Prevention Systems — Verify intrusion prevention systems are automatically and frequently updated with the latest signature sets and configured to actively block EK activity. Intrustion Preventions Systems (IPSs) should be used in the outbound web channel to prevent EK delivery of ransomware to victim machines.

- This control can also actively block communications used by ransomware installs, as well as command-and-control and reverse-proxy systems used as channels by ransomware.
- Data harvested from alerts, such as, but not limited to, domains, URL patterns, IP addresses, and binary hashes, can be reused and fed into other controls via IOC-funnel automation.

Most content-filtering solutions can block uncategorized websites. Although turning this feature on may lead to a mountain of work or significantly affect the business, it is important for enterprises to rationalize this decision appropriately and adopt strategies and technologies that aid in understanding the threats associated with gray websites, including newbie analysis in which the age of the domain is taken into consideration. Consideration of other factors, such as the reputation of associated domains or related or concurrent domains, should also drive decisioning around uncategorized websites.

While all of these content controls sound sophisticated and have great potential to address the ransomware threat delivered through the web channel, none of these controls will work if the communication between the victim computer and EK, reverse-proxy, or command-and-control channel, is encrypted. To provide visibility into controls like IPS, SSL-interception is required. Some inline content filtering solutions provide this capability out of the box, but care should be taken during control deployment or tuning so the implementation of features like SSL-interception do not negatively affect performance to the point where the channel is rendered unusable.

Attack Vector #3 — Vulnerability Exploit via JBoss and Secondary Web Shell

Detective security controls may prove more effective than preventative measures with regards to this vector. While it has been widely reported that SamSam ransomware was delivered via compromised systems running vulnerable versions of software like JBoss Enterprise Application Platform (EAP), the two topics (i.e., SamSam and JBoss vulnerabilities) are, at best, tangentially linked in that the JBoss vulnerability could be leveraged for a number of purposes beyond the installation of SamSam or other ransomware. In any case, servers may be compromised through vulnerabilities present in JBoss management consoles (i.e., jmx-console), web shells, remote-access toolkits, and other installed tools, allowing attackers to execute a number of secondary attacks, including ransomware attacks. Control tuning and deployment should, at a minimum, encompass the following:

Intrusion Detection and Prevention Systems — Deployment and activation of relevant signatures, particularly those related to JBoss console access attempts, is recommended. Mature sets of JBoss-related signatures are available for both Snort and TippingPoint products.

- Security Event & Incident Monitoring (SEIM) correlation rules based on solid asset information that correctly prioritize events related to this vulnerability and reduce or prevent the effects of ransomware delivered via this vector.

Hardening of JBoss Server Deployments — Lock down TCP/8080 using IPtables or another firewall technology so that only authorized connections to the management console can be made. It goes without saying that patching vulnerable systems is paramount here; however, this is no small task if the applications written for the server are version dependent and becomes even more challenging if an application or system itself is a third-party product. In any case, the following steps should be pursued:

- Assess all server environments for use of Java and track in asset and vulnerability management systems as appropriate.
- Scan for open management ports and lock down as appropriate (account for load-balancers, translated ports, and IP addresses).
- Many JBoss vulnerabilities are related to Java data serialization; therefore, the use cases for these should be understood within applications and those use-cases should be whitelisted, while all the rest should be denied.

Deployment of Reliable and Up-to-Date Server Antivirus — This is always recommended, even on Linux-based servers, and especially if they are Internet-facing. The JBoss vulnerability is a great example of software that can be left intentionally out-of-date to accommodate business requirements, but leaving the server without antivirus protection is tantamount to putting your valuables in the front yard with a sign that says "first come, first served."

- The addition of host-based tools, such as file-integrity monitoring and endpoint detection and response suites, can assist in the detection of compromise. Some tools, if properly configured, can block the execution of ransomware binaries loaded through a web shell or other means.
- These host-based suites can also be utilized as a detection mechanism, which may be more applicable to the server-compromise attack vector for ransomware.

Common Control Surface Strategies and Ransomware

Desktop Patching — While many enterprises are able to effectively and rapidly patch desktop operating system components, this is not always the case for third-party software packages.

- Patching becomes especially critical for third-party software packages since software, such as Java and Flash, is frequently targeted by EKs that have been observed delivering ransomware.

Desktop Antivirus — The "antivirus is dead" argument can be made as often as needed, but Deloitte rarely sees an enterprise without this table-stakes component as part of its security controls suite. Given the destructive potential of ransomware, tools like antivirus software should not be discounted.

- The key is minimizing issues like orphaned installs and out-of-date signatures on endpoints to the extent possible and addressing alerts associated with these conditions.

Micro-Sandboxing and Application Sandboxing Technologies — Per-process isolation can prevent an endpoint from becoming victimized by ransomware either by preventing the exploitation of a system via the attack vector, or by isolating a process like ransomware and preventing its effects across an infected system. While these technologies can be tax system performance and in some cases may require a high level of "touch" associated with configuration and management, they should be prioritized for deployment as needed, especially to critical users and systems.

Additional Considerations

Resiliency Options — Disaster recovery programs need to incorporate the threat of large-scale data loss due to ransomware into their planning and recovery procedures. Since many variants of this threat can encrypt data located on file shares, mapped drives, and drop-box folders, the need for data backups is heightened as the ransomware threat can appear in multiple ways and via different vectors.

Attack Vector #3 — Vulnerability Exploit via JBoss and Secondary Web Shell (cont.)

- Data storage and local retention policies should be reinforced for end users so that the only a single copy of data and work product is not residing exclusively on an endpoint.
- Many enterprises do not rely on endpoint-specific data backups and instead back up shared data storage systems. While this works great for users in the office, connected to the local network all the time, highly mobile users may not benefit or be able to comply with data storage policies all the time. Data backups for these endpoints should be considered.
- It is critical that good backups remain good; that is, that they are not corrupted by normal backup procedures overwriting good data with ransomed data. Many enterprises only keep a one-week rolling full-to-incremental backup set, refreshing a full backup over the weekend across the same media from the prior week, then performing incremental backups during the week, only to repeat this process again at the end of the following week. Depending on the timing of the attack, this procedure could wipe out any good data before ransomware is detected. A multistage data backup strategy should be employed in which several backup sets are used so that Friday's data is not replaced over the weekend with ransomed data.
- IT operations and resiliency programs related to data backups are crucial. In many cases, the only safe copy of data may be the previous night's backup. This is especially true for data file shares, enterprise file sharing, drop-box systems, and other user-accessible data stores. Near-line and offline data stores and backups should be tested regularly to ensure recoverability.

Communication — Communication within an enterprise is critical so that the threat of ransomware is consistently and predictably addressed. Communication plans should be developed to address:

- Outages caused by ransomware, including media and public relations communications policies.
- User training that includes not only what to do during a ransomware event, but also what not to do, who to communicate with, and how to address the impact appropriately.
- Additional security policy training regarding data handling procedures and threat recognition.
- Identification of key third parties and groups that can aid in recovery, such as law enforcement.
- Internal communications during and after recovery.

A Note About Recovery

Recovery from ransomware damage is dependent on a number of factors, including, but not limited to:

- Criticality of data lost
- Availability of data backups
- Impact scope of the infection / encryption
- Ability to pay the ransom, if required
- Coverage scope of cyberinsurance or other similar instruments

Questions related to these factors must be answered by an organization in order to ascertain what needs to be done in the event of a ransomware attack. Knowing the state of the last backup set, for example, will provide situational awareness and drive good decisions around how to react and recover when facing this threat. External threat intelligence regarding ransomware, such as vulnerability awareness, is also useful and can help guide decisions. Other questions to consider include:

- Has an impact assessment of the data loss been performed?
- Does any copy of the affected data exist in any form elsewhere, even an out-of-date copy?
- What is the estimated time to recover?
- Have other systems and entry points into the enterprise been examined for compromise?
- Does the organization have the means to acquire payment methods like Bitcoin?
- Does the enterprise maintain a data forensics retainer with incident-response specialists capable of analyzing the origin and scope of the incident?
- Does the organization's cyberinsurance cover losses incurred from ransomware?

Various interested groups, security researchers, law enforcement, software vendors, and others, were able to mitigate, break, and eventually render various ransomware kits useless in the past by providing decryption services, creating and making publicly available all permutations of the kit's encryption keys, and/or exploiting various weaknesses in the encryption schemes or key-handling mechanisms to recover or brute-force encryption. While these opportunistic remedies have helped many victims, they have also (as a byproduct) aided the development of ransomware capabilities.

With this in mind, all of the security challenges addressed by advanced encryption (which are often incorporated into modern advanced

Attack Vector #3 — Vulnerability Exploit via JBoss and Secondary Web Shell (cont.)

ransomware) become liabilities to victims when they suffer a ransomware event. Since encryption technologies are designed to ensure data is not recoverable by unauthorized parties, the option of last resort for recovery is, unfortunately, paying the ransom.

It is critical for enterprises to understand that paying the ransom, while not ideal, may be the only option if controls have failed, if data is not recoverable, and if business operations cannot continue without the recovery of the affected data or systems. It is also important to note that paying the ransom is no guarantee that data will be recovered. While it is in the best interest of criminals to ensure that data is recoverable, sometimes it is not. Ransomware does not come with a warranty or any kind of service-level agreement. Technical failures may occur that prevent successful recovery, and criminals will not provide a money-back guarantee if data decryption fails.

Obviously, paying a ransom may make oneself or an organization the target of future attacks; therefore, paying a ransom should be considered only as a last resort and should be undertaken only after all other recovery options have been exhausted. Additionally, reasonable measures should be taken so that the enterprise does not immediately become subject to additional criminal activity subsequent to ransom payment. To accomplish this, an enterprise should establish that other systems and data stores are not affected, that other backdoors do not exist, and that users are not silently suffering because they are too embarrassed to let administrators know they "did something wrong." Additionally, engaging a third-party incident response organization that has experience dealing with the criminals, the threat, and the recovery steps, is highly recommended if the payment path is chosen as this kind of company can aid in obtaining the proper payment means in the correct nonattributable way, executing the payment in a way that avoids embarrassment or reputational damage, acts as an intermediary between the enterprise and the criminal, and ensures that the steps needed to recover post-payment are well understood, planned, and executed appropriately.

Conclusion

This threat study represents a thorough analysis of ransomware, including some of the well-known variants, evolution, vectors, notable attacks, and how to prevent an organization from becoming the next victim. From Deloitte's analysis, it is clearly evident that ransomware will grow in sophistication and become more widespread as it continues to plague individual users, as well as the enterprise. The successes thus far in the extortion of money from victims is paving the way for more cybercriminals to utilize ransomware as their main tactic. Deloitte Advisory hopes that by leveraging this study, your organization will be armed with the necessary knowledge and tools to protect your environment.

References

[1] TLP: WHITE information is subject to standard copyright rules, and may be distributed freely, without restriction

[2] L. Abrams, "Emsisoft releases Decrypter for the LeChiffre Ransomware," Bleeping Computer, 25 January 2016 [Online]. Available: http://www.bleepingcomputer.com/news/security/emsisoft-releases-decrypter-for-the-lechiffre-ransomware/. [Accessed April 29, 2016 [Online].

[3] K. Laffan, "A brief history on ransomware," Varonis Bolog, November 10, 2015 [Online]. Available: https://blog.varonis.com/a-brief-history-of-ransomware/. [Accessed April 28, 2016].

[4] nakedsecurity.sophos.com

[5] K. Wagstaff, "Big Paydays Force Hospitals to Prepare for Ransomware Attacks,"NBC News, April 23, 2016 [Online]. Available: http://fedscoop.com/ransomware-attacks-up-300-percent-in-first-quarter-of-2016/. [Accessed April 30 2016].

[6] Admin, "2015 — The year of the Ransomware," Apps & Tech, News, December 17, 2015 [Online]. Available: http://www.impulsegamer.com/2015-the-year-of-the-ransomware-plague/. [Accessed 20 May 2016].

[7] http://www.pcworld.com/article/2084002/how-to-rescue-your-pc-from-ransomware.html&bvm=bv.122448493,d.cWw&psig=AFQjCNEAedCov_LnVax_qbq4qUOp-K2BGQ&ust=1463827853401384

[8] http://www.tripwire.com/state-of-security/latest-security-news/decryption-tool-released-for-cryptxxx-ransomware/&psig=AFQjCNHyZGkP2n6u-RC7ou0j7nxmi4tYwA&ust=1463841392018232

[9] FBI IC3, "criminals continue to defraud and extort funds from victims using cryptowall ransomware schemes," Alert # I-062315-PSA, June 23, 2015 [Online]. Available: https://www.ic3.gov/media/2015/150623.aspx/. [Accessed April 28, 2016].

[10] Email Statistics Report, 2015-2019 Executive Summary: http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf

[11] One Billion Malicious Spam Emails Sent Globally Every Day: http://www.spamfighter.com/News-19626-One-Billion-Malicious-Spam-Emails-Sent-Globally-Every-Day.htm

[12] Deloitte Development LLC

[13] Angler exploit kit pushes new variant of ransomware: https://isc.sans.edu/forums/diary/Angler+exploit+kit+pushes+new+variant+of+ransomware/19681

[14] Locky Ransomware Installed Through Nuclear EK: http://researchcenter.paloaltonetworks.com/2016/03/locky-ransomware-installed-through-nuclear-ek/

[15] http://urlquery.net/report.php?id=1462426892216

[16] The doctor will see you, after he pays the ransom: http://blog.talosintel.com/2016/03/samsam-ransomware.html

[17] Maryland hospital group hit by ransomware launched from within : http://arstechnica.com/security/2016/03/maryland-hospital-group-hit-by-ransomware/

[18] C. Wisniewski, "Location-based threats: How cybercriminals target you based on where you live," Sophos, 3 May 2016 [Online]. Available: https://blogs.sophos.com/2016/05/03/location-based-ransomware-threat-research/. [Accessed May 3, 2016].

[19] Staff, "Cryptolocker new spam campaign targeting Scandinavia," Deloitte, December 22, 2015 [Online]. G-TN-EN-15-00347.

[20] Staff, "Android.Lockdroid ransomware targeting Japan," Deloitte, April 1, 2016 [Online]. G-TN-EN-16-00231.

[21] Staff, "Ransomware Explosion Continues: CryptFlle2, BrLock and MM Locker Discovered," ProofPoint, April 27, 2016 [Online]. Available: https://www.proofpoint.com/us/threat-insight/post/ransomware-explosion-continues-cryptflle2-brlock-mm-locker-discovered. [Accessed April 28, 2016].

References (cont.)

[22] C. Boyd, "TeslaCrypt: Video game Safety 101," Malwarebytes, April 20, 2015 [Online]. Available: https://blog.malwarebytes.org/cybercrime/2015/04/teslacrypt-videogame-safety-101/. [Accessed April 19, 2016].

[23] Staff, "Tax Day Extortion: PowerWare Crypto-ransomware Targets Tax Files," Trend Micro, March 31, 2016 [Online]. Available: http://blog.trendmicro.com/trendlabs-security-intelligence/tax-day-extortion-powerware-crypto-ransomware-targets-tax-files/. [Accessed April 19, 2016].

[24] F. Sinitsyn, "Locky: the encryptor taking the world by storm," SecureList, April 6, 2016 [Online]. Available: https://securelist.com/blog/research/74398/locky-the-encryptor-taking-the-world-by-storm/. [Accessed April 19, 2016].

[25] Staff, "New Android ransomware Dogspectus," Deloitte, April 27, 2016 [Online]. G-TN-EN-16-00298.

[26] Staff, "GinX ransomware-as-a-service attacks OS X and Windows operating systems," Deloitte, February 11, 2016 [Online]. G-TN-EN-16-00108.

[27] Staff, "KeRanger ransomware targets OS X, found in legitimate software," Deloitte, March 8, 2016 [Online]. G-TN-EN-16-00164.

[28] Staff, "Encryption ransomware threatens Linux users," Dr. WEB, November 6, 2015 [Online]. Available: https://news.drweb.com/show/?i=9686&lng=en. [Accessed 28 April 2016].

[29] Staff, "Linux.Encoder.1," Dr. WEB, November 6, 2015 [Online]. Available: http://vms.drweb.com/virus/?i=7704004&lng=en.

[30] Staff, "New variant of CTB-Locker targeting websites," Deloitte, February 24, 2016 [Online]. G-TN-EN-16-00140.

[31] D. Sinegubko, "Website Ransomware — CTB-Locker Goes Blockchain, Sucuri, April 12, 2016 [Online]. Available: https://blog.sucuri.net/2016/04/website-ransomware-ctb-locker-goes-blockchain.html. [Accessed April 28, 2016].

[32] Staff, "Four European hospitals targeted by malware attacks, healthcare ransomware incidents on the rise," Deloitte, February 22, 2016 [Online]. G-TN-EN-16-00126.

[33] Staff, "California hospital suffers ransomware attack, networks remain offline," Deloitte, February 16, 2016 [Online]. G-TN-EN-16-00114.

[34] Staff, "Kentucky's Methodist Hospital suffers ransomware attack," Deloitte, March 24, 2016 [Online]. G-TN-EN-16-00202.

[35] N. Biasini, "The Doctor will see you, after he pays the ransom," Cisco Talos, March 23, 2016 [Online]. Available: http://blog.talosintel.com/2016/03/samsam-ransomware.html. [Accessed April 19, 2016].

[36] Staff, "Targeted attack using SamSam ransomware," Deloitte, March 1, 2016 [Online]. G-TN-EN-16-00154.

[37] Staff, "MedStar Health infection confirmed as Samsam ransomware, Deloitte, March 31, 2016 [Online]. G-TN-EN-16-00224.

[38] Staff, "Compromised hospital website serving TeslaCrypt ransomware," Deloitte, March 22, 2016 [Online]. G-TN-EN-16-00197.

[39] M. Sconzo, "Threat Alert: "PowerWare," New Ransomware Written in PowerShell, Targets Organizations via Microsoft Word," Carbon Black, March 25, 2016 [Online]. Available: https://www.carbonblack.com/2016/03/25/threat-alert-powerware-new-ransomware-written-in-powershell-targets-organizations-via-microsoft-word/. [Accessed April 19, 2016].

[40] Staff, "Ransomware infects Michigan utility company's network," Deloitte, April 27, 2016 [Online]. G-TN-EN-16-00300.

[41] D. Storm, "No, Israel's power grid wasn't hacked, but ransomware hit Israel's Electric Authority," Computerworld, January 27 2016 [Online]. Available: http://www.computerworld.com/article/3026609/security/no-israels-power-grid-wasnt-hacked-but-ransomware-hit-israels-electric-authority.html. [Accessed April 28, 2016].

About Deloitte's Threat Studies

These studies are the result of detailed research conducted by our Threat Analysis & Research (TAR) team on an ongoing threat or emerging threat trend, typically focusing on a specific threat actor or a specific technical issue that is persistent over time. It contains detailed information on adversary TTPs and IOCs.

About Deloitte's Threat Analysis & Research

TAR is delivered as an annual subscription service that provides client-specific threat insights and business impact through collection & analysis of data across numerous sources of information including darkweb, criminal forums, third-party intelligence or other sources. Our professionals have advanced language skills and regional knowledge, and extensive intelligence experience from law enforcement, government, military, and cyber intelligence companies.

Secure.Vigilant.Resilient.™

To grow, streamline and innovate, many organizations have difficulty keeping pace with the evolution of cyber threats. The traditional discipline of IT security, isolated from a more comprehensive risk-based approach, may no longer be enough to protect you. Through the lens of what's most important to your organization, you must invest in cost-justified security controls to protect your most important assets, and focus equal or greater effort on gaining more insight into threats, and responding more effectively to reduce their impact. A *Secure.Vigilant. Resilient.* cyber risk program can help you become more confident in your ability to reap the value of your strategic investments.

- **BEING SECURE** means having risk-focused defenses around what matters most to your mission.
- **BEING VIGILANT** means having threat awareness to know when a compromise has occurred, or may be imminent.
- **BEING RESILIENT** means having the ability to regain ground when an incident does occur.