RANSOMWARE:

UNLOCKING THE LUCRATIVE CRIMINAL BUSINESS MODEL

unit42

REPORT BY BRYAN LEE

PALO ALTO NETWORKS | 3000 Tannery Way | Santa Clara, CA 95054
www.paloaltonetworks.com

paloalto NETWORKS®

Executive Summary

Ransomware, specifically cryptographic ransomware, has quickly become one of the greatest cyberthreats facing organizations around the world. This criminal business model has proven highly effective in generating revenue for cyber adversaries in addition to causing significant operational harm to affected organizations. It is largely victim agnostic, spanning the globe and affecting all major industry verticals. Small organizations, large enterprises and individual home users are all potential targets.

Ransomware has existed in various forms for decades. However, in the last several years, cybercriminals have perfected the key components of these attacks. This has led to an explosion of new malware families that have made techniques more effective and drawn new malicious actors into launching these lucrative schemes.

- The financial impact of ransomware is enormous. Estimates vary, but total costs are likely in the billions of dollars.[1]
- Ransomware is one of the few cybercriminal business models where the same attack could harm a Fortune 500 company, a local restaurant down the street and your grandmother.
- Bitcoin is fueling the success of this scheme. The payment mechanisms that early forms of ransomware relied on have been shut down or forced to regulate their payments, but bitcoin has no central authority against which law enforcement can take action.
- Initially, ransomware attacks primarily targeted Windows-based systems, but adversaries have begun branching out to target other platforms, such as the Mac® OS X® operating system.
- Until organizations around the world adopt a prevention mindset and stop paying ransoms to retrieve their data, this criminal scheme will continue to threaten all internet-connected devices.

Since the initial creation of this report, business has been booming for ransomware operators. In 2016, it was thought that there were fewer than 100 active ransomware variants out in the wild. Today, ransomware variants number at least 150, if not hundreds more. On the criminal side, tactics have largely stayed the same, leveraging such common attack vectors as phishing and exploit kits to deliver ransomware. The value of bitcoin has also gone up significantly, briefly surpassing US$19,000 per bitcoin at one point in late 2017. Understanding the combined facts of effective attacks with low costs of entry and a burgeoning value in ransoms, it is not surprising that instances of ransomware attacks have grown exponentially.

[1] http://www.zdnet.com/article/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin/, https://www.ic3.gov/media/2015/150623.aspx

The prevalence and efficacy of ransomware attacks have not gone unnoticed by other adversaries, either. 2017 saw multiple attacks that, while appearing to be typical ransomware on the surface, had completely different motives from the profit-driven aims generally associated with ransomware attacks. Even though the actual ransoms paid in these attacks were fairly minimal at scale, the disruption and instability they caused were far more impactful than simply monetary loss. As is often said, "it is a copycat world," and now that adversaries are cognizant of how effective ransomware-style attacks can be from both the profit-motivated and subterfuge perspectives, it is a simple reality that we should be prepared for more, similar attack scenarios.

Although the future may seem dire based on our observations over the last few years, the truth is that all these attacks are preventable. It can be difficult to conceptualize, especially considering the sheer onslaught of ransomware attacks we all face on a day-to-day basis. However, adversaries are neither using techniques we haven't seen before nor such fundamentally different tools that they cannot be stopped. If anything, we understand the various tactics, techniques and procedures deployed by the adversaries quite well. However, as always, the challenge lies in translating the intelligence and understanding into actionable outcomes.

Preparation

- **Backup and Recovery:** Back up data so that it will be easily recoverable after a successful ransomware attack.
- **Network Share Access Control:** In order to halt ransomware's spread, review use of network shares to ensure that write access is limited to the smallest number of users and systems possible.

Prevention

- **Email and Executable Controls:** Ransomware often begins with an email message carrying a Windows® executable. Network security devices, such as a next-generation firewall, can identify these files when they are traversing the network and should block or quarantine them.
- **Unknown Malware Prevention**: Signature-based detection systems have proven unreliable for detecting new malware. Unknown malware prevention systems should be used to augment network security devices.
- **Endpoint Control:** While network-based security devices are sometimes blind to attacks, endpoint-based controls can stop the execution of malicious files before they start.

Response

- **Understand the Threat:** In some cases, security vendors have found ways to decrypt files without paying the ransom. You can identify some ransomware using information included in the ransom note left on your system or by making use of malware analysis or intelligence systems.
- **Prepare for the Worst:** Paying a ransom to retrieve files should be a last resort. If you decide to pay the ransom, you should be prepared to make that payment in a timely manner.

TABLE OF **CONTENTS**

Introduction

The concept of holding goods for rasnsom is not a new one. Throughout human history, ransom has been a common ploy, from ancient Rome to the Age of Piracy to modern-day terrorist kidnappings. Today, cybercriminals are able to easily distribute highly effective ransomware attacks to generate profit and hold digital resources hostage using encryption technologies initially meant to secure our systems. In just a few short years, ransomware went from a niche attack to a widespread threat, impacting networks large and small.

To better understand how the current state of ransomware came to be, we have to examine the evolution of ransomware from its humble beginnings to the powerhouse it is today. Its origins reveal to us how one of today's most vexing cryptographic problems came to be, what drove cyberattackers toward it and what we can do to better protect our data.

Defining Ransomware

When most people discuss ransomware today, they think of cryptographic ransomware, which identifies valuable data on a compromised system and encrypts it, preventing the victim from accessing it unless that person makes a payment to the attacker. Although cryptographic ransomware is the most common and successful type of ransomware, it is not the only one. It's important to remember that ransomware is not a single family of malware but a criminal business model in which malicious software is used to hold something of value for ransom.

To execute a successful ransomware attack, an actor must be able to do the following:

1. **Take control of a system or device.** This may be a single computer, mobile phone or any other system capable of running software. Most ransomware attacks begin with the attacker using social engineering to trick users into opening an attachment or viewing a malicious link in their web browser. This allows attackers to install malware onto a system and take control.

2. **Prevent the owner from accessing it.** This may happen through encryption, lockout screens or even simple scare tactics, as described later in this report.

3. **Alert the owner that the device has been held for ransom, indicating the method and amount to be paid.** Although this step may appear obvious, one must remember that the attackers and the victims often speak different languages, live in different parts of the world and have very different technical capabilities.

4. **Accept payment from the device owner.** If the attacker cannot receive a payment, and, most importantly, do so without becoming a target for law enforcement, the first three steps are wasted.

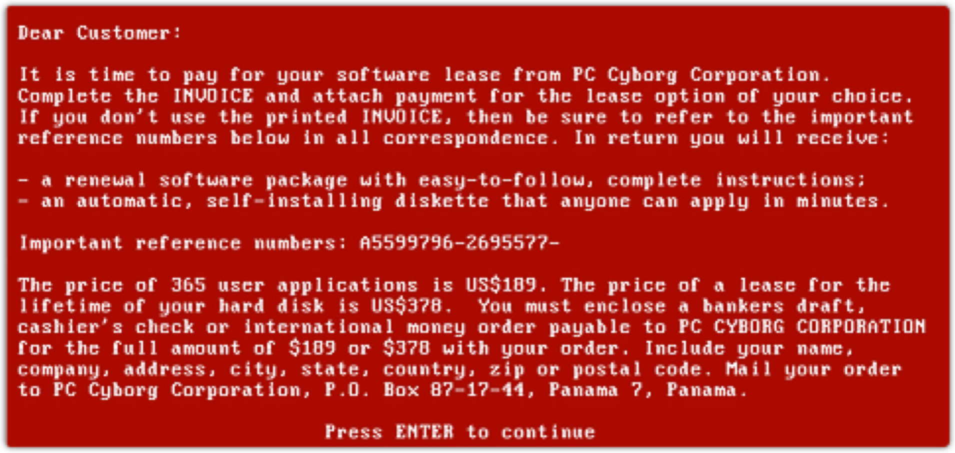
5. **Return full access to the device owner after payment has been received.** Although an attacker may have short-lived success with accepting payments and not returning access to devices, this will destroy the scheme's effectiveness over time. Nobody pays a ransom when they don't believe their valuables will be returned.

If the attacker fails in any of these steps, the scheme will be unsuccessful. Although the concept of ransomware has existed for decades, the technology and techniques, such as reliable encrypting and decrypting, required to complete all five of these steps on a wide scale were not available until just a few years ago.

Though the malware deployed in the current generation of cryptographic ransomware attacks is not especially sophisticated, it has proven very effective at not only generating revenue for the criminal operators but also preventing impacted organizations from continuing their normal operations. New headlines each week demonstrate that organizations large and small are vulnerable to these threats, enticing new attackers to jump onto the bandwagon and begin launching their own ransomware campaigns.

Ransomware History

Imagine we are back in 1989. Chicago's "Look Away" is the top hit on the Billboard 100, and you have just bought a brand new 486DX system running at a blazing 33 Mhz. There is currently a global HIV/AIDS epidemic in which the United States alone has documented 100,000 cases so far. You are an AIDS researcher, and you have just received a 5.25-inch floppy disk in the mail titled "AIDS Information Introductory Diskette" from a company called "PC Cyborg Corporation." You run the application on the disk, which appears to be a program to gauge a person's risk of contracting AIDS based on a series of questions. Suddenly, after the 90th boot up of your computer system, you are presented with this screen:



```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378.  You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

                         Press ENTER to continue
```

Figure 1: "AIDS" ransomware message

The **"AIDS"** virus, as it became known, is credited as the first documented ransomware malware in computing history. Dr. Joseph Popp was an evolutionary biologist actively involved in AIDS research who had concocted a plan to distribute 20,000 diskettes containing his AIDS Trojan to more than 90 countries, using the fictitious "PC Cyborg Corporation" as a cover. To this day, Popp's motivation is unclear – his attorneys argued at the time of his trial that he was planning to donate the proceeds of the ransom payments to further AIDS research, perhaps in an attempt to signify that he was potentially a Robin Hood-esque character. The Guardian news publication, however, presented evidence that Popp may have been motivated by rejection from a position with the World Health Organization. In either case, what Popp accomplished would provide the foundational for future ransomware authors to use.

Popp and his AIDS Trojan took victims by complete surprise in an age predating the internet and even email. In fact, there were no laws to even deal with this type of case once Popp had been apprehended – the prosecutors had to rely on the 1968 Theft Act to even attempt to take action against him. Popp's tactics were fairly sophisticated for their time, but several flaws would be revealed that cybercriminals would learn from and address to evolve into today's crypto ransomware.

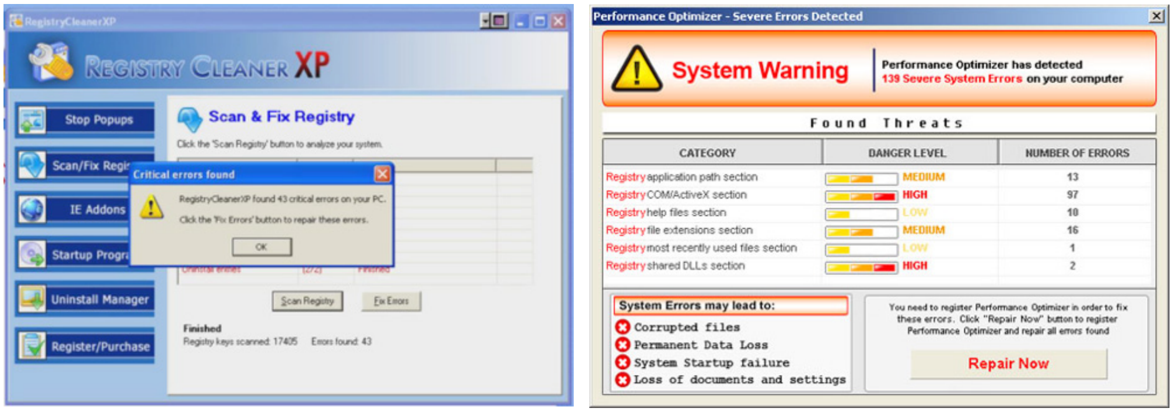
Popp's initial social engineering attack was clever, leveraging a well-known cultural topic as an attractive lure. The Trojan itself used a decoy application in the guise of a survey, which functioned as one would expect. However, in the background, AIDS replaced the startup script AUTOEXEC.BAT with malicious instructions, whereupon with the 90th boot up of the victim host, the ransom screen was presented, and all file directories and filenames were encrypted with a custom encryption algorithm. The ransom screen requested a payment of US$189 via money order or cashier's check, sent to a P.O. box in Panama in exchange for the decryption key. Future analysis of the AIDS Trojan would reveal several critical flaws:

- The file system itself was not encrypted. Only the filenames and directory names were encrypted. Thus, all files still existed on the victim host in a non-encrypted space but were inaccessible.
- Symmetric encryption was used to encrypt the filenames and directory names. This meant that the key used for encryption was the same as the key used for decryption and embedded into the malware itself.
- The payment system was not user-friendly. Sending a cashier's check or money order to an unknown P.O. box in Panama with the hope that a decryption key would be sent back was time-intensive and lacked any sort of guarantee that it would even work.

Due to the innate flaws of the AIDS Trojan, not long after the initial panic, security analysts were able to create two tools for file recovery: AIDSOUT and CLEARAIDS. The damage was done, however; one Italian research organization reported losing 10 years of research due to the AIDS Trojan. In addition, the analysis revealing the flaws would become the stimulus for a research paper by Adam L. Young and Moti Yung detailing how the use of asymmetric cryptography, specifically the use of a public key infrastructure, could have significantly increased the efficacy of the AIDS Trojan and future crypto ransomware.

Branches of Ransomware

In 2005, ransomware malware forked into two forms: misleading applications – or what would come to be referred to as "scareware"– and an evolution of cryptographic ransomware. Scareware would become the prevailing style of ransomware during this time frame, likely due to lower barriers of entry and simpler functionality. Scareware is exactly what it sounds like: a form of malware or similar behavior using scare tactics, such as aggressive notifications of nonexistent issues with a computer system that could allegedly be resolved with an easy payment of US$30–$90.



Click the 'Scan Registry' button to analyze your system.

Critical errors found

RegistryCleanerXP found 43 critical errors on your PC.

Click the 'Fix Errors' button to repair these errors.

Finished
Registry keys scanned: 17405 Errors found: 43

Performance Optimizer - Severe Errors Detected

System Warning

Performance Optimizer has detected
139 Severe System Errors on your computer

Found Threats

CATEGORY	DANGER LEVEL	NUMBER OF ERRORS
Registry application path section	MEDIUM	13
Registry COM/ActiveX section	HIGH	97
Registry help files section	LOW	10
Registry file extensions section	MEDIUM	16
Registry most recently used files section	LOW	1
Registry shared DLLs section	HIGH	2

System Errors may lead to:
- Corrupted files
- Permanent Data Loss
- System Startup failure
- Loss of documents and settings

You need to register Performance Optimizer in order to fix these errors. Click "Repair Now" button to register Performance Optimizer and repair all errors found

Figure 2: Examples of scareware

These applications were quite unsophisticated and sometimes not even applications at all. Authors of scareware used any possible tactic they could to extort money, whether that was simple tools that appeared to be legitimate system tools, banner ads, images or even simple pop-ups. At this time, the internet was still a newer concept to the masses, and due to lack of education, awareness and bad practices in web design, distribution of scareware in all its various forms was widespread. This style of ransomware, however, would ultimately become more of a nuisance than a real threat since nothing of value was actually held hostage nor was access denied to any sort of digital resource. In addition, payment systems in this era were still quite immature, which made payment attempts by victims challenging.

While scareware was rapidly spreading and quickly becoming a significant nuisance to the growing number of users on the internet, a secondary development regarding crypto ransomware was underway. A new family of crypto ransomware called **"GPCode"** or **"PGPCoder"** was discovered in mid-2005, primarily targeting Russian organizations and thought to originate from a Russia-based author. In its initial iterations, the malware claimed to use PGP encryption to deny access to files, but analysis of the malware quickly revealed that the actual encryption model was custom-made by the author and incredibly weak.

The initial variants of GPCode used many of the same tactics that modern-day crypto malware would come to use, targeting files with specific extensions, attempting to maintain persistence on the victim host, and generating a helpful text file containing instructions on how to recover files by paying a ransom of US$100–$200 through the (now defunct) E-Gold or Liberty Reserve digital currencies. Unfortunately for the author of GPCode, due to the weak custom encryption model, researchers were able to crack the encryption quite easily, and decryption tools were created and shared. However, the author would continue to develop GPCode for the next five years, with each iteration evolving, fixing flaws and becoming more effective in its mission.

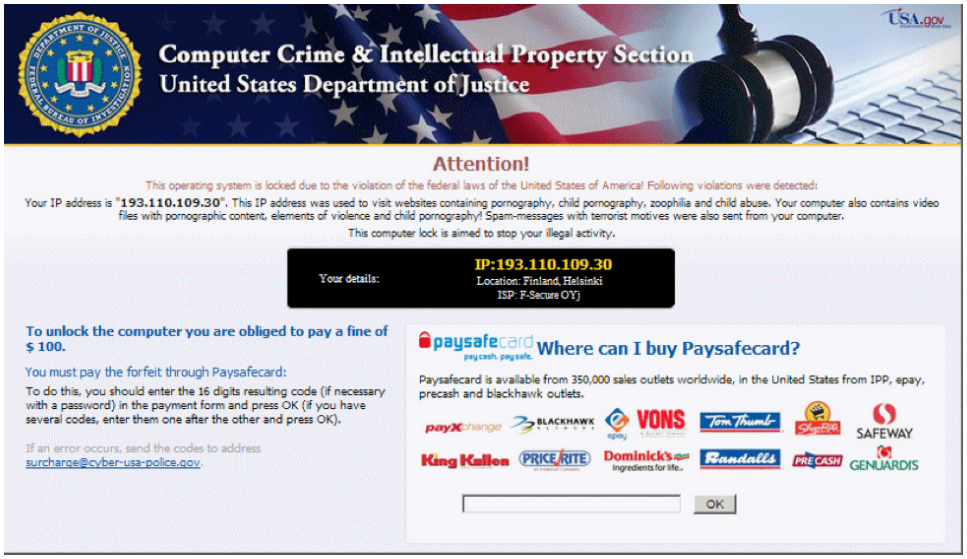
New GPCode variants attempted to be more effective at denying users access to their files by writing encrypted files to a new location and deleting the originals. This tactic proved ineffective as a simple "undeletion" or file restore utility would allow victims to recover their files. The final iteration of GPCode would prove to be a prototype for modern crypto ransomware, using RSA-1024 and AES-256 as the encryption algorithms and physically overwriting any files that were encrypted. The use of RSA-1024 introduced an asymmetric encryption model where previous variants used symmetric encryption. In this model, rather than embedding the encryption key for the files inside the malware, it generated a new symmetric key for each infection. It then used an embedded RSA public key to encrypt the symmetric key such that only the attacker's private key could decrypt it. Variants of the encryption model would be deployed by the majority of ransomware that followed years later.

Although the criminal behind GPCode had successfully solved one of the major challenges for launching a successful ransomware attack, very few followed that lead. Instead, adversaries continued to deploy and evolve their scareware attacks, moving into an area informally called Fake Antivirus or FakeAV. This was a natural step for the previous types of scareware in terms of escalation – because there had been so much attention paid to the previous scareware variants and other spyware types of misleading applications, adversaries attempted to capitalize on that specific fear by aggressively displaying alerts and notifications about potential malware issues on a victim host.

Continuing to prey on the fear, uncertainty and doubt of the normal internet user, attackers simply modified the message from previous scareware to extort users based on their fear of malware. Between 2008 and 2009, FakeAV was by far the most prolific type of malware seen in the wild. With FakeAV, cybercriminals began using any means necessary to load their malware onto systems, as any infected computer could generate revenue for them. Their tactics included loading the payload into exploit kits, using SEO manipulation to redirect users from their legitimate searches to malicious sites set up for malware distribution, phishing emails, banners, pop-up ads, browser toolbars – the list goes on. However, other than aggressive notifications and being a major nuisance, FakeAV and other scareware variants did not generally harm the victims or their organizations. At worst, they were extremely bothersome and annoying applications that resided in the background and would continuously and persistently alert a user on false reports.

During the scareware and FakeAV eras, multiple legal actions were taken by organizations who wanted to stop this activity, including Microsoft® and the U.S. Federal Trade Commission. These actions may have led to the slowdown and eventual end of the use of scareware. Additionally, law enforcement agencies around the world began to lay heavy pressure on banks to shut down merchant gateways that had been taking part in processing the ransoms associated with scareware. This would also lead to many of the fledgling internet monetary transaction organizations to shut down due to accusations of fraud and large numbers of credit card chargebacks that were issued.

There would be one final hurrah for the scareware style of ransomware, though, with the introduction of the "locker" ransomware from 2011 to 2012, the most well-known family being Reveton. Lockers are very similar to previous scareware variants, relying on fear, uncertainty and doubt in hopes to extort money from victims. Where they differed, however, was that they would actively deny victims access to their systems. No files were affected, but an infected user would be greeted with a seemingly legitimate image purporting to be from a law enforcement agency or other organization, claiming that it had observed the victim performing illegal activities.


Computer Crime & Intellectual Property Section
United States Department of Justice

Attention!

This operating system is locked due to the violation of the federal laws of the United States of America! Following violations were detected:

Your IP address is "193.110.109.30". This IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

Your details: IP:193.110.109.30
Location: Finland, Helsinki
ISP: F-Secure OYj

To unlock the computer you are obliged to pay a fine of $ 100.

You must pay the forfeit through Paysafecard:

To do this, you should enter the 16 digits resulting code (if necessary with a password) in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

If an error occurs, send the codes to address surcharge@cyber-usa-police.gov.

Where can I buy Paysafecard?

Paysafecard is available from 350,000 sales outlets worldwide, in the United States from IPP, epay, precash and blackhawk outlets.

Figure 3: An example of locker-style ransomware

An easy payment would, however, restore access to a victim's system with all files intact and the locker removed. The variants of the locker-style ransomware were quite effective to the point that one man actually turned himself in to the local authorities because he actually had been performing illegal activities on his computer. As effective as this type of ransomware was in scaring people into opening their wallets, it was, fortunately, not extremely difficult to remedy. Simple strategies, such as performing a system restore, booting into safe mode and removing the persistence mechanism, or, later on, using free tools created by security vendors, allowed for straightforward removal of the malware. Lockers were the final wave for this branch of ransomware as adversaries began to shift their tactics, seemingly asking themselves, "What can we do to be more effective at extortion?" The answer would be found in 2013, with the introduction of CryptoLocker.

CryptoLocker

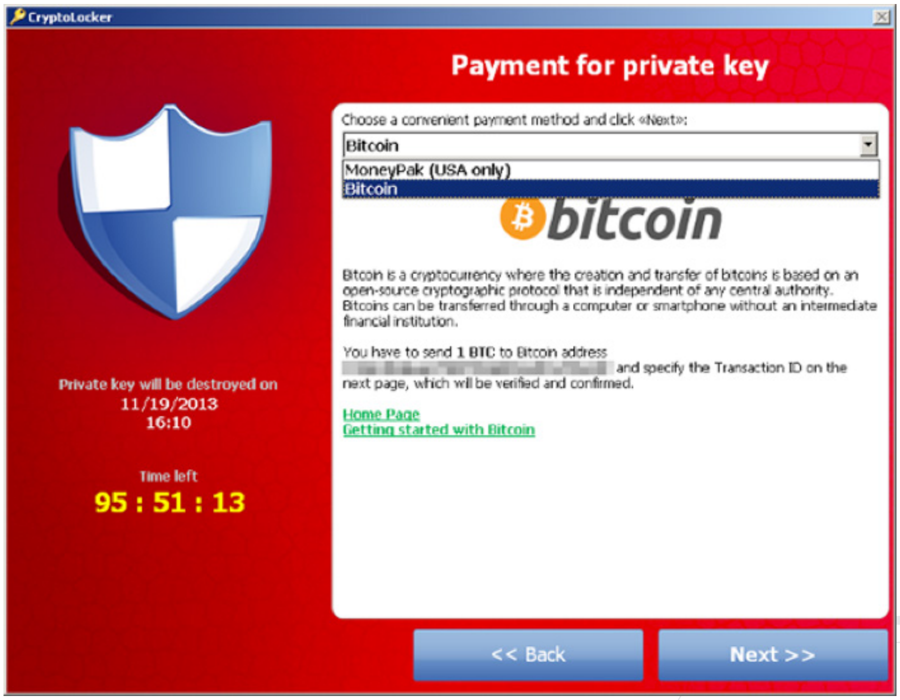
In late 2013, reports across the internet began appearing regarding some sort of encryption-based malware that was infecting Windows-based systems. This malware would come to be known as "**CryptoLocker"** and prove to be a vanguard of the multimillion dollar crypto ransomware industry.

CryptoLocker was unique in that it appeared the authors and operators had actively studied previous variants and styles of ransomware and aimed to remedy the flaws that had been previously exposed. It also proved to be a shift in tactics by cybercriminals as, until the release of CryptoLocker, widespread ransomware was almost exclusively scareware, where no actual damage was being done to digital assets (outside of GPCode). This was a fundamental shift in how attackers operated, and it showed that they would continue to develop and escalate as needed to accomplish their goals of generating profit.

CryptoLocker did not use particularly sophisticated tactics; it actually shared similar distribution models to those of previous ransomware variants, primarily relying on phishing attacks with portable executable attachments. At times, an extra layer of obfuscation was used via double extensions to disguise the real .exe extension. The operators of CryptoLocker generally relied on social engineering and lack of user awareness to lure potential victims to launch the malware itself, although there was also some propagation via the Gameover ZeuS botnet.

Once running on the system, CryptoLocker demonstrated its true capabilities and efficacy from previous lessons learned. First, it would install itself to the user's profile folder. Next, it would add a registry key to run at startup to maintain persistence. Then, it would attempt to communicate with a command-and-control server to generate an RSA-2048 key pair and send the public key back to the victim host. The use of a very strong asymmetric encryption model would prove to be extremely effective as every key pair was unique, and there was no way to retrieve the private key used for decryption because it resided on the command-and-control servers.

RSA-1024, used by GPCode, had already proven to be uncrackable via brute force by this point. Additionally, the command-and-control servers used domain generation algorithms based on a pseudo-random number generator, which made it even more challenging to track down or prevent command-and-control communications until the algorithm was reverse-engineered. After generation of the unique key pair, encryption would begin on the affected host, targeting business-related document files instead of the entire file system. After successful encryption, a notification would appear indicating that the private key used for decryption would be destroyed, in effect causing the data to be lost forever, if the ransom was not paid within a set number of hours.



Private key will be destroyed on
11/19/2013
16:10

Time left
95 : 51 : 13

Choose a convenient payment method and click «Next»:

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send 1 BTC to Bitcoin address [redacted] and specify the Transaction ID on the next page, which will be verified and confirmed.

Figure 4: CryptoLocker countdown

Payment was made possible via MoneyPak or the better-known alternative, bitcoin. The increased popularity of bitcoin during this time frame, in conjunction with its inherent function as a cryptocurrency, was certainly attractive to the CryptoLocker operators. It was a relatively simple, reliable and semi-anonymous form of payment that was not tied to any organization or government that might shut it down or confiscate funds. In the year that CryptoLocker was in the wild, the attackers behind the scheme generated an estimated revenue of approximately 42,000 bitcoin, or about US$27 million.

At this point, the cybercriminals behind CryptoLocker were not only preying on the fear of affected users via the threat of permanent loss of their data, but also the active denial of access to a victim's data via encryption. To put it bluntly, the attackers were no longer using bluffing strategies but actually taking action against their victims. However, all was not lost as the shift in tactics introduced new flaws in the scheme.

As the asymmetric key pair was generated on the fly only after successful command-and-control communication, if communications were interrupted or never established, no encryption would occur. In addition, early variants did not remove shadow volume copies, which could allow for a user to use the system restore function in Windows to restore to an uninfected state. Lastly, even if the key pair for encryption was created, and encryption began on the victim host, there was a small time window when encryption could potentially be interrupted while it was iterating through the targeted files.

In the summer of 2014, the U.S. Department of Justice executed a takedown of the Gameover ZeuS botnet, dubbed "Operation Tovar," which also impacted the CryptoLocker infrastructure. Fortunately for victims of this scheme, one of the security firms involved in the takedown, Fox-IT, was able to gain access to the private key database of CryptoLocker, effectively nullifying the asymmetric encryption it used by making all the private keys used for encryption freely available. The isolation and access to CryptoLocker's private key database would effectively end its operations, but it did not stop the overall threat of ransomware. If anything, other cybercriminals were able to observe how effective this business model was and use the experience of CryptoLocker as a launching point for numerous clones, bringing us into the Age of Crypto Ransomware.

Ransomware Today

Every week, we see new headlines describing organizations whose operations have been shut down or severely degraded by ransomware attacks. Although the theft of information may go unnoticed or unreported, ransomware attacks can have a very public impact. Ransomware has transitioned from a niche attack into one of the largest threats to organizations large and small today.

Unit 42 currently tracks more than 150 different crypto ransomware families in the Palo Alto Networks® AutoFocus™ contextual threat intelligence system. These crypto ransomware families are all distinct but follow very similar playbooks to the one demonstrated by CryptoLocker. The differences we have observed between the clones are more refinements than significant evolutions, with the exception of non-profit-motivated ransomware variants.

Distribution models have been updated to take advantage of additional attack vectors. **CryptoWall** was infamous for leveraging various exploit kits to allow for delivery and execution of the payload without requiring user interaction for a successful infection. **Locky** was well-known for being packaged inside macros embedded in malicious documents to be loaded and executed. Other variants, such as **SamSa**, have been observed being loaded manually by operators without any command and control, automated communications, or delivery. As more organizations began stripping files with .exe extensions, the **TeslaCrypt** operators shifted to using JavaScript files inside .zip archive files as the downloader for its payload.

Other parts of the attack scheme have also been refined, such as the use of various anonymous networks, like TOR or I2P, for command-and-control communications to evade network inspection, the use of CAPTCHAs for payment landing pages to evade security researchers, and even additional features for usability for victims. Many variants of crypto ransomware now offer features such as live chat for technical support and localization efforts, providing translated instructions based on the geolocation of a victim host's IP address.

As adversaries have continued their development of technologies and tactics in their ransomware attacks, more delineations have been created between developers and operators. Cybercriminals can now execute ransomware attacks with little to no expertise in the development of malware or even in-depth understanding of cyberattacks. Ransomware has become so commoditized that the concept of "ransomware as a service" is now a distinct and very real facet of ransomware attacks. One of the most infamous variants that leveraged a RaaS business model is **Cerber**. By licensing or leasing Cerber for a fee or percentage of the ransom, even non-technical cybercriminals can simply navigate to the RaaS website, input a few parameters and immediately have access to customized ransomware variants that are being continuously updated and developed to contain new functionality and evasion tactics. Ransomware has now become more accessible to the common criminal, even managing to break through the technological expertise barrier.

Cybercriminals have realized ransomware is a lucrative business with little or low cost barriers to entry and, using the frameworks laid down by AIDS, GPCode and CryptoLocker, have mastered all five steps required to succeed with this criminal business model. They have also begun expanding their attacks to platforms outside of Windows. This includes Android® phones via third-party APK files that are loaded with user interaction and, more recently, Mac OS X systems. Until March 2016, OS X had largely been either ignored or not effectively targeted by crypto ransomware operators. On March 6, 2016, we discovered the first documented instance of crypto ransomware specifically targeted at OS X hosts, called KeRanger.

KeRanger was distributed in a manner that was slightly unique – the operators compromised the website of a popular BitTorrent® client named Transmission and trojanized the installation package on the website. This was not a new tactic when it came to general malware distribution, but it had not been observed previously in relation to ransomware on OS X.

Ransomware as an Espionage Tool

By and large, profit-motivated ransomware attacks have remained the same in terms of tactics, techniques and procedures. In 2017, however, we began to observe attacks that leverage ransomware-style tactics while seeking espionage-based outcomes.

RanRan

In March 2017, we discovered a completely new ransomware variant targeting several organizations in the Middle East, which we named **"RanRan."** To this day, the attacks we discovered in that time frame, in that specific region, are still the only instances of RanRan that have ever been reported or discussed.

RanRan was extremely unique in that it was not profit-driven at all. Instead, once a user was infected with RanRan, the ransom note requested that the victim create a specific website and place inflammatory and violent remarks against a political leader in the region. This was not an attempt to generate monetary gains; instead it was political extortion. Other than the rather unique motivation and ransom note, the actual malware itself behaved very similarly to other known ransomware, enumerating potentially important files throughout the file system and encrypting them with a specific key.

WannaCry

While RanRan was quite obviously ransomware deployed as an espionage measure, it was still fairly isolated both in time frame and region. The attack known as WannaCry, WanaCrypt0r, WannaCrypt and so on would rapidly change our view of just exactly how ransomware could be leveraged to cause mass disruption.

On May 12, 2017, a ransomware attack was launched and, within a day, more than 230,000 users in more than 150 countries were reported to have been infected. This attack, WanaCrypt0r, was the first instance of a ransomware worm. On the surface, it appeared to be like most other ransomware variants, enumerating important system files, encrypting them and requesting about US$300 in ransom to decrypt the files and allow for resumption of operations.

Worming attacks are unique in that their delivery mechanism after an initial infection is generally automated in nature. The objective of any worm attack is generally to infect as many systems as possible, as rapidly as possible. As the attack grows in scale, the speed of the infection also grows exponentially as more and more victims join the infected. One of the most famous worms ever discovered was **Conficker**, back in November 2008. Conficker was thought to have infected up to 15 million systems globally, with the end goal to create a massive botnet from which a criminal element would profit. Since that time, we had not observed worming attacks at that scale until WanaCrypt0r.

The WanaCrypt0r attack was an interesting scenario due to the various factors at play causing it to become so effective and receive so much attention. The initial victimology pointed to the United Kingdom's National Health Service, which immediately reported that its operations had been disrupted by a large-scale, self-propagating ransomware worm. As the worm continued to spread beyond the UK NHS and more analysis was completed on it, several things became apparent:

- Two tools possibly developed by a government entity were being used for propagation.
- There was no way for the ransomware operators to identify unique victims and their payments.
- The ransomware itself contained a "kill switch."

The tools in use for propagation were called ETERNALBLUE and DoublePulsar. Both tools had been previously disclosed in a data dump by an entity called The Shadow Brokers, with claims that a U.S. government entity had developed them for offensive operations. ETERNALBLUE was an exploit for a vulnerability in the Microsoft Windows Short Message Block, or SMB, protocol, which is primarily used for file transfers. It allowed for arbitrary execution of transferred files, in this case executing the DoublePulsar backdoor. DoublePulsar is a backdoor tool that runs in memory, allowing it to be "fileless," and was used after being executed by ETERNALBLUE to then install the actual WanaCrypt0r ransomware payload.

Beyond the mechanism for self-propagation and installation, it quickly became apparent that, based on the way the WanaCrypt0r ransom note was written – using a handful of hard-coded bitcoin wallets – there was no way for the operators to identify specific victims. There was simply no obvious differentiator for victims, such as a unique victim ID, wallet to pay to, or encryption key. This begs the question: what was the ultimate goal of this attack?

Lastly, while the worm was continuing its propagation and attack, a security researcher discovered a "kill switch" function in the WanaCrypt0r payload itself. The ransomware payload, when executed on a victim host, would perform an initial check into a specific domain, expecting it to be unresponsive. If a response was made, the ransomware would immediately cease execution. The leading theory on why this specific function was included in the payload is that it may have been used as an anti-analysis technique to evade sandboxes and other analysis environments. The idea was that, in a sandbox or similar environment, any network activity would be responded to in order to cause the malware to believe it is infecting an actual victim. Unfortunately for the creators of WanaCrypt0r, they had neglected to register the domain, which meant that as soon as a security researcher registered the domain and began responding to any check-ins, all future infections would immediately fail. Because of these efforts, the WanaCrypt0r attacks were effectively halted by May 15, 2017, three days after the initial outbreak.

Examining this attack post-mortem reveals several interesting points from multiple perspectives. First, there is the question of patching – Microsoft had issued a patch for the SMB vulnerability exploited by ETERNALBLUE in March 2017, well in advance of this attack. Second, even if the patch was not applied, why was SMB exposed to external networks at so many organizations? SMB had generally been associated with file transfers within intranets, compared to other protocols that may be better suited to external networks. Third, the attack itself had several factors that didn't quite add up, such as the generic ransom notes that weren't specific to victims and the inclusion of a kill switch. Two things are certain, however: this attack caused significant disruption throughout the world and gained significant media notoriety.

NotPetya

As the world was still reeling from the fallout of the WanaCrypt0r ransomware worm and reimagining how ransomware tactics could be deployed for motivations other than pure profit, we observed another attack using ransomware techniques that were, again, wholly different. On June 27, 2017, a type of attack known as a "supply-chain" attack was launched, where an accounting software heavily used in Ukraine, called "MeDocs," began to push a Trojanized version of itself to its users via a software update. MeDocs is thought to have about 400,000 users and is in use by over 90 percent of all tax firms in Ukraine. An adversary is thought to have compromised internal MeDocs systems, allowing that person or group to distribute the Trojanized version via a legitimate update channel.

The payload within MeDocs initially appeared to be a version of a well-known ransomware variant called Petya. Petya was unique in that it was a ransomware that did not target files and instead would encrypt the master boot record, rendering the victim system inoperable. The version found embedded inside MeDocs had been modified to also target individual files, as well as to contain the distribution mechanism found in WanaCrypt0r, using ETERNALBLUE and DoublePulsar. Further analysis of the payload showed that the modifications were so extensive that it began to be called NotPetya and other variants, such as SortaPetya and Nyetya. NotPetya contained significantly more capabilities than the original Petya ransomware, including file overwriting, remote access, credential harvesting and arbitrary file execution. NotPetya also had the ability to identify and fingerprint unique hosts, suggesting this attack was far more targeted in nature.

The attack was primarily isolated to the country of Ukraine, but due to the borderless nature of networks in contrast to geographic borders, some organizations outside of Ukraine were also affected. It is estimated 80 percent of all infections were in Ukraine. Several ministries, banks, state-owned transportation services and energy services were affected. Although victims were shown the standard Petya ransom note, claiming files could be easily reclaimed by paying the ransom amount shown, NotPetya actually overwrote important files, leaving the victim hosts permanently damaged. Furthermore, the attack was executed on the eve of a Ukrainian public holiday, Constitution Day. It is likely government offices would have been empty, potentially leading to a more successful attack.

Due to these factors, it is believed the NotPetya attack was likely a targeted attack with the goal of disrupting and crippling the country of Ukraine, specifically, while masquerading as a traditional ransomware attack.

By June 28, 2017, the Ukrainian government released a statement indicating the attack had been halted. On July 4, 2017, after potential evidence of continued access by the NotPetya operators was discovered, Ukrainian police raided the MeDocs office and seized its servers.

The Future of Ransomware

The recent success of ransomware is showing no signs of slowing down or stopping. The ransomware business model has proven very effective at turning infected computers into revenue for cybercriminals and is now displacing previous models. Displaying pop-up ads and sending spam is no longer as lucrative as it once was, but nearly all computers or devices are potential candidates for ransom.

In addition to the profit-motivated adversaries we have always associated with ransomware attacks, we are now beginning to see more attacks where ransomware techniques are being leveraged by espionage-motivated adversaries. Considering how effective these attacks have been even in limited volume by attacks launched, it is without doubt that we will observe more attacks with these types of tactics being deployed.

In the future, we can expect to see the following developments in ransomware.

More Platforms

As noted in the previous section, ransomware has already moved from Windows to Android devices and, in one case, targeted Mac OS X. No system is immune to attack, and any device that an attacker can hold for ransom will be a target in the future.

This concept will become even more applicable with the growth of the internet of things. Although an attacker may be able to compromise an internet-connected refrigerator, it would be challenging to turn that infection into a revenue stream. The ransomware business model can be applied in this or any other case where the attacker can achieve all five steps for a successful ransomware attack identified earlier in the document. After infecting the refrigerator, the attacker could remotely disable the cooling system and only re-enable it after the victim has made a small payment.

Higher Ransoms

The majority of single-system ransomware attacks charge a ransom of between US$200 and $500, but the values can be much higher. If attackers are able to determine that they have compromised a system that stores valuable information, and that infected organization has a higher ability to pay, they will increase their ransoms accordingly. We have already seen this in a number of high-profile ransomware attacks against hospitals in 2016, where the ransoms paid were well over US$10,000.

Targeted Ransom Attacks

A targeted intrusion into a network is valuable to an attacker in many ways. Selling or acting on stolen information is a common technique, but it often requires additional "back-end" infrastructure and planning to turn that information into cash. Targeted ransomware attacks are an alternative for attackers who may not know how else to monetize their intrusion. Once inside a network, attackers can identify high-value files, databases, and backup systems and then encrypt all of the data at one time. These attacks, using the SamSa malware, have already been identified in the wild and proven lucrative for the adversaries conducting them.

Espionage-Motivated Ransomware

Espionage-motivated adversaries have shown how effective using ransomware-style techniques in their attacks can be to cause disruption, instability and panic throughout entire countries, and even globally. Adversaries are well-known for copying tactics from each other based on efficacy, and just from the WanaCrypt0r and NotPetya attacks, it is quite apparent that these types of techniques are extremely effective. Pandora's box has been opened, and we will continue to see these types of tactics

Defense Against Ransomware

While defending against a ransomware attack is not entirely different from defending against other attacks involving malware, it does present new challenges and opportunities for network defenders, system administrators and users. Understanding how exactly ransomware evolved to its current state allows us to better understand why cybercriminals may be using certain tactics or methodologies and how to defend against them.

No organization wants to be shut down by a ransomware attack or forced to pay a ransom to retrieve its data. To avoid this situation, it's much better to be aware of the threat and create a plan for how to stop it before it becomes an issue. Defense against ransomware can be broken down into three primary categories: preparation, prevention and response.

Preparation

Backup and Recovery

One of the best defenses against ransomware is through your backup and data recovery process. If you can recover encrypted files from backups, you'll be able to recover from a successful ransomware attack with little to no impact on your organization. Backups should be kept in a location that is not accessible to the ransomware – not a connected USB drive, for instance.. Attackers have been known to targeted backups as part of their efforts to encrypt all valuable files. Testing the process of recovering files from a backup is almost as important as the backup itself. If you have never tested your recovery process, you may find out your backups are not as secure as you thought.

Network Share Access Control

Network drives that are mounted to multiple systems and contain shared data are especially vulnerable to ransomware attacks. If a system or user who is able to write to the mounted drive is infected with ransomware, all of the files stored on the network share may also be encrypted. This turns a single infection into a network-wide outage. Organizations should review their use of network shares to ensure that write access is limited to the smallest number of users and systems possible. As most ransomware attacks occur when users are browsing the web or reading email, limiting this activity on systems with write access is extremely prudent.

Prevention

As ransomware attacks act quickly – typically within minutes of an infection – the "detect and respond" model provides little value in limiting their impact. If a detection system alerts you that an infection has occurred, it's very likely already too late to stop your files from being encrypted. It is critical to deploy controls that are able to prevent malware from entering the network and executing on the systems storing your valuable data.

Email and Executable Controls

Ransomware attacks most often begin with an email message carrying a Windows executable file or a user clicking on a link that downloads one. There are very few legitimate scenarios in which a user should be receiving an executable file sent as an email attachment. Downloading executable files through a web browser is also a rare event that deserves additional scrutiny. Network security devices, such as next-generation firewalls, can identify these files when they are traversing the network and block or quarantine them. While this will not stop all ransomware attacks, it will prevent many of them and is a good first step toward prevention.

Unknown Malware Prevention

Signature-based detection approaches have proven unreliable for detecting new malware that has not yet been observed in the wild. Attackers launching ransomware campaigns test their attacks against these systems before deploying them to ensure they will not be detected. In order to protect your organization from these rapidly changing malware variants, you need the ability to identify never-before-seen threats and automatically send new protections back down to the network. As opposed to matching known malicious patterns, these systems leverage sandbox analysis to identify malicious behaviors through both static and dynamic analysis in a virtual environment, including global threat intelligence sharing.

Endpoint Control

Network-based security devices are sometimes blind to attacks, especially those leveraging SSL encryption or other forms of network traffic obfuscation. In these cases, the best defense is an endpoint-based control that stops the execution of malicious files before they start.

User Identity Protection

Being able to protect individual user credentials is pivotal for cybersecurity overall. Using techniques such as forced multi-factor authentication throughout the network can help with several ransomware-style attacks. In a worming scenario, such as WanaCrypt0r, forcing users to reauthenticate as they were attempting to access another system over the SMB protocol may have slowed down the spread or even isolated it to a single system. Oftentimes, in ransomware scenarios, adversaries will compromise legitimate mailboxes via credential harvesting to distribute their ransomware via phishing from legitimate email addresses. Again, deploying multi-factor authentication can help with preventing adversaries from gaining access to a user's mailbox even if the password has been compromised.

Response

If your prevention controls have failed and you find yourself the victim of a ransomware attack, it is important to have a response plan in place. This plan will help you make the right decisions to recover your data as quickly as possible with the least impact to your organization.

Understand the Threat

With more than 150 families of ransomware in the wild and new variants uncovered every day, an important first response step is knowing exactly with what you are dealing. The majority of new ransomware families use strong cryptography that cannot be easily reversed, but in some cases, security vendors have found ways to decrypt files without paying the ransom. The only way you'll know this is by identifying the family first.

Oftentimes, we can identify some ransomware using information included in the ransom note left on your system. Information such as the adversary's email address, the text of the ransom note or even the bitcoin wallet address can help identify the specific ransomware family. Another option is to use automated malware analysis or intelligence systems that can identify ransomware families.

Prepare for the Worst

Paying a ransom to retrieve files should be the last resort for any organization. Payments help fund criminal enterprises and perpetuate attacks by encouraging others to hold more data for ransom. Even if you have no backups of your encrypted data, consider your options before making a payment:

- Can you recreate the stolen data?
- Do you have an old version of the files that can be updated with new information?
- Does the data exist anywhere else, such as on a system that wasn't impacted at another location?

If all else has failed and you have decided to pay the ransom, you should be prepared to make that payment in a timely manner. Nearly all ransomware requires payment through the bitcoin cryptocurrency, but acquiring thousands of U.S. dollars' worth of bitcoin in a matter of hours can be quite tricky. Part of any ransomware response plan should include details on how to facilitate the payment in the worst-case scenario.

unit42

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com