RANSOMWARE:

UNLOCKING THE LUCRATIVE CRIMINAL BUSINESS MODEL

unit 42

REPORT BY BRYAN LEE

PALO ALTO NETWORKS | 4401 Great America Parkway | Santa Clara, CA 95054
www.paloaltonetworks.com

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 to be highly effective in generating revenue for cyber adversaries in addition to causing significant operational impact to affected organizations. It is largely victim agnostic, spanning the globe and affecting all major industry verticals. Small organizations, large enterprises, individual home users – all are potential targets.

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

- The financial impact of ransomware is enormous, with several high-profile infections leading to millions of dollars in ransom paid to attackers.[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.
- The cryptocurrency Bitcoin has provided a payment mechanism that 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.
- Thus far, ransomware attacks have primarily targeted Windows-based systems, but adversaries have begun branching out to target other devices, such as attacks against 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.

Preparation

- **Backup and Recovery:** Backup 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.

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

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 transiting 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 using malware analysis or intelligence systems.
- **Prepare for the Worst:** Paying a ransom to retrieve files should be the last resort of any organization. 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 a ransom for goods is not a new one. Throughout human history, ransom has been a common ploy, from ancient Rome to the Age of Piracy and 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 exactly it is that one of today's most vexing cryptographic problems came to be, what drove cyber attackers 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 – ransomware that 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. While 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.** While 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, receive the payment 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.** While an attacker may have short-lived success with accepting payments and not returning access to devices, in time this will destroy the effectiveness of the scheme. Nobody pays a ransom when they don't believe their valuables will be returned.

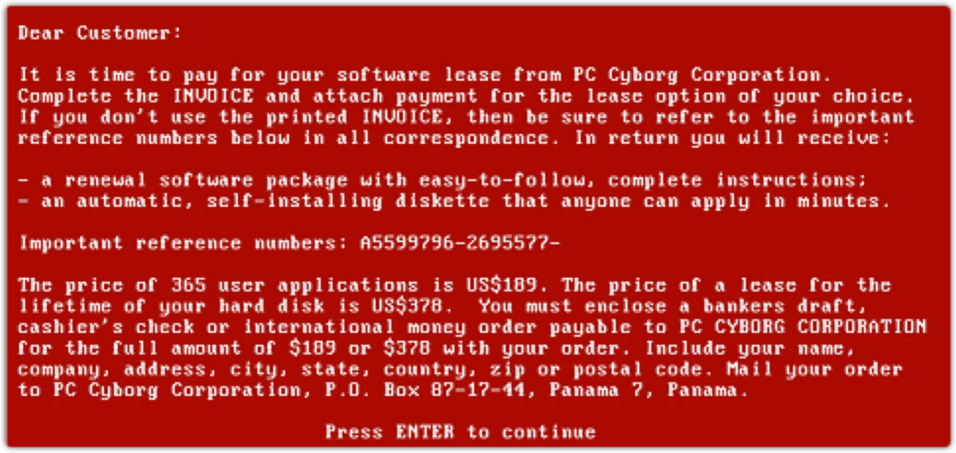
If the attacker fails in any of these steps, the scheme will be unsuccessful. While the concept of ransomware has existed for decades, the technology and techniques, such as reliable encrypting and decrypting, required to complete all five of these steps on a wide scale were not available until just 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 in preventing impacted organizations from continuing their normal operations. New headlines each week demonstrate that organizations, large and small, are vulnerable to this threat, 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 where 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 does appear 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:

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 to over 90 countries containing his AIDS Trojan using the fictitious "PC Cyborg Corporation" as a cover. To this day, Dr. 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



```
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
```

was potentially a Robin Hood-esque character. The Guardian news publication, however, presented evidence that this behavior may have simply been vengeance for a job rejection at the WHO for Dr. Popp. In either case, what Dr. Popp accomplished would provide the foundational groundwork for future ransomware authors to use.

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

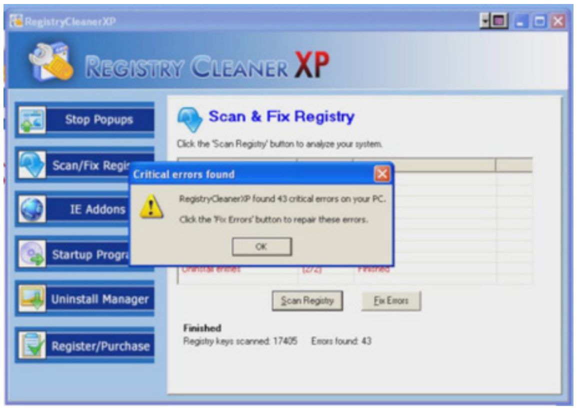
Dr. Popp's initial social engineering attack was clever, leveraging a well-known cultural topic as an attractive lure. The Trojan itself used a decoy application in the guise of a survey, which functioned as one would expect. However, in the background, AIDS replaced the startup script AUTOEXEC.BAT with 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 $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 ten 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 non-existent issues with a computer system that could allegedly be resolved with an easy payment of US$30-$90.



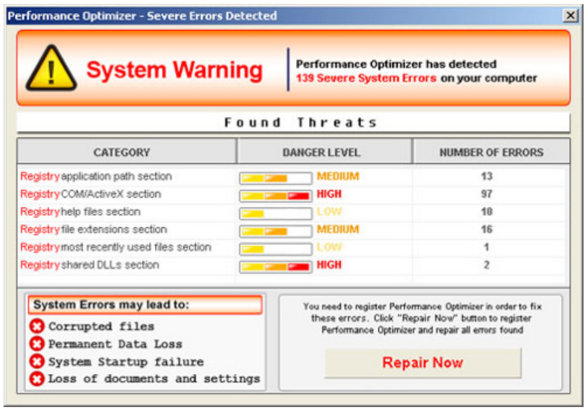
Click the 'Scan Registry' button to analyze your system.

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

These applications were quite unsophisticated and sometimes were 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 a challenge in itself.

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. The malware itself in its initial iterations 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.

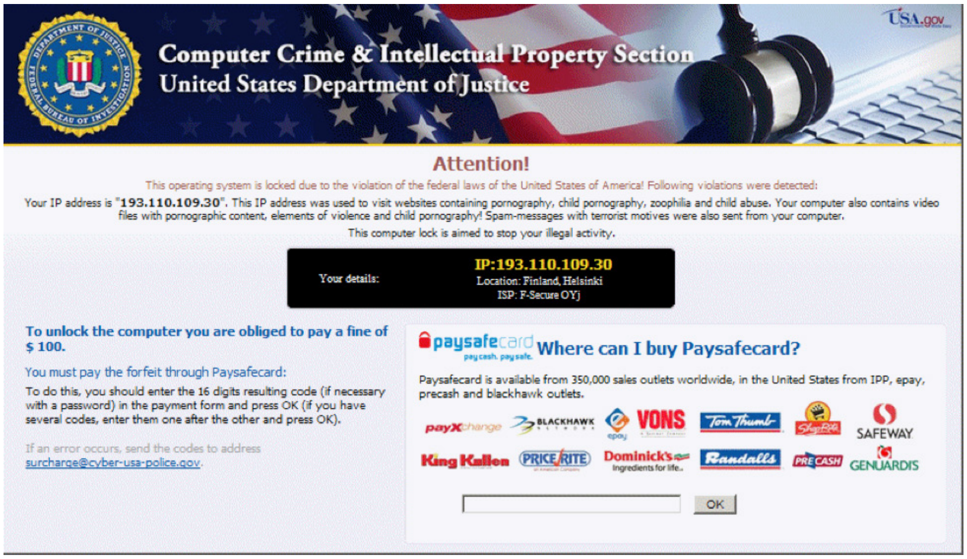
New GPCode variants attempted to be more effective at denying users access to their files by writing encrypted files to a new location and deleting the original file. This tactic proved ineffective as a simple "undeletion" or file restore utility would allow victim to recover their files. The final iteration 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.

While 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 Anti-Virus 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 of this type of ransomware 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 a victim access to their systems. No files were affected, but an infected user would be greeted with an apparently 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.

paysafecard paycash. paysafe. 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.

An easy payment of US$200 would, however, renew 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 from which to recover. 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

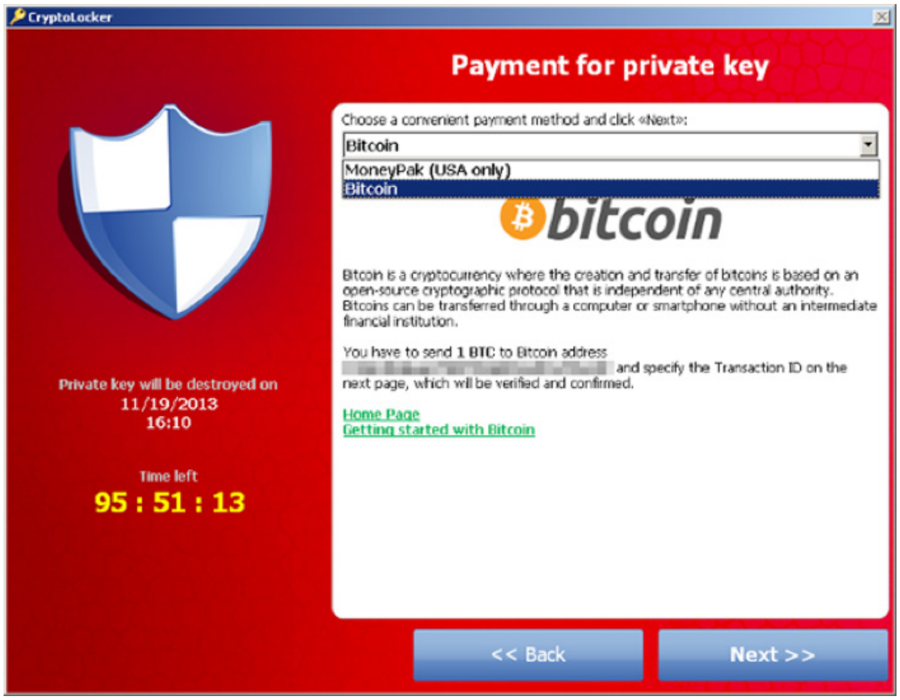
In late 2013, reports across the Internet began appearing regarding some sort of encryption-based malware that was infecting Windows-based systems. This malware would come to be known as CryptoLocker and prove to be a vanguard of the multi-million dollar crypto ransomware industry.

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 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 a lack of user awareness and social engineering to lure potential victims to launch the malware itself, although there was also some propagation via the Gameover ZeuS botnet as well.

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, in order to maintain persistence. Then, it would begin attempts to communicate back to a command and control server in order 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 was shown to the user indicating that the private key used for decryption would be destroyed, which, in effect, would cause the data to be lost forever if the ransom was not paid within 72 hours.



Choose a convenient payment method and click «Next»:

Bitcoin

MoneyPak (USA only)
Bitcoin

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.

Home Page
Getting started with Bitcoin

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

Time left
95 : 51 : 13

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 users who were affected by it, 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 used the experience of CryptoLocker as a launching point for numerous clones, bringing us into the Age of Crypto Ransomware.

Ransomware Today

Every week now we see new headlines describing organizations whose operations have been shut down or severely degraded by ransomware attacks. While 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 threat to organizations large and small today.

Unit 42 currently tracks thirty different crypto ransomware families in the Palo Alto Networks® AutoFocus™ 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.

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 also localization efforts, providing translated instructions based on the geolocation of a victim host's IP address.

What we are observing at this point is that 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 something that had not been observed previously in relation to ransomware on OS X.

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 the future we can expect to see the developments in ransomware that follow.

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" (IoT). While 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 $200 and $500, but the values can be much higher. If attackers are able to determine that they have compromised a system which 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 $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.

Defense Against Ransomware

While defending against a ransomware attack is not entirely different from 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 (i.e., not a connected USB drive). 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 or a user clicking on a link that downloads an executable. There are very few legitimate scenarios in which a user should be receiving an executable sent as an email attachment. Downloading executables through a web browser is also a rare event, which deserves additional scrutiny. Network security devices, such as a next-generation firewall, can identify these files when they are transiting 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 to ensure they will not be detected before deploying their malware. In order to protect your organization from these rapidly changing malware variants, organizations 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.

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

As there are currently at least 30 families of malware that hold files for ransom, and that list grows 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.

You can identify some ransomware using information included in the ransom note left on your system. Another option is to use 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 of 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

4401 Great America Parkway
Santa Clara, CA 95054

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

www.paloaltonetworks.com