WHITE PAPER

McAfee
Together is power.

Understanding Ransomware and Strategies to Defeat it

McAfee Labs

Table of Contents

Understanding Ransomware and Strategies to Defeat it

McAfee® Labs

Held Hostage in Hollywood: In February 2016 the Hollywood Presbyterian Medical Center, in Los Angeles, **paid a ransom** of about US$17,000 to hackers who infiltrated and disabled its computer network with ransomware. **The hospital paid the ransom** of 40 Bitcoins (currently worth about $16,664) after a "network infiltration" began on February 5, when employees reported being unable to access the hospital's network and electronic medical records system. "The malware locked access to certain computer systems and prevented us from sharing communications electronically," said hospital CEO Allen Stefanek.

Hollywood Presbyterian employees were forced to move back to paper and transmit information to doctors and others by fax machine while the IT team and outside consultants rushed to restore the network. Eventually, hospital officials decided that "the quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key," Stefanek explained. "In the best interest of restoring normal operations, we did this."

No one wants to be part of a story like this. What exactly is ransomware? Where did it come from? Why is it so pervasive? How can we help secure our computing resources today?

Ransomware History

It may surprise you to know that ransomware has been around for quite a long time. The first asymmetric ransomware prototypes were developed in the mid-1990s. The idea of using public-key cryptography for computer attacks was introduced in 1996 by Adam L. Young and Moti Yung in the **1996 Proceedings of the IEEE Symposium on Security and Privacy**. In the abstract, Young and Yung said their prototype was meant to show how cryptography could be "used to mount extortion-based attacks that cause loss of access to information, loss of confidentiality, and information leakage, tasks which cryptography typically prevents." Young and Yung presented a proof-of-concept cryptovirus for the Apple Macintosh SE/30 using RSA and TEA asymmetric block ciphers.

"It is said that if you know your enemies and know yourself, you will not be imperiled in a hundred battles;

If you do not know your enemies but do know yourself, you will win one and lose one;

If you do not know your enemies nor yourself, you will be imperiled in every single battle."

—Sun Tzu, The Art of War

Connect With Us

What does "asymmetric" mean and why does that matter? The defining characteristic of public-key cryptography is the use of an encryption key by one party to perform either encryption or decryption and the use of another key in the counterpart operation. In symmetric-key algorithms, there is a single key used and shared between receiver and sender, thus the key used by the receiver and sender is "symmetric" because it is the same. The use of multiple keys in asymmetric public-key cryptography allows ransomware to encrypt items on a system with a public key while never exposing the private key, thus keeping it secret. For ransomware, this is essential for "mangling" data files without exposing anything that someone could use to figure out how to undo the encryption.

Even though this first asymmetric ransomware prototype was well publicized, there was a logistical problem. How could the ransom be paid without exposing the malware author to risk? Send payments to a post office box? **The "AIDS" Trojan ransomware** author tried that and law enforcement officials tracked the money and arrested him. Thus until a usable ransomware "food chain" could be created, there wasn't much point in trying to leverage the idea of malicious encryption for making money.

As a result, things were pretty quiet until 2005, when GPCode, also called PGPCoder, was launched.

Timeline of Some Noteworthy Ransomware Familes

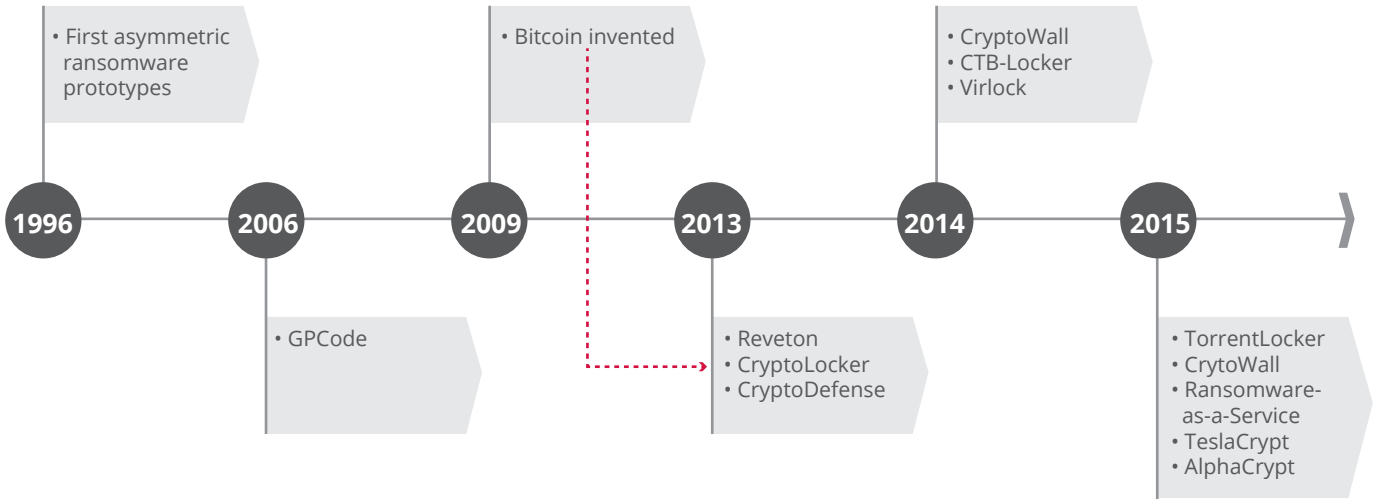

Figure 1. Ransomware proofs of concept are 20 years old, but the business really took off in the past three years.

It was a relatively simple Trojan encrypting common user files that matched the extensions matching those in its code. (These extensions included .doc, .html, .jpg, .xls, .zip, and .rar.) The Trojan would drop a text file that demanded payment in each directory with affected files. Back then, the payment was typically between $100–$200 in e-gold or a Liberty Reserve account. The security industry was able to come up with a variety of solutions to this Trojan (such as virus detection and utilities to combat GPCode). GPCode was considered modestly successful in that the malware author(s) behind GPCode and its variants were able to collect some money, but many variants had flaws (using symmetric encryption, deleting the unencrypted files in a way that allowed disk scanners to recover the files, etc.) that permitted users to recover data without paying the ransom.

CryptoLocker CopyCats

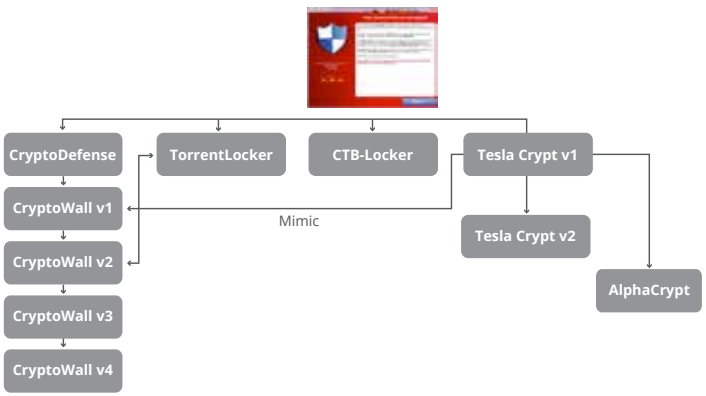

Figure 2. The incestuous nature of ransomware.

CryptoLocker was a ransomware Trojan that launched in September 2013. By combining capabilities such as more powerful asymmetric encryption methods and using the new cyber currency of Bitcoin as payment, ransomware started to really take off. (In Figure 1, we see a dotted line leading from Bitcoin to CryptoLocker, which was the first of a new generation of ransomware using Bitcoin for payments.) CryptoLocker was estimated to have earned its author $27 million in Bitcoin before it was shut down. Law enforcement working together with the threat intelligence community succeeded in taking down the botnet that was spreading CryptoLocker, but not before other malware authors saw the promise of CryptoLocker and spawned variants that persist to this day.

Many new variants of ransomware are directly related to CryptoLocker. As seen in Figure 2, CryptoLocker has spawned whole families of derivative ransomware, including CryptDefense, TorrentLocker, CTB-Locker, CryptoWall, TeslaCrypt, and AlphaCrypt. McAfee Labs has confirmed that code from CryptoLocker exists in all of these derivatives.

In summary, the success of CryptoLocker plus the combination of business models, digital currency, and evasion techniques has led to the pervasiveness of ransomware in today's threat landscape.

The World of Digital Currency Payments

This brings us to the subject of ransomware payment methods. The first payment methods for ransomware were e-gold and Liberty Reserve, as used by GPCode. E-gold was the world's first digital currency that was backed by hard assets of gold and silver bullion.

E-gold was shut down in large part because the US Secret Service caught wind of criminals using it to transact illegal commerce.

However, the invention of Bitcoin really sparked the imagination of the hacker community. Bitcoin is essentially a digital asset and payment system invented by Satoshi Nakamoto and released as open-source software in 2009. Bitcoin is the first decentralized digital currency. It is unique in that it solves a number of problems that plagued earlier attempts to produce this kind of currency.

- Bitcoin owners can prove they have funds without risk to the owner.
- There is no central bank or authority for the currency, which eliminates the ability of the currency's value to be manipulated by that authority.
- Transactions on the Bitcoin network are pseudonymous, meaning that although a currency transaction is announced on the network, there is no easy way to link Bitcoin account addresses to real-world identities, so the people conducting the transaction have a significant amount of privacy.
- Transactions are not location-specific, so currency can be seamlessly sent across borders.
- Basic transactions are irreversible. Once a transfer is made, there is no way for a third party to force a chargeback (as with a credit card).
- Here's the really clever part: There are no hard assets (such as gold) backing Bitcoin. Rather than relying on hard assets, Bitcoin miners use Bitcoin mining software to solve Bitcoin algorithms and earn Bitcoins. The algorithms are extremely hard to solve and require a lot of computation. Thus the number of Bitcoins being generated is relatively steady but low, similar to mining gold. **Here's a video about how it works**. (The ability to create value has led to "Bitcoin mining" malware, in which malware authors secretly take over your computer and force it to help solve the Bitcoin algorithms.)

These characteristics make Bitcoin very attractive to ransomware developers as a payment method for their schemes.

Why Ransomware Has Such Strong Growth

Massive Ransomware Growth

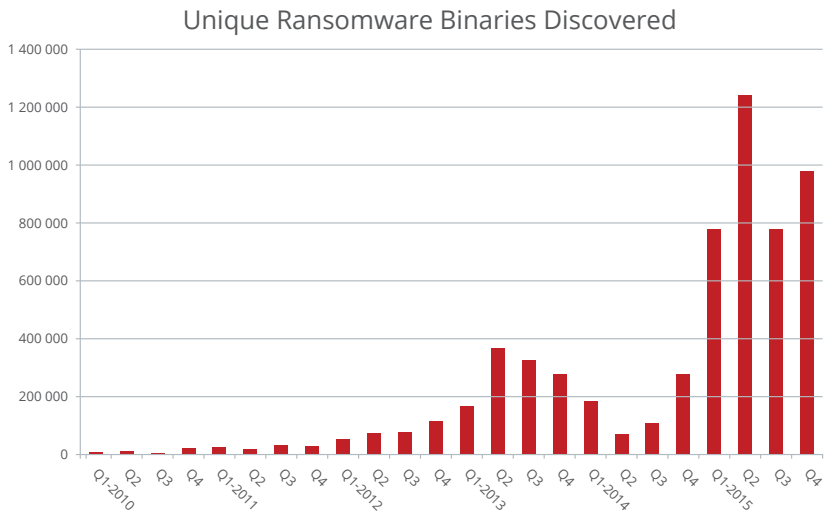

Figure 3. Ransomware grew considerably in 2015. Source: McAfee Labs, 2016.

McAfee Labs predicted this rise in 2014 based on trends in the Dark Web.

- Explosive increase in new, unique ransomware in 2015
- Affiliate programs make it easy for amateurs to earn thousands of dollars per week
- Polymorphic technique with minor changes leads to unknown malware and greater obfuscation

Looking at ransomware overall, McAfee Labs has measured a massive spike in new unique ransomware binaries starting in Q4 of 2014. This is due primarily to two things: Ransomware authors figured out how to make it ridiculously easy to get involved in the ransomware food chain; and ransomware authors have made it harder to detect ransomware binaries.

In Figure 3, we see that there was a spike of ransomware building to a peak in Q2 of 2013, and then dying down until mid-to-late 2014, when the pace picked up again. The initial surge, subsequent decrease, and then sustained surge can be explained: During 2013 and 2014, the security community was very good at working with each other as well as with law enforcement to identify specific ransomware threat families, tracking down how they were being distributed and how the control systems worked, and then shutting them down. That explains the initial peak and subsequent decrease in activity. Now let's look at why there is a sustained surge.

Starting in late 2014, ransomware toolkit authors opened up revenue sharing and created a lucrative, automated business model that has grown virally and is very easy to participate in. The financial rewards are significant. The affiliate programs generally split money (Bitcoin) 70/30 in favor of the affiliate. So for a $400 ransom, the affiliate will receive $280. You read that right: The script kiddie (distributor) makes more than the author. Why? Because the script kiddie takes all the risk, with payment credentials in the open, and they do the work of spreading the malware. (Some affiliates brag that they make $70,000–$80,000 per week.) According to the FBI's Internet Crime Complaint Center (IC3), more than 992 CryptoWall-related complaints were received between April 2014 and June 2015. During that period, victims reported more than $18 million in losses. Based on the McAfee Labs detection of unique ransomware binaries, we estimate that the value of losses on a rolling 15-month average will easily surpass this figure during 2015–2016. It is clear that the financial rewards are significant with the new business models. The other aspect of these affiliate programs is the notion of "Ransomware-as-a-Service."

Ransomware Authors Appeal to Affiliates

Figure 4. An example of Ransomware-as-a-Service.

"Ransomware-as-a-Service" means that the affiliate does not need any special programming skill, simply the willingness to spread the ransomware (typically through email botnets that are easy for a nonprogrammer to set up). The affiliate can sign up as an affiliate and simply download a customized ransomware binary (see Figure 4). The malware has custom payment instructions and

Advanced programming knowledge is not needed to distribute ransomware and become a criminal.

payment credentials and allows the affiliate to easily take part in the ransomware game. Some new variants of ransomware even have customizable malware actions. Check out these customization options from Ransom32, the world's first ransomware written in JavaScript:

- **Fully lock the computer:** By default the lock screen will pop up each xx seconds after being minimized. The affiliate can configure it so the victim will not be able to minimize the lock screen, further exacerbating the user's frustration.
- **Reduce CPU capabilities:** The ransomware will encrypt files at 0%–25% speed while the lock window is not shown, so the process will be less noticeable in the Task Manager due to high CPU consumption.
- **Latent timeout:** The ransomware will go into a dormant state and wake up, connect to the server, and start encrypting only after a certain number of seconds has passed after installing. The ransomware won't connect to the server until it wakes up, which allows ransomware to escape detection. This is a particularly nasty evasion technique, as it is simple and will fool many security sandboxing techniques that assume that malware will start its malicious activities immediately after installation.
- **Show lock screen before encrypting:** By default the ransomware will show the lock screen after encrypting many files in the computer (file size under 50MB) and will continue encrypting in the background. The affiliate can program the ransomware to show the lock screen immediately after installing, before encrypting any files in the background. Some affiliates feel that this gets results more quickly without having to wait hours or days for encryption to be mostly completed. The downside is that if the victim tries to check files just as the window pops up, he or she will notice that files are being manipulated in the background, which may cause the victim to take immediate action (stopping the program, shutting down the computer) thus making the ransomware less effective.
- **Show a message box:** This box will be shown before installing and before any latent timeout is applied.

Ransomware authors are now officially organized crime, and they have made it easy for wannabees and affiliates to participate in their crime wave and spread this malware.

Telemetry Tracks Revenues

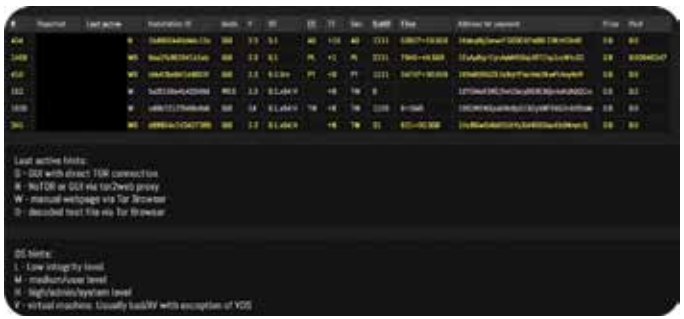

Figure 5. Ransomware offers sophisticated telemetry.
Source: McAfee Labs 2016.

The automated ransomware business model includes sophisticated tools such as the telemetry dashboard. (See Figure 5.) It reports all kinds of useful information, such as the price for the campaign, the amount paid per

binary, the operating system that is infected, time zone, and more. Affiliates now have detailed capabilities to see how effective their campaigns are and can tune their efforts to extract the maximum benefit for themselves without leaving the comfort of their homes.

Another reason for the growth in unique binaries is that ransomware authors now use polymorphism, a technique that allows ransomware to use a different, unique signature on each targeted system. Thus, one family of ransomware can theoretically create an unlimited number of unique ransomware binaries with a single ransomware toolkit and fuel the growth we see in Figure 3.

Polymorphism has been around for decades, and endpoint security technology can be highly effective against it. The main differentiator between technologies that are effective and those that are not is where the polymorphic engine resides.

- If the polymorphic engine is local (on the host or endpoint), then the engine activity can be analyzed and beaten in a straightforward way because the actions taken by the polymorphic engine can be observed on the endpoint.
- However, if the engine is on the server, then defeating the engine is more problematic because the engine is a "black box" in its actions.

The real explosion in ransomware binaries is from the family PolyRansom, which uses host-side polymorphism and can be defeated by strong signature-based antimalware. (Thus keeping your security content up to date is both effective and essential.) Although PolyRansom accounts for the largest number of binaries detected and the best signature coverage, it is not representative of what causes the most harm, which is families that use server-side polymorphism.

McAfee Labs researchers estimate that the millions of unique samples are derived from only 12 to 15 toolkits.

From a Few Come Many

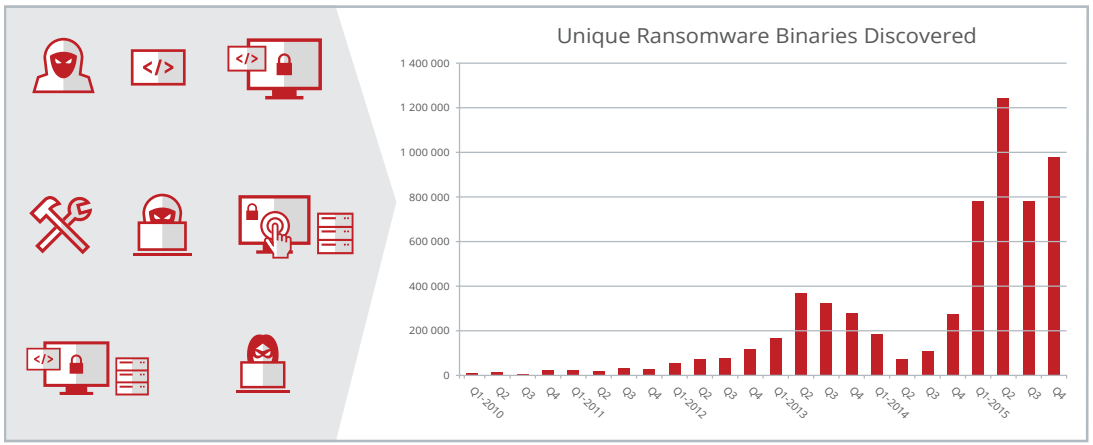

Figure 6. A handful of toolkits leads to millions of unique binaries.
Source: McAfee Labs, 2016.

Ransomware that employs server-side polymorphism does not prevent today's security from being highly effective, however. We will discuss a number of steps you can take to improve your current posture.

Here's an example of the effect of polymorphism. Figure 6 shows that although McAfee Labs detected millions of unique ransomware binaries in 2015, our malware research team estimates that only about 12 to 15 toolkits are responsible for all of these unique samples.

Primer: How Ransomware Works

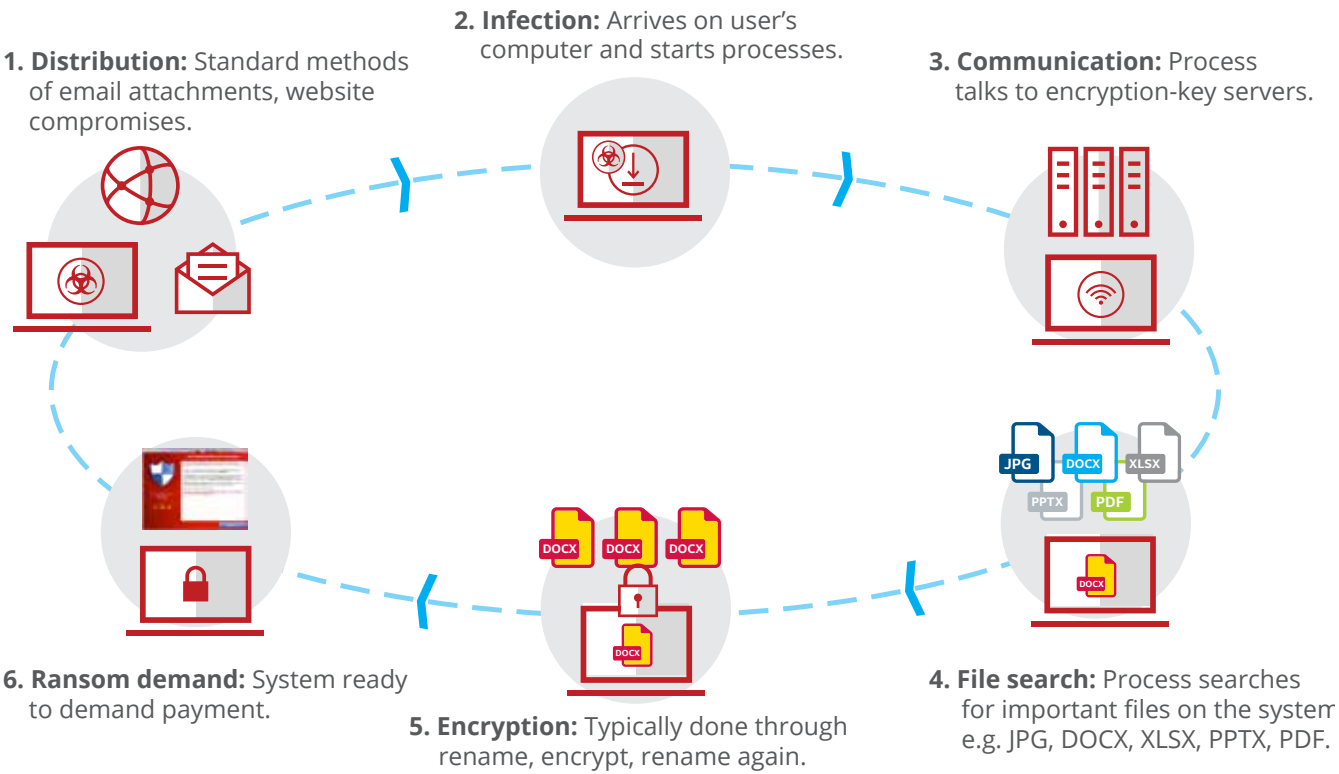

Figure 7. Ransomware follows a number of typical steps to success. Source: McAfee Labs, 2016.

We have described the technologies that ransomware leverages, and the business model and evasion techniques that fuel its growth and success. Let's take a look at the basic model of operation.

There are six steps that ransomware generally uses to accomplish its goals. (See Figure 7.)

The first step is distribution: Ransomware uses standard methods of distribution. Generally it is spread through phishing schemes involving email attachments or downloads and installs on an endpoint through website compromises. The old ways are still the best ways.

Figure 8. Examples of why phishing is so successful. Source: Verizon 2015 Data Breach Investigations Report.

Lest you think that this approach is old school and not effective, consider this: Almost one out of four recipients open phishing messages and, shockingly, more than one out of 10 click on attachments to phishing messages. In addition, nearly half of all recipients open phishing emails and click on the links within the first 60 minutes of receiving the emails. Despite all the corporate training, news articles, and public awareness, the "human operating system" is still the weakest link.

Drive-by downloads are still very effective as well. CryptoWall 3 uses compromised WordPress sites combined with the Angler Exploit Kit to invisibly direct a user's browser to a malicious website that hosts an exploit kit with ransomware. Attracting victims can occur with "malvertisements," or simply from a legitimate site that has been compromised.

The second step is infection. The binary arrives on the user's computer and starts the processes it needs to complete its malicious activities. These may include quite a bit of new, sophisticated behaviors. For example, CryptoWall 3 will do the following:

- Generate a unique computer identifier
- Ensure "reboot survival" by installing the program to run at start-up (through service entry, scheduled task, AutoRun key, etc.)
- Deactivate shadow copies, start-up repair, and Windows error recovery

- Stop Windows Security Center, Windows Defender, Windows Update Service, error reporting, and BITS
- Inject itself into explorer.exe and svchost.exe
- Retrieve the external IP address
- Then move to Step 3.

The third step is communications. The ransomware process will talk to encryption-key servers to retrieve the public key needed to encrypt data. CryptoWall 3, for example, connects to a compromised WordPress site and reports its status. All control server traffic is encrypted using the RC4 encryption algorithm.

The fourth step is file search. The ransomware process searches for files on the system in a systematic fashion. It typically looks for files that are important to the user and cannot be easily replicated, such as files with extensions of jpg, docx, xlsx, pptx, and pdf.

The fifth step is encryption. This is typically done through moving and renaming the targeted files, then encrypting and renaming the files after a successful encryption.

The sixth and final step is the ransom demand, typically through taking over the screen of the infected endpoint and demanding payment.

Figure 9. Example of a ransomware demand screen.

At this point, the user typically has no choice but to pay the ransom and hope for the delivery of a usable key to unlock the files, or pursue other remediation strategies such as an image restoration of the endpoint using a known-good snapshot.

The Latest in Ransomware Tricks

Ransomware authors have developed a number of clever tricks to make it hard to undo their work. McAfee Labs also predicts a few techniques ransomware developers may soon employ.

- **Name encryption:** The latest versions of ransomware now encrypt names of files along with each file's data. Encrypted files have names made up of random numbers and letters:

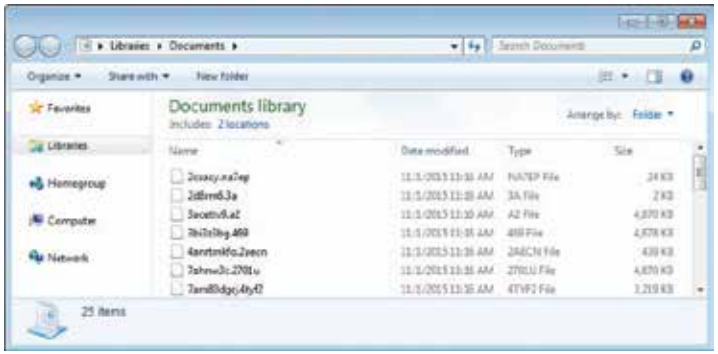

Figure 10. Encrypted filenames make finding important files just about impossible.

- **Backup and publish:** Some ransomware now claims that copies of the files have been moved to the attackers' servers and, if you don't pay, they will publish the files on the Internet.
- **PCs, and Windows, and websites:** Ransomware such as Linux.Encoder.1 will inject itself into websites with known vulnerabilities (such as shopping cart programs) and once on the host machine will encrypt all the files in the home directories and many of the directories referenced by typical websites (site images, scripts, code libraries, etc.).

Predictions from McAfee Labs

Delayed ransom demands: Ransomware will encrypt in the background, so that backup and archive programs pick up the encrypted files and overwrite the backups. Once the encryption key expires, both the data and the backups will be held hostage.

- **Hold the network hostage:** Ransomware will use worm technologies to spread and remain dormant before initiating encryption, using networks, using shares, etc. Combined with a Stuxnet approach, an attacker could hijack an entire network.
- **Encryption on the fly:** Ransomware will use kernel components to hook the file system and encrypt files on the fly as they are accessed by the user to ensure maximum damage.
- **Asymmetric encryption without the need for a centralized repository:** Ransomware authors realize that using a centralized repository for the encryption keys is a weak point in their strategy because it gives an attack point for security defenses. McAfee Labs predicts that we will see asymmetric encryption that does not use a centralized repository.

McAfee Malware Operations

What is McAfee doing proactively to shift the balance in the good guys' favor?

McAfee malware research:

- McAfee is working with law enforcement agencies on operations against a number of ransomware families. We can't tell you the details, but stay tuned. **Here's an example** of the kinds of things this effort involves.
- **Cyber Threat Alliance:** McAfee is one of the founding partners of the CTA and was heavily involved in an operation around the CryptoWall 3 ransomware family.

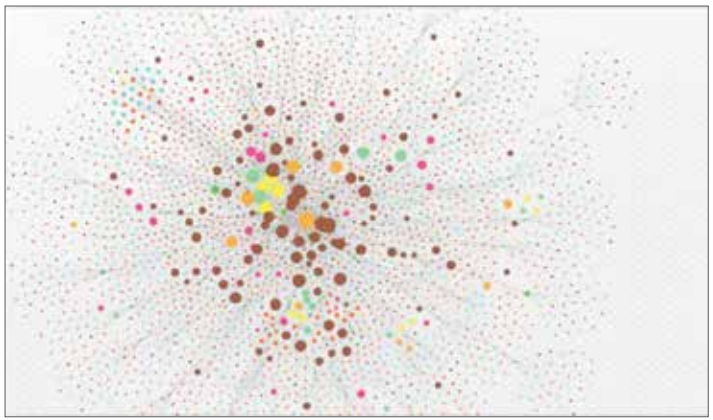

Figure 11. A connectivity map showing an example of ransomware research.

- Figure 11 illustrates an example of malware research. This connectivity map shows a combination of data around a ransomware family. The dots and lines indicate how a hash is associated with an IP address, which is hosted on a certain server, and the server is based in a certain country, and the location of certain Bitcoin wallets, and how many transactions took place with that wallet, and how the money was distributed, which email addresses are involved, and so on. The point of this image is to illustrate the massive complexity and spread of a single campaign. Here's what the research team found out:
  - The team monitored Bitcoin wallets involved from February–October 2015, and estimated an average Bitcoin "ransomware-paid" value during this time.
  - The actor group gained $30 million through the Angler exploit kit.
  - The total amount traced was about $321 million alone paid to infections.
  - The analysis of the transactions coupled with other data resulted in evidence of actors involved in multiple ransomware campaigns.
  - **Read the CTA report** that details how CryptoWall 3 works and indicators of compromise.
- **Proactive hunting:** The McAfee Labs malware research team hunts with several tools and systems explicitly for ransomware. In many cases, the team will manually analyze ransomware samples to determine how families are related (a bit like ancestry research, though ransomware is highly incestuous in its reuse of code). We also analyze spam and phishing campaigns for common traits and mechanisms. The team verifies whether a ransomware signature is up to date. For example:
  - When the team receives a ransomware sample, they also receive a notification that a sample was submitted.
  - The team checks whether we already have this sample. If yes, we ignore the sample; if no, the team ensures that the ransomware signature can detect the new sample, and we categorize the sample. (What family does it belong to? Is the signature successful at detecting it?)
- **Analysis of behavior and spotting new indicators:** This is basic analysis of new ransomware actions. For example, if a new ransomware family control server is detected, we pass this information to the threat intelligence team to ensure that McAfee protections act correctly when the new ransomware families show up on a network. The team employs multiple approaches, including:

- SSDeep
- Imp-hash
- Static analysis
- Dynamic analysis
- Memory analysis
- Machine learning

Primer: Ransomware Remediation Strategies

What can you do to protect your systems and networks? Let's take a brief look at a number of ransomware remediation ideas. We'll cover some basics and how they could be applied, emphasizing steps you can take today with current technologies or as general antimalware IT actions. (For example, an archival cloud-based backup is always a good defense against all malware.)

Understand how ransomware works.

- **The distribution stage:**
  - **Build a "human firewall":** The biggest threat is users who let the ransomware on their endpoints. People are the weakest link.
  - **Stop ransomware before the endpoint:** The most-proactive method of protecting a network from ransomware attack (other than the human firewall) is to keep ransomware from reaching the endpoint in the first place. Consider a web-filtering technology.
  - **Apply all current operating system and application patches:** Many ransomware strategies take advantage of vulnerabilities in the operating system or in applications to infect an endpoint. Having the latest operating system and application versions and patches will reduce the attack surface to a minimum.
  - **Spam filtering and web gateway filtering:** Again, the ideal approach is to keep ransomware off the network and the endpoint. Spam filtering and web gateway filtering are great ways to stop ransomware that tries to reach the endpoint through malicious IPs, URLs, and email spam.
  - **Allow only whitelisted items to execute:** Use an "application control" method that offers centrally administered whitelisting to block unauthorized executables on servers, corporate desktops, and fixed-function devices, thus dramatically reducing the attack surface for most ransomware.
  - **Limit privileges for unknown processes:** This can be done easily by writing rules for host intrusion prevention systems or access protection rules.
- **The infection stage:**
  - **Don't turn on macros unless you know what's happening:** In general, do not enable macros in documents received via email. Notice that Microsoft Office turns off autoexecution of macros for Office documents by default. Office macros are a popular way for ransomware to infect your machine, so if a document "asks" you to enable macros, don't do it.
  - **Make yourself "weaker" when working:** Don't give yourself more login power than you need. If you allow yourself administrator rights during normal usage, consider restricting this. Surfing the

To learn more about the role of social engineering within cybersecurity, read **Hacking the Human Operating System**.

web, opening applications and documents, and generally doing a lot of work while logged in with administrative rights is very dangerous. If you get hit with malware while you have fewer rights, you will reduce your risk because malware will also execute with fewer rights, which will reduce the threat's attack surface.

- **Use access protection rules on software installs:** Write access control rules against targeted file extensions that deny writes by unapproved applications. This complements host intrusion prevention systems rules with a similar strategy.
- **Use sandboxing for suspicious processes:** If a process is flagged as suspicious (due to low age and prevalence, for example), that process should be sent to a security sandboxing appliance for further study.
- **Block "unapproved" processes from changing files:** Block these by writing rules for host intrusion prevention systems or access protection.
- **The communications stage:**
  - **Firewall rules can block known malicious domains:** Writing rules to block malicious domains is a standard capability of network firewalls.
  - **Block access to Tor:** Tor is an anonymous Internet communication system based on a distributed network. Tor is a toolset for organizations and people who want to improve their safety and security on the Internet. Tor is also used by ransomware to obfuscate control server communications. For organizations that do not need access to Tor (and other anonymous Internet communication systems) administrators should consider blocking access to these unneeded networks. Current ransomware will stop if it can't establish control, so blocking Tor will cause ransomware that uses Tor to stop itself at the communications stage.
  - **Proxy/gateway scanner signatures for known traffic:** For those with proxy and gateway appliances, these technologies can be configured to scan for known ransomware control server traffic and block it. Most ransomware cannot continue operations if it cannot retrieve the public encryption key needed for asymmetric encryption.

The encryption stage:

- **Back up and restore files locally:** By creating a storage volume and running archival differential-based file backups to that storage volume, remediation is as easy as removing the ransomware, going back in time with the backup to a point before the ransomware affected the files, and restoring all the affected files. This can be done today by network administrators who could either use external storage volumes with a good archival backup utility or partition a local drive and run the backup utility against that.
- **Limit shared file activities:** Many ransomware variants will look for access to files on storage other than the boot volume—such as file servers, additional volumes, etc.—and will encrypt everything they can find to inflict maximum damage. Consider limiting operations allowed on shared volumes.

- **The ransom demand stage:**
  - **Restore from backup, keep a recent backup offsite and "air gapped":** Store a set of multiple, complete backups and assume an attack. An "air-gapped" backup is not connected to the computer or the network anywhere. (For an individual this could mean back up to an external hard drive. When the backup is done, unplug the drive and keep it in a drawer, away from any computers. That way ransomware cannot detect the backup and damage it.) Consider using a "bare metal backup" utility, which not only backs up your user files, but also lets you erase all storage volumes (in case the machine is stolen) and get you back to a usable state with all your applications and data restored.

About McAfee Labs

McAfee Labs is one of the world's leading sources for threat research, threat intelligence, and cybersecurity thought leadership. With data from millions of sensors across key threats vectors—file, web, message, and network—McAfee Labs delivers real-time threat intelligence, critical analysis, and expert thinking to improve protection and reduce risks.

www.mcafee.com/us/mcafee-labs.aspx

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com