SOPHOS
Security made simple.

CryptoLocker, CryptoWall and Beyond: Mitigating the Rising Ransomware Threat

By **Chester Wisniewski**, Senior Security Advisor

Ransomware is malware that prevents you from using your files or your computer, and then extorts money from you in exchange for a promise to unlock them. While forms of ransomware have existed for many years, this category of malware re-emerged in September 2013 in a form that is far more effective and dangerous.

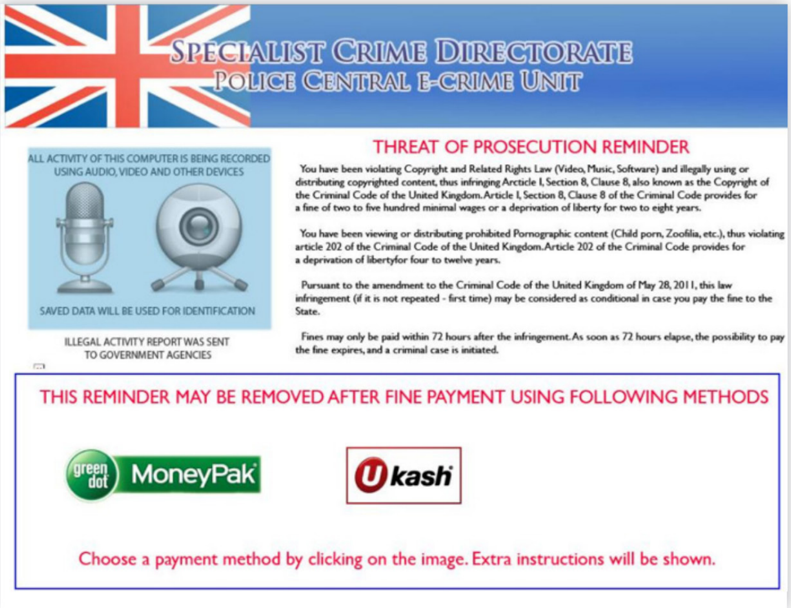
As criminals have learned how to construct and distribute highly-effective ransomware, they have built multi-million-dollar enterprises based on victimizing individuals and organizations. In this white paper, Sophos reviews the evolution and current state-of-the-art in ransomware, demonstrates how it works and why it is so dangerous, and — most important — offers specific recommendations that can dramatically reduce your vulnerability.

A Brief History of Ransomware

Many early forms of ransomware simply "locked" a user's computer and displayed a ransom message, instructing the user to send a code via text message to a premium-rate SMS number. The user would then receive a message containing an "unlock code," which — when entered — would allow them to use their computers again. The ransom paid was the cost of the premium-rate text message, which might vary widely, but was generally relatively low.

Later, variants arose — also locking the user's computer, but now displaying a full-screen message allegedly from a law enforcement agency, claiming that the required payment was a penalty for illegal activity such as violating copyright or viewing child pornography. Based on the user's IP address, the malware's authors would customize its message to reflect the user's language and local law enforcement authority. Now, the criminals typically demanded significantly higher payments, through online payment systems such as Ukash, Paysafecard, or MoneyPak: $100, £100, or €100 were common price tags. Once payment was made, users would receive a code via email that would unlock their computers.

These forms of ransomware — often called "PC lockers" or "Winlockers" (since they typically ran on Windows systems) — could be annoying and costly. They presented their ransom messages in full-screen windows that blocked access to other programs and left the computer unusable by anyone without unusual technical savvy. However, they were generally fairly easy for anti-malware software to recognize, prevent, and/or remove. Moreover, they rarely damaged user files; once removed by anti-malware software, the problem would be gone.


Specialist Crime Directorate
Police Central e-crime Unit

ALL ACTIVITY OF THIS COMPUTER IS BEING RECORDED USING AUDIO, VIDEO AND OTHER DEVICES

SAVED DATA WILL BE USED FOR IDENTIFICATION

ILLEGAL ACTIVITY REPORT WAS SENT TO GOVERNMENT AGENCIES

THREAT OF PROSECUTION REMINDER

You have been violating Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted content, thus infringing Arcticle I, Section 8, Clause 8, also known as the Copyright of the Criminal Code of the United Kingdom. Article I, Section 8, Clause 8 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

You have been viewing or distributing prohibited Pornographic content (Child porn, Zoofilia, etc.), thus violating article 202 of the Criminal Code of the United Kingdom. Article 202 of the Criminal Code provides for a deprivation of libertyfor four to twelve years.

Pursuant to the amendment to the Criminal Code of the United Kingdom of May 28, 2011, this law infringement (if it is not repeated - first time) may be considered as conditional in case you pay the fine to the State.

Fines may only be paid within 72 hours after the infringement. As soon as 72 hours elapse, the possibility to pay the fine expires, and a criminal case is initiated.

THIS REMINDER MAY BE REMOVED AFTER FINE PAYMENT USING FOLLOWING METHODS

Choose a payment method by clicking on the image. Extra instructions will be shown.

Figure 1: Winlocker ransomware

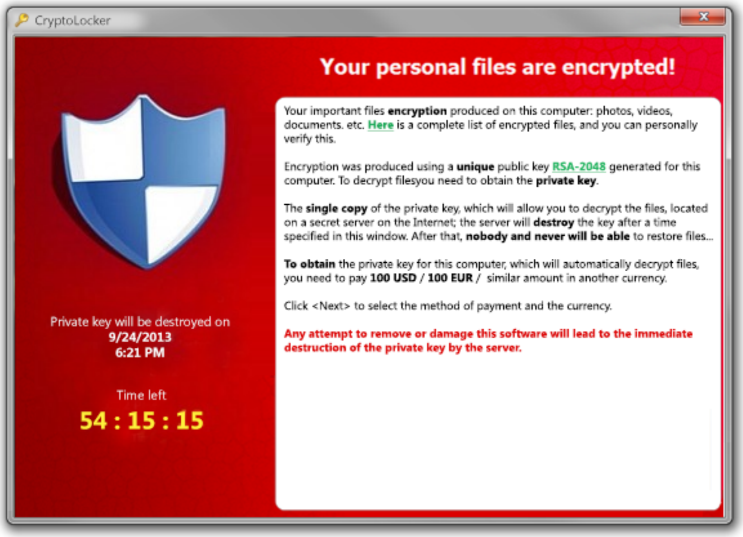
As recently as 2013, Winlockers were the most common forms of ransomware encountered by SophosLabs, perhaps because they were the easiest to create, distribute, and maintain. (And, over the past two years, we've seen Winlocker-style ransomware appear on Android smartphones: an example of how older patterns of PC malware seem to be recurring on newer mobile platforms.)

However, the newest versions of PC ransomware are far more sophisticated and dangerous. Now, the criminals encrypt all the files you care about. Moreover, they use industrial-strength encryption you can never overcome, unless you pay them a fortune for a key only they possess.

Encrypting Ransomware: A New Scourge Arises

With the rise of CryptoLocker in 2013, a criminal gang first demonstrated the ability to reliably combine remote encryption with remote extortion on a mass scale. CryptoLocker was taken down by law enforcement authorities in May 2014, and for the next several months, there was a significant reduction in the prevalence of ransomware.

However, CryptoLocker effectively offered a template for criminals who would follow. It not only showed how encrypting ransomware could be made to work: it also showed just how lucrative this malware business could be. According to US Department of Justice filings, CryptoLocker earned $27,000,000 for its owners in just two months. Researchers at the University of Kent estimate 1 in 30 people in the UK were attacked by it, and 40% of those paid.



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents. etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt filesyou need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR /** similar amount in another currency.

Click <Next> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

Private key will be destroyed on
9/24/2013
6:21 PM

Time left
54 : 15 : 15

Figure 2: CryptoLocker ransom warning

Since CryptoLocker's architecture and components are now well understood — and since many of its characteristics have recurred in more recent ransomware — it's worth walking through a CryptoLocker attack. We'll show you how it worked, which of your vulnerabilities it attacked — and where it, in turn, was vulnerable. Then, we'll show you how newer ransomware attackers have built on the CryptoLocker formula, while becoming even more elusive and dangerous.

CryptoLocker's Attack: Fiendishly Clever, Brutally Efficient

CryptoLocker executed its attack in five fiendishly clever and efficient stages:

1. **Installation.** CryptoLocker was often distributed through machines that had already been infected by Gameover Zeus, which itself was most often distributed through malicious phished email attachments telling users they had received a package shipment. Once installed, CryptoLocker would set keys in the Windows Registry to start itself automatically every time your computer boots.

2. **Contacting headquarters.** Before CryptoLocker (or one of its successors) could attack you, it needed to contact a server operated by the criminal gang that owns it. But where? How? CryptoLocker generated and visited 1,000 unique domain names every day, drawing on a prearranged list. Usually, it would eventually find a server that was up and running.

3. **Handshake and keys.** Next, the CryptoLocker client and server identified each other through a carefully arranged dance of actions on each side. Once they shake hands, the server would generate two cryptographic keys: one public and one private. It would send the public key to your computer, where it would be used for encryption. Until this public key arrived on your computer, encryption couldn't begin. The criminals would hold their newly-generated private key — required for decryption — on their own server. That key would never go anywhere near your computer — until you paid.

   Sophos disrupts this step of the infection process with the latest advance in our next-generation endpoint product: Malicious Traffic Detection (MTD). It has generally proven difficult for ransomware authors to establish and maintain new key servers capable of sending and receiving encryption keys. Sophos maintains a list of known destinations where encryption keys are being served in connection with ransomware and other malware. Our latest endpoint client will prevent computers from accessing these servers, thereby detecting the communication that must be established before encryption can begin. Since MTD runs directly on client systems, it protects users wherever they go — even when they are outside their corporate networks.

4. **Encryption.** With these cryptographic keys established, the CryptoLocker software on your computer would start encrypting every file it finds with any of dozens of common file extensions. It grabbed everything from Microsoft Office documents to AutoCad engineering drawings to that precious .JPG photo or .MP4 movie of your child's first step. Its creators systematically went after files you would find irreplaceable.

Infographic:
5 Stages of
a Crypto-
Ransomware
Attack

Download now

What's more, like their successors, they used the same industrial-strength AES-256 encryption security companies use to protect critically important data. (Sophos SafeGuard Encryption for Cloud Storage, for example, uses AES-256 to encrypt your data before you store it in the cloud.) Even the US National Security Agency finds AES-256 extremely difficult to break. You sure can't break it on your own.

(One reason industrial-strength encryption may become ever more ubiquitous in ransomware is that it is becoming much easier to apply. For example, Microsoft offers Windows developers standard cryptographic libraries they can use instead of crafting a less reliable and less effective solution entirely from scratch.)

5. **Extortion.** Next, the criminals demanded cash. With CryptoLocker, they would display a screen giving you 72 hours to pay up. The typical price: $300.

   If you didn't pay within 72 hours, CryptoLocker offered its victims one more opportunity to restore their files. You could upload an encrypted file to their secret server on the hidden TOR network. But, sorry, since you missed the $300 offer, decryption would now cost you several thousand dollars.

   Generally, people who paid CryptoLocker's extortionists did get their files back. But the criminals behind CryptoLocker didn't perform complete QA testing on the decryption portion of their software. Sometimes it just didn't work — especially if users tried to run anti-virus software after their files had already been encrypted.

There's a surprising coda to the CryptoLocker story. By now, most of those victimized by CryptoLocker have long since paid the ransom, found old backups, or given up and abandoned the files they lost. However, when law enforcement took down CryptoLocker's servers, it found the secret keys that the criminals were charging their victims for. Two security vendors have established a site, https://decryptcryptolocker.com/, that enables CryptoLocker victims to see whether their own keys can be found; if so, their files just might be decryptable after all. If you're ever victimized by ransomware, you might want to keep a copy of the encrypted files around just in case law enforcement ever finds the keys — but we certainly wouldn't count on it.

CryptoWall 1.0, 2.0, and 3.0: The Next Generations

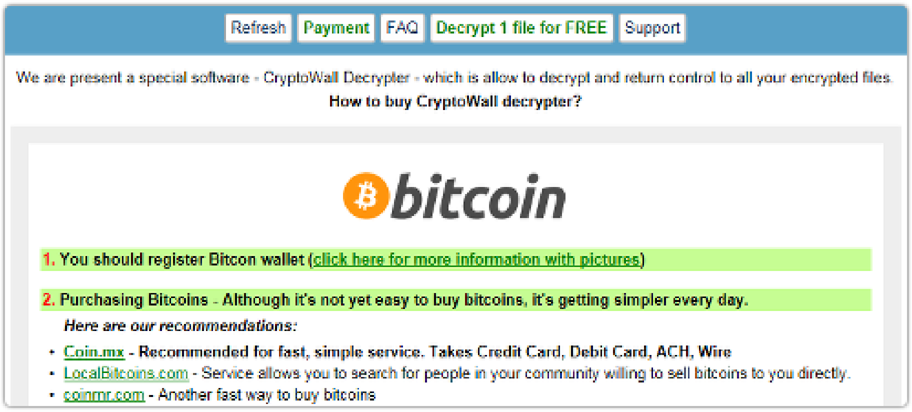
CryptoLocker was the state-of-the-art in ransomware in early 2014, when it was disabled by international law enforcement. But it didn't take long for other criminals to steal its approach and attempt to build new global extortion rings of their own. The most successful of these attacks quickly came to be known as CryptoWall.

First observed in spring 2014, CryptoWall grew explosively in May and June, and was reportedly a million-dollar business by August, spreading through web exploit kits, phished emails, and corrupted attachments and PDF files. By the end of 2014, a new version, dubbed CryptoWall 2.0, had become distressingly widespread. While CryptoWall infections were originally found mostly in the UK and US, they have rapidly grown in Australia, as well as non-English speaking countries such as Spain, Turkey, and Germany. In January 2015, yet another version appeared, suggesting that the criminals are becoming quicker to learn from experience and enhance their malware: CryptoWall 3.0.

Each version of CryptoWall has followed the five-step infection process described earlier in this paper; some have been delivered by Web exploit kits as well as phished emails. However, CryptoWall 2.0 and 3.0 have featured innovations that made them more effective and elusive.

For example, CryptoWall 2.0 establishes command-and-control through servers on the hidden Tor network, designed to make all traffic anonymous. To facilitate communication with its victim, it uses a web-to-Tor gateway, or offers to let its victim download a Tor browser. CryptoWall 3.0 uses a different approach to anonymity: a peer-to-peer anonymity network based on the I2P protocol.

These steps, of course, make it far more difficult to trace the servers running the network, as well as the criminals' payment instructions to victims. Further complicating the process, CryptoWall 2.0 and 3.0 now demand payment in Bitcoin — making it more difficult to trace the payments and requiring users to learn how to use this electronic form of currency.



We are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files.

How to buy CryptoWall decrypter?

1. You should register Bitcon wallet (click here for more information with pictures)

2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

- Coin.mx - **Recommended for fast, simple service. Takes Credit Card, Debit Card, ACH, Wire**
- LocalBitcoins.com - Service allows you to search for people in your community willing to sell bitcoins to you directly.
- coinmr.com - Another fast way to buy bitcoins

Figure 3: CryptoWall pay page

From the criminals' perspective, these enhancements are a double-edged sword. Ransomware's Achilles heel has long been the need for two-way personal communication with its victims: criminals must communicate payment instructions, and victims must deliver payment. By using technologies like Tor, I2P, and Bitcoin, CryptoWall's owners make their chain of payment more anonymous and resistant to criminal investigation.

However, they may also make it harder for victims to pay. Users must first learn how to use Bitcoin. In some cases, they will also have to learn how to manually install and use a Tor browser, too. It will be interesting to see how the criminals manage this tradeoff between security and greed: will they eventually make payment easier, and thereby make detection by law enforcement easier?

Additional recent CryptoWall enhancements have demonstrated that ransomware gangs are learning from the best practices of other malware authors. For example, like some other malware we've seen, CryptoWall 2.0 first probes your computer to determine if it's running in a virtualized sandbox. If so, this might be a signal that it's being studied on a security company's computer. If it recognizes a sandbox, it won't install its full malware package; instead, it shuts down and erases itself.

Other Variants: Innovations in Crime

While CryptoWall is currently the most widespread version of ransomware we encounter, it's not the only one.

For example, Sophos recently detected W32/VirRnsm-A, a virus that isn't limited to spreading solely through e-mail or browser vulnerabilities. W32/VirRnsm-A infects files and changes them to .exe files that can run as programs. It still permits the user's file to open initially, increasing its opportunity to spread. After some time, however, it locks the user out of his or her files. In contrast to CryptoWall, files infected with W32/VirRnsm-A can usually be recovered.

We've also seen versions of encrypting ransomware that store encryption keys locally, avoiding the need to communicate with a remote key server (but also making it theoretically possible for a user to recover his or her own files without paying).

The point is: ransomware criminals are still actively exploring and innovating, determining what will work best for them — and cause you the most misery.

How to Protect Yourself

Since encrypting ransomware has proven extremely lucrative, we believe it will be an unfortunate fact of life for years to come. This means you need to protect yourself. Fortunately, you can. Here's how:

1. **Keep backups!** Backup media are cheap now: a $20 thumb drive can save plenty of precious files and images. Nowadays, there are plenty of easy-to-use online options, too. Remember two important points, however.

First, most current ransomware will attempt to encrypt files on all connected drives you can access, even across the network. If you leave your backup drive permanently connected, it might encrypt your backed-up files, too. If possible, disconnect that drive when your backup is complete. (Ideally, you should store it off-premise or, failing that, in a secure location on-premise.)

Second, if you use an online backup service, keep in mind that most of these services automatically check to retrieve the latest versions of your files. If the latest version has been encrypted, it might replace your usable file with the encrypted version — and that won't do you any good. Check to see if your service offers the option to store the last several versions: this will help you preserve copies you can actually use.

2. **Patch, patch, patch.** The vast majority of vulnerabilities used to deploy ransomware are old. Patches exist for them. Make sure you have a system (preferably automated) for deploying them. If the underlying software (e.g., Windows XP, Office 2003) is no longer being patched, maybe it's time to upgrade.

3. **Use stricter access controls and user privileges.** Simply telling Windows that programs can't run from your AppData folder will halt plenty of malware in its tracks. Restrict write permissions on file servers as much as possible, and don't give people more rights than they need. Use administrative accounts sparingly, and when user roles change, adjust their permissions. If your users aren't admins, ransomware can only encrypt their own files. If they are admins, ransomware can roam your network encrypting everything their accounts can access.

4. **Stop spam.** Anti-spam software is frontline defense. Tools like Sophos Secure Email Gateway aren't quite perfect, but they're stunningly good at blocking messages with links to websites infected with exploit kits that deliver drive-by downloads.

5. **Use advanced web, network, and endpoint protection.** Before ransomware can do its dirty work, it must contact a live command and control server. Up-to-date next-generation firewalls such as the Sophos UTM can help block that. So can today's best client anti-malware software. Sophos's next-generation endpoint protection offers Malicious Traffic Detection (MTD) that goes wherever you go, detecting and stopping malware when it connects to attackers' servers.

6. **Keep anti-malware up to date.** Best-in-class client anti-malware software such as Sophos Endpoint Protection, kept up to date, can usually detect and block ransomware executables before they ever run. Features like host-based intrusion prevention system (HIPS) offer an additional line of defense, recognizing patterns of behavior associated with malicious applications.

7. **Make sure you've actually turned on the security features you've paid for.** (This may sound obvious, but you'd be surprised!) For example, if you're using Sophos Endpoint Protection managed by the Sophos Enterprise Console, enable Live Protection, HIPS Behavior Monitoring, and Web Protection.

8. **Immediately isolate infected devices.** If one user finds that the files on their computer have been encrypted, immediately remove that computer from the network until it has been fully cleaned.

9. **Continue educating your users.** For example, remind them not to open unexpected file attachments, and to contact IT if they encounter a file or computer behavior that seems suspicious.

The Best Defense: Next-Generation Enduser Protection

Next-Generation Enduser Protection is the integration of Sophos's innovative endpoint, mobile and encryption technologies to deliver better protection and simpler management. From malicious traffic detection integrated into the endpoint to cloud-managed policies that follow users across devices and platforms, we're redefining what it means to provide comprehensive enduser security. And as we continue to innovate, you'll benefit, as it becomes easier than ever to provide sophisticated protection for your users and data.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA

SOPHOS