1. Collaborators: Ashley Hansberry, Allan Lasser, Andrew Tarrh
2. Sources: See final page

Cryptolocker: 2013's Most Malicious Malware

by Ashley Hansberry, Allan Lasser, Andrew Tarrh

Over the last six months, a new computer virus has emerged, turning encryption schemes upside down, kidnapping your files, and demanding a hefty ransom for their recovery. This virus, accurately named *Cryptolocker*, surfaced shortly before the holiday season in 2013. When it did, news of the virus spread like wildfire through the computer security and IT communities.

Cryptolocker is classified as ransomware[1], malware that demands a sum of money after restricting a user's ability to access their computer or files. Using a combination of social engineering and technical expertise, the malware became a media sensation when news outlets began to report on victims like the Swansea Police, whose sensitive files were held hostage until the police themselves had no other choice but to pay $750 to unlock them.[2] Yes, tax dollars are funding cyber criminals. In spite of the police department's attempt to discourage payment of the ransom, many businesses (the police force included) are forced to do just that, because their data is so valuable. Even more alarming is the method of payment. The criminals demand payment in Bitcoin, using encrypted transactions. Bitcoin's anonymous transaction system means the criminals cannot be caught. For these reasons, a CBS News article called Cryptolocker "the perfect crime."[3]

It's worth noting that the main targets of Cryptolocker, and ransomware in general, are businesses. The trojan version of Cryptolocker disguises itself as UPS and Xerox PDF attachments, while the newer worm version can traverse internal networks and travels on USB drives. The Cryptolocker encryption specifically targets professional-class file types, like Word, Excel, Photoshop, and InDesign, while ignoring music and video files. As ABC News points out[4], personal files just aren't valued as highly, or seem more easily replaceable. It seems like businesses are the obvious target since they place a much higher value on their data and are more likely to pay the ransom, since they have higher incentives and the cash to pay.

The attack begins once a malicious email attachment is downloaded and a ZIP file, disguised as a PDF, automatically runs and downloads the malware. It will save itself with a random filename in the root file system with a user's other applications. Once active, the malware first establishes a connection with

[1] A thorough overview of ransomware is available from Symantec at http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf

[2] http://boston.cbslocal.com/2013/12/18/cryptolocker-ransomware-being-described-as-the-perfect-crime/

[3] We noticed in this same article, WBZ-TV correspondent Joe Shortsleeve described the malware as a phishing scheme, which is incorrect. Phishing is an attempt to steal user data such as usernames, passwords, or credit card info by tricking users into volunteering their personal information. Cryptolocker acts in an entirely different manner.

[4] http://abclocal.go.com/kgo/story?section=news/technology&id=9415487

the attacker's control server.[5] While early versions of Cryptolocker had static IP addresses hard-coded, newer versions use a domain name generation algorithm to connect to what looks like a random domain name. Random strings like "xeogrhxquuubt.com" and "qaaepodedahnslq.org" were found to be active in September 2013, but these change rapidly. The algorithm works by generating a pseudorandom string based on the time or date. With the algorithm, it is trivial for the hackers to decide which domains they should make active on any given day.

Once connected to an active server, the malware begins a key exchange protocol using public key crypto. Requests and responses between the malware and the server are done via RSA encrypted HTTP POST commands. The malware already contains the server's 2048-bit RSA public key when it is downloaded. It uses this public key to encrypt a request for a unique, machine-specific encryption key to be used later. Along with this request, the malware sends along some information about the machine it is running on, including the malware version, system language, and a numeric ID. After the server has decrypted this message with its own 2048-bit RSA secret key, the server generates the key response. Its response includes the victim's IP address and a unique RSA public key. It is only then that the file encryption begins.[6]

In what system admins on various forums have recognized is alphabetic order,[7] the malware begins looking for specific filetypes in directories and mapped network drives. For each matching file found, there is an intricate encryption process. First, the malware generates a new 256-bit key to use in AES encryption of the file. AES is the Advanced Encryption Etandard and is a symmetric key crypto system—it encrypts much faster than 2048-bit RSA. The AES key is used to encrypt the contents of the file. Instead of storing the key somewhere else, the malware encrypts the AES key using the unique RSA public key received in the key exchange. Each RSA-encrypted AES key as well as the AES-encrypted file contents are saved back to the file.

To decrypt the file contents, the infected user needs to receive the secret RSA key that corresponds to the user's unique private key. Brute force decryption of the files without the decryptor is not feasible due to the 2048-bit RSA encryption. After payment via Bitcoin or Moneypak is verified, the Cryptolocker server looks up the corresponding secret key. It is not known exactly how this process works, but it is clear that the server stores some information about the user's unique ID and their public key in order to look up the secret key. The server sends an automated decryptor to the infected user that already contains the secret key. For each file, the the secret RSA key is used to decrypt the AES key

[5] http://blog.emsisoft.com/2013/09/10/cryptolocker-a-new-ransomware-variant/
[6] http://www.bleepingcomputer.com/virus-removal/CryptoLocker-ransomware-information
[7] http://www.reddit.com/r/sysadmin/comments/1p32lx/cryptolocker_recap_a_new_guide_to_the_bleepingest/

stored in the file. The decrypted AES key is then used to decrypt the file contents.[8] The decryptor automates this process for the infected system. Depending on the number of files on the system, the decryption process can take many hours.

Cryptolocker is mostly spread by email, so prevention is not especially difficult. Modern antivirus software provides ample protection from the virus; a warning will pop up if a user attempts to run the executable, and the user would have to ignore warnings from their anti-virus program in order to install Cryptolocker on their system. Although many popular anti-virus software can prevent the malware from executing, the only way to reverse the encryption is to pay the ransom for the secret key. One tactic some system administrators have used, as described in a discussion thread on Reddit[9], to detect the malware's presence in their network is to create a honeypot. The honeypot, a directory that would be visited alphabetically-first by the malware, would be populated with garbage data and monitored for access. If the honeypot directory is ever accessed, this means a Cryptolocker attack is likely occurring. The honeypot would continue to generate garbage files to trap the malware until an administrator could take control of the infection. This is considered a last-ditch security measure, after other defenses like email monitoring and antivirus software have failed (this technique could, of course, be subverted by changing Cryptolocker to access directories in random order). The nefarious design of Cryptolocker, though, means it will likely bypass these initial safeguards, leaving very few options for prevention.

Cryptolocker's main consequence is economic. Victims of the malware must determine whether or not their data is "worth" the demanded ransom. For all the ransoms that are paid, Cryptolocker's authors profit handsomely: at minimum, they have already collected tens of thousands of Bitcoin ransoms (which, at current conversion rates, is tens of millions of US Dollars)[10]. It is not an outrageous assumption that Cryptolocker, and other ransomware virii, are used to fund more nefarious malware schemes.

However, *Cryptolocker 2.0*, a new software by (allegedly) different authors, is more nefarious. For one, it operates as a worm instead of a trojan. This means it replicates and installs itself across computers, instead of disguising itself as an email attachment. Suddenly, whole internal networks can be compromised by a single Cryptolocker 2 infection. Further, while computers are infected and the malware is waiting for the notice of a paid ransom, it will turn the infected machine into a botnet node. This botnet participates in distributed denial of service (DDoS) attacks and, more notably, Bitcoin mining. Now, the attackers are mining their own Bitcoins while waiting to receive the Bitcoins of others! Cryptolocker 2.0

[8] http://www.bleepingcomputer.com/virus-removal/CryptoLocker-ransomware-information
[9] http://www.reddit.com/r/sysadmin/comments/1mizfx/proper_care_feeding_of_your_cryptolocker/ccp17kr
[10] Statistics supported by Symantec (fn:1), and a link to a Bitcoin account from a Reddit thread.

shows that ransomware is beneficial enough for its authors (and, conversely, harmful enough to its victims) to warrant a continued investment in the software.

Cryptolocker is a security researcher's dream, but a computer user's nightmare. The malware's careful combination of domain name generation, public key cryptography, symmetric key cryptography, and even machine takeover makes it a major threat. The United States Computer Emergency Readiness Team (US-CERT) issued an official statement in November 2013, warning the public about Cryptolocker and providing an outline of their suggestions for preventing and dealing with ransomware infection.[11] The damage of Cryptolocker attacks on even the most valuable machines can be mitigated by paying careful attention to downloads and remedied by frequently backing up data. With education and prevention the only real solutions, it seems as if Cryptolocker and other malware of its kind are here to stay.

[11] http://www.us-cert.gov/ncas/alerts/TA13-309A

1. Collaborators: Ashley Hansberry, Allan Lasser, Andrew Tarrh
2. Sources: See final page

Sources

- http://www.us-cert.gov/ncas/alerts/TA13-309A
- http://www.reddit.com/r/sysadmin/comments/1p32lx/cryptolocker_recap_a_new_guide_to_the_bleepingest/ccyffbf
- http://www.reddit.com/r/sysadmin/comments/1mizfx/proper_care_feeding_of_your_cryptolocker/ccp17kr
- http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf
- http://boston.cbslocal.com/2013/12/18/cryptolocker-ransomware-being-described-as-the-perfect-crime/
- http://en.wikipedia.org/wiki/Phishing
- http://abclocal.go.com/kgo/story?section=news/technology&id=9415487
- http://blog.emsisoft.com/2013/09/10/cryptolocker-a-new-ransomware-variant/
- http://www.bleepingcomputer.com/virus-removal/CryptoLocker-ransomware-information
- http://www.reddit.com/r/sysadmin/comments/1p32lx/cryptolocker_recap_a_new_guide_to_the_bleepingest