Locky: The New Face of Ransomware

Jeanna Long

East Carolina University

ICTN 4040 601/602

Those of us in the Information Technology (IT) field all know what ransomware is. It is a type of malicious software that blocks access to a computer or computer system and demands payment, “ransom”, to have access to the computer system again. Over the years, ransomware has evolved and become more malicious.

It started out in its infancy as what is now being called scareware. Scareware is a type of malicious software that tried to “scare” or create anxiety in users that their computer has become infected with malware or viruses in hopes that they will purchase unwanted software. This software can be bogus and non-functioning or it can be malware. The next generation of ransomware is Lockscreen ransomware. This was designed to keep a user from being able to use the computer until a ransom was paid. Fortunately, users were generally able to boot the computer into recovery mode, download a program that will find and uninstall the malware so the computes can be used again.

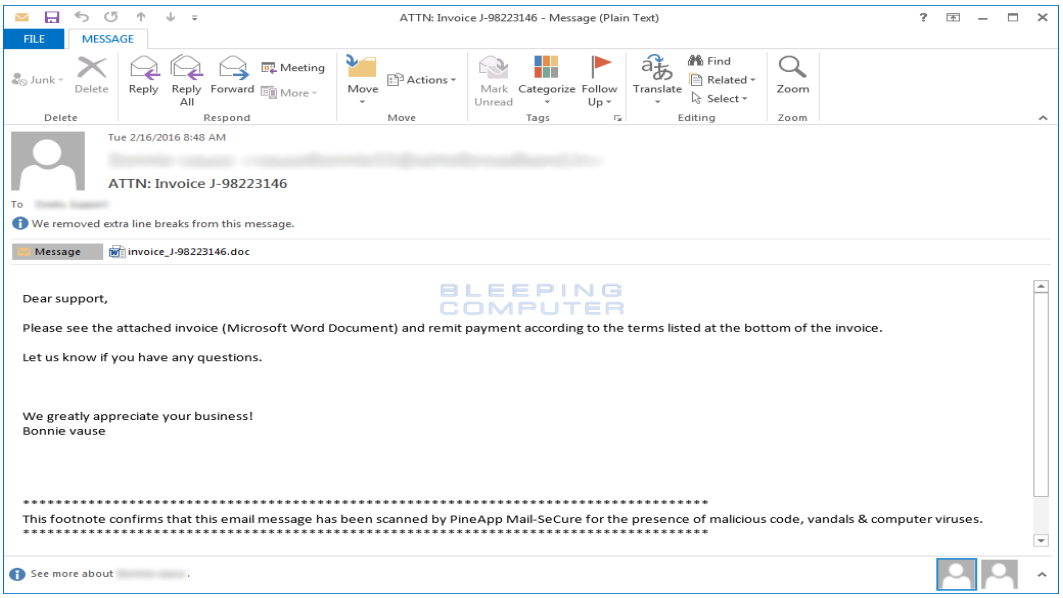
The latest ransomware epidemic is encrypted ransomware. Ransomware authors create the software to encrypt system’s files on the hard drive or act less malicious by only locking the system and displaying messages to try to force the user pay the ransom. The focus of this article is encrypted ransomware named Locky. According to Wright (2016), “The latest strain of ransomware sweeping workplaces is called Locky: It locks, scrambles and renames all of your files, giving them the extension ".locky."” I chose this virus specifically because it has recently been wreaking havoc at my place of employment.

The authors of Locky at this time are unknown, but John Leyden who writes for *The Register* has called them “greedy miscreants”.

Locky was constructed to use AES-128 encryption to encrypt a user's data. Once the data has been encrypted, the user receives a demand for bitcoins as payment to have access to their data again. (AES is an encryption algorithm that uses block cipher to encrypt text.) With this method data is encrypted in blocks instead of bits. By encrypting blocks of data instead of bits it lessens the chances unencrypting without a key since identical or similar blocks of data will not be the same. The key that is generated to encrypt these blocks is the same key used to unencrypt them. Once the data in a victim's files are encrypted it scrambles the file names and renames them. All the new scrambled files end in a .locky extension.

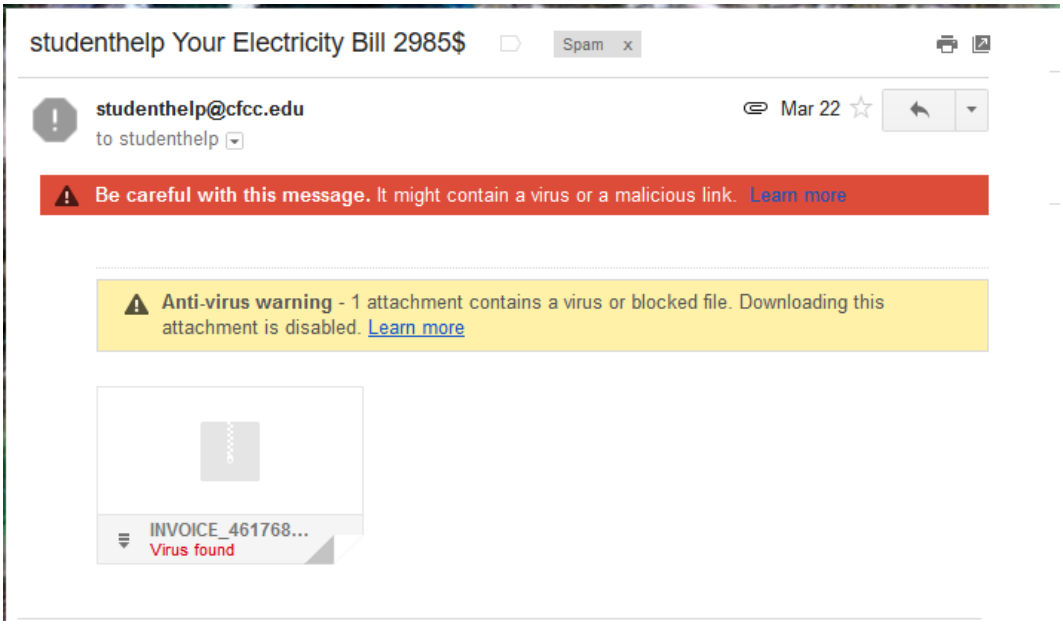
The next step in the process is for Locky to delete the computer's shadow copies. (Shadow copy is a feature of Microsoft Windows.) This feature allows the computer to take automatic or manual snapshots of the computer's files or volumes. This is done even when the computer is in use. With Locky deleting these files there is no option of recovering anything that is not backed up in another location and not attached to the infected computer.

Locky starts its attack by email. In my place of employment, we began seeing a number of incoming emails that contained these attachments. There were a variety of them. The first to be received were "invoices". Once someone downloaded the "invoice" Locky would open a document with a message telling the user that if the invoice does not appear properly to download macros to correct it. Downloading macros does not change the appearance of the document but it does download an executable that is Locky. Once downloaded, Locky starts encrypting files. Below is an example of one of the emails.



Locky "Invoice" email. Image from www.bleepingcomputer.com.

At my place of employment, the IT department sends out emails anytime numerous incoming spam emails are detected. When IT noticed the "invoice" emails coming in, an email was sent to all users with a warning not to open any attachments if they were not expected. Users were further instructed that if an attachment was opened in error, not to download macros even if prompted to. Unfortunately, there were a few people who did just that and subsequently infected their computers. (The picture below is one we received at the helpdesk. Before it was marked as spam there was no indication it was malicious.)

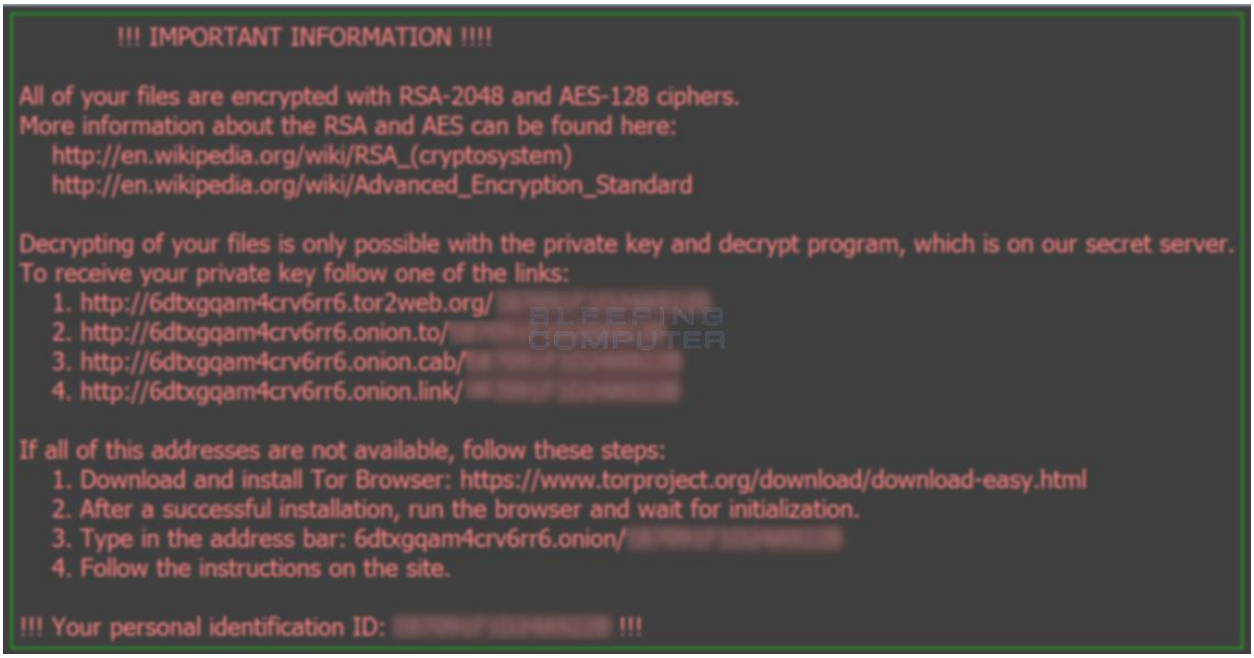


When IT received an alert that a virus had been detected, they confiscate the computer, re-image it, and restore any files that are backed up. This would be the end of the issue until another virus was downloaded. Locky, unlike previous ransomware viruses, attacks more than just mapped files on local drive. Abrams informs us in his article "It is important to stress that Locky will encrypt files on network shares even when they are not mapped to a local drive." It also infects any external drives attached to the computer and bitcoin wallets.

At some point the virus finds its way from someone's computer to the shared drives even if those shared files were not mapped on their computer. Since Locky infects the unmapped shared network files, regardless of point of entry, the IT team must remove all access to the shared drive server for a day. During that time the encrypted files are replaced with the backed up copies. There were over 30,000 encrypted files on the shared drives. At that point the emails had decreased in volume but unfortunately .zip files were coming through and finally pdf attachments. Even after numerous emails from IT staff, an employee opened and downloaded a pdf sent from their email address and infected their computer.

Once Locky has encrypted files on the computer, a ransom note is generated. It presents itself on the desktop and has 3 sections to it. The first section informs the user that all of their files have been encrypted and even list the types of encryption used: RSA-2048 and AES-128. It even provides link to the Wikipedia pages for these encryption types. The second section states you can only decrypt your files with the private key and decrypting program on their secret server. The perpetrators provide 3 links to choose from to get the key and program. These links are for a Tor site, Locky Decrypted Page. There are steps on the Tor site

that walk a user through the process of paying the ransom. The third section provides steps to take if the above links don't work. The last item listed is the user's personal identification ID.



Locky wallpaper. Image from bleepingcomputer.com

When presented with the ransom note, the user has a couple of options. They can give in and follow the links and directions to pay the ransom, or they can try to recover the files themselves. If a user decides to pay the ransom they must pay with bitcoins. At this time one bitcoin is worth $400. Locky authors are charging 0.5 to 1.00, $200 to $400, bitcoins to have access to the original files. In order to purchase bitcoins, a bitcoin account must be created. This account connects to a method of payment for someone to purchase the number of bitcoins desired. Once the user has purchased the bitcoins they follow the instructions and pay.

If the files have been backed up the user can remove the virus by various methods, and replace the encrypted files. Currently there is at least one program with which a victim can attempt to recover the encrypted files called Recuva.

There are a few ways to avoid becoming infected with Locky.

- Back up files stored on your computer regularly
- Have security software installed on your computer and kept up to date
- Keep the operating system and other software programs updated
- Ensure all patches are installed if software is not kept up to date
- Treat emails with caution if they contain attachments. Delete or spam any suspicious emails.
- Educate other email users about email risk such as not opening attachments unless they know who sent them and they were expecting the attachment
- Be very cautious of emails that ask to have macros enabled
- If macros will not be needed, disable them.

If macros cannot be disabled, an alternative is provided in an article by Nadia Kovacs. "If you are unable to disable macros, you can also try using Word Viewer by Microsoft. Word viewer will allow you to view a Microsoft document, however, it does not support macros, therefore will not run them."

At this point numerous businesses and organizations have been hit by Locky. These include schools, hospitals as well as city offices. There have been at least two hospitals that have been impacted by Locky. Methodist Hospital in Henderson, Kentucky, received a ransom note demanding four bitcoins, ($1600) to gain access to their decrypted files. This was a minimal amount compared to the ransom demanded from Hollywood Presbyterian Medical Center. "Hollywood Presbyterian Medical Center, the Los Angeles hospital victimized by ransomware, ended up paying out ten times the amount demanded of Methodist Hospital to regain access to its systems." (Gallagher, 2016) Now the concern of the ransom demand

amounts increasing is growing quickly. Some suggest not to pay the ransom since it encourages the malicious behavior. Melendez, (2015) “When victims make ransom payments, it provides validation to the attackers that their ransomware operations are successful. The ultimate goal of these attackers is to make as much money as possible.”

Locky is a sophisticated ransomware virus that spread rapidly. It is clear from the makeup of it that the authors are quickly finding ways to exploit vulnerabilities in software, computer systems, and people. The authors of Locky have demonstrated their greed and disregard for people’s wellbeing by attacking medical facilities and in at least one case drastically increasing the amount of the ransom demand. The viciousness of this ransomware is a prime example of why people and businesses should always take measures to protect themselves. Follow the rules of having a security software installed, backup often, update and patch all software often, and always take great caution if with emails with attachments.

References

Wright, A. D. (2016). Locky ransomware virus sweeps U.S. businesses. *HRNews,* Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1766271688?accountid=10639 *

Abrams, L. (2016, February 16). The Locky Ransomware Encrypts Local Files and Unmapped Network Shares. Retrieved April 01, 2016, from http://www.bleepingcomputer.com/news/security/the-Locky-ransomware-encrypts-local-files-and-unmapped-network-shares/

Kovacs, N. (2016, February 18). New Ransomware Variant Locky Spreading Like Wildfire Since the Day It First Appeared [Web log post]. Retrieved March 01, 2016, from https://community.norton.com/en/blogs/norton-protection-blog/new-ransomware-variant-Locky-spreading-wildfire-day-it-first-appeared

Gallagher, S. (2016, March 23). Kentucky hospital hit by ransomware attack. Retrieved April 01, 2016, from http://arstechnica.com/security/2016/03/kentucky-hospital-hit-by-ransomware-attack/

Melendez, M. (2015). *Ransomware: An analysis of a growing threat landscape* (Order No. 1605452). Available from ProQuest Dissertations & Theses Global. (1752223374). Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1752223374?accountid=10639*