“How Safe are Your Files?”: A Survey of Ransomware and its Characteristics.

William Berry, Garrett Cole, Glen Pringle, Macoony Cambron, Andrew Hoban, Daniel Bonaparte
William.Berry, Garrett.Cole, Glen.Pringle, Macoony.Cambron, Andrew.Hoban, Daniel.Bonaparte@email.saintleo.edu

ABSTRACT
Ransomware has been harming the industry as a whole for over 16 years. It has cost millions of dollars around the world as it is mostly nearly impossible to revert once you have been infected with most Ransomware. Currently there are a few strains of ransomware that are developing. This paper will take a look at the history of Ransomware as a whole and take steps to prepare users to defeat it.

Categories and Subject Descriptors
D.3.3 [**Cyber security**]: Viruses, Trojans

General Terms
Trojans, Ransomware, Encryption, malware.

Keywords
Trojans, Ransomware, Encryption, CryptoLocker.

I. Introduction

The advent of new computer technology has changed the aspects of information technology completely. With increasing amounts of data being stored on servers and on networks, criminals have moved to target this data and withhold the availability of it from the rightful owners through blackmail. One of the ways that criminals can execute this is a type of malware called ransomware. In this paper, a thorough review and examination of the background of ransomware will be done in order to ease understanding of a complicated subject. Understanding the modus operandi of the malware will follow, with a relevant example and case study of Saint Leo University. Finally, an attempt to track the future of ransomware will be done.

II. History

Ransomware is a type of malware that is used to lock a computer remotely. After the computer is locked, a pop-up window generally appears requesting a sum of money to regain access to the computer once again. There are multiple ways in which ransomware can be installed, like other malware: email attachments, bad links, or even social media sites. (Microsoft). One of the first versions of ransomware was discovered in Fall 2013, named CryptoLocker. This version of ransomware used asymmetric encryption methods; it required both a public and private key that are used for data verification and decryption to lock the user files on the computer (Trendmicro). CryptoLocker spawned newer versions and many copycats; however, CryptoLocker was disable after the U. S. Department of Justice seized the malware’s connected server in June 2014 (Trendmicro). A newer ransomware has been discovered and it is called Onion. The Onion ransomware uses Tor network and elliptical curve cryptography to avoid being detected. Laptops and desktops are not the only devices affected by Ransomware; in June 2014, the first account of Ransomware was discovered on the Android mobile platform. It has affected users in 13 different countries. The mobile ransomware originates from a Trojan known as Pletor which is being sold on the black market at $5,000. Though hope is not lost, Kaspersky Lab Researcher Roman Unuchek, has stated that all versions of this ransomware so far have a key that can be used to decrypt affected files (Trendmicro).

The first known ransomware was written by Joseph Popp in 1989, where it was called the “AIDS” Trojan. The creator only asked for $189 to be paid to the PC Cyborg Corporation in order to unlock the system. It wasn’t until May 2005 that extortion ransomware became prominent around the world. In 2006, worms like Gpcode, TROJ.RANSOM.A, Archiveus, Krotten, Cryzip, and MayArchive began utilizing more sophisticated RSA encryption schemes, with ever-increasing key-sizes.

In 2008, Gpcode.AK bust upon to the computer scene, and in 2013, with the propagation of CryptoLocker which began the use of Bitcoin digital currency to collect ransom money, revitalized the ransomware threat. ZDNet estimated from October 15 to December 18, 2013, the operators of CryptoLocker had collected about 27 million dollars from infected users. In August 2010, Russian authorities arrested ten individuals that were using a new ransomware worm known as WinLock that would displayed pornographic images, and the users to send ten dollars to get the key to unlock their machines. With WinLock running across Russia and all nearby countries, it was reported that the group made over 16 million dollars. In 2014, the Trojan-Ransom.32.Onion came to prominence.

III. Statistics

Below are the infection statistics as of July 20, 2014. Most attempted infections took place in the CIS, while there were individual cases recorded in Germany, Bulgaria, Israel, the United Arab Emirates and Libya. Trojan-Ransom.Win32.Onion was detected in the following countries:

Country	Number of users attacked
Russia	24
Ukraine	19
Kazakhstan	7
Belarus	9
Georgia	1
Germany	1
Bulgaria	1
Turkey	1
United Arab Emirates	1
Libya	1

The included graph shows a 24 hour period around the world in 2014 with just the Trojan-Ransom.Win32.Onion. The number of users attacked was actually much greater than the stats suggest because this stat was just for one verdict. Kaspersky Lab found an unknown number of samples also proactively detected as products of "PDM:Trojan.Win32.Generic". The data is not included into the statistics above.

As reported by Trend's Smart Protection network cloud, the US headed the list with just over 2,000 infections, ahead of Germany on 1,203, and Hungary on 561. Other countries reporting in the hundreds include France, Russia, Australia, Italy and Taiwan. After existing at very low levels for years, ransom attacks suddenly started to spike in mid-2010.

IV. Modus Operandi of Ransomware

Ransomware typically installs itself on a user's computer surreptitiously. It can be received from a variety of different vulnerable areas, including malicious executables, open ports, or unsecured networks. After being installed, the program will then run its payload and begin its encryption. As it does this, it does not allow the user to access their own files by this encryption, and will not allow them to access them until a fee has been paid. This violates the availability and integrity of the files. It is difficult to halt the spread of ransomware as it propagates. Some ransomwares will not encrypt immediately, increasing the difficulty of determining the source of the infection. Even Saint Leo University was not free from the clutches of ransomware.

There were a pair of incidents regarding ransomware at the Saint Leo campus. The two separate events were months apart. Examining how the computers were infected and how they evaded protection, we see that these users voluntarily downloaded and installed the programs. At the time, Saint Leo did not have an IDS active anti-virus program installed on the host machines. Firewalls were unable to block this traffic because it came through the allowed HTTP port 80 on both cases. The next section will examine this attack more closely.

V. Real-World Examples

Saint Leo University has been subject to two Ransomware attacks in recent years. The first infection failed due to remediation efforts on the part of the user of the system and the hard drive was not recovered until two weeks after the original infection, leaving the ransomware ample time to employ it's effects. At this time, the files were already encrypted with a 2048 bit RSA encryption. The drive was flashed, and reset – and the ransomware propagated itself again on the new drive. This is a statement to that strain's tenacity and self-sustainability.

The second infection's source date was determined through forensics to have been acquired via advertisements on Facebook. This proves the deleterious effect of a simple misclick, which may result in a harmful experience. The active user that was also not the assigned personnel to the device; however, it is not believed that said individual intended to inflict harm on the system.

Speaking with Mr. Overton, CISO at Saint Leo University, he recommended an increased amount of awareness and being proactive with data– as proactive as possible. "Once your files are encrypted, that's it. There's nothing more [that can be done]." He stated. "In order to attempt to decrypt your files – I need to know the encryption used and then it make take a considerable amount of time to decrypt by force." He continued to say. It is imperative that users practice good security habits in everyday use. Mr. Overton also advised to never pay any ransom – it may decrypt your files but your computer will remain infected. "It just shows the hacker that you're willing to pay. They know you're a good target now. Expect an encryption to happen again in a month. Maybe a week. Maybe a day. Maybe this afternoon." He continued. Also of note is that the delivery system for the infection may have been removed – however it is irrelevant once your files have been encrypted. This is due to files already having been encrypted, and the delivery system no longer being needed save a reminder that you have little time before the key is deleted to the encryption.

Protection against ransomware should start at home – regardless of the place the infection took place. Mr. Overton pushed heavily into that any work on a USB drive could easily transfer the infection to a home computer to a networked business location. He recommended investing and getting an active anti-virus – which will help the user monitor against make mistaken downloads. Furthermore, he recommended frequent backups of all important documents you have – citing that backup drives generally only cost around $50 for more space than most users could use on just documents.

Another example of the devastation ransomware may incur is in Austrailia[SEE BELOW - #1], where the Australian broadcasting service was disrupted by a computer that had acquired a strain of CryptoLocker, and was forced to move their broadcast to another location until the issue was resolved. This begs the question: what can we do to remove the infection when you have your files encrypted? You can pay the ransom – which is not recommend. As stated – your files could easily be encrypted again. We have not found evidence of this happening, but it's certainly a possibility that anyone willing to make a living encrypting your files would break a "code of honor" and encrypt your information again after payment.

It is not possible at this time, with anything short of a supercomputer to recover data once it's been encrypted by a 2048 bit encryption.

VI. Prevention of Ransomware

Currently, the only defense against ransomware attacks is to be proactive in backing up any important data. The underlying principle is not to put all of one's eggs in one basket. This needs to be done regularly, with the frequency dependent on how sensitive the most important data is to changes. However, setting a daily or real-time backup may be counterproductive. For, if the backup drive updates to the changes made by the ransomware, then the data may be lost for good. One sure way to be prepared for that contingency is to make sure that one's backup software has the ability to store and recall previous versions of a file.

These dangers apply just as much to data stored on cloud computers as much as they do to data stored on local machines. In this situation where one's primary data is stored on the cloud and work is done there, the solution is reversed. Instead of storing the backup drive on a cloud, it would be stored on the local machine (or possibly even another cloud drive.) The more independent copies of personal data that a person owns and regularly maintains, the less susceptible he/she is to a ransomware attack.

VII. Law Enforcement's Involvement

According to the FBI, "ransomware" is something that has become a lot more common over the years, in which attackers have been infecting people and businesses around the globe. When an individual is targeted by ransomware, there are precautions that must be made before ultimately deciding to get any kind of law enforcement involved. While some may claim that the best course of action is to immediately contact the police, it's actually recommended that individuals not contact law enforcement right away. This is because, once the police are brought in to solve a ransomware case, then the victim's computer system, and everything in it, become open for law enforcement to view. It's important for individuals to understand that they have the right to disclose any personal information and files that lie in their computer, and that once law enforcement are involved those rights go out the window.

Now for some people, this may not be an issue, but for other's this may prove to be an irritating result of being a ransomware victim. Any kind of non-disclosure agreement one may think they hold, is no longer a factor when police are called in to solve a ransomware case. Ironically, common ransomware techniques involve attackers impersonating law enforcement by stating that the victim has been viewing illicit material online and that they must pay a certain fine to avoid persecution. Unfortunately, this intimidating situation often results in the victim feeling as though they have no choice but to give in to their attackers. More recently, a local police department in Swansea, Massachusetts paid attackers approximately $750 after a ransomware attack left hundreds of files encrypted and locked up by the malware on police computer systems. Many claim that it is wise for ransomware victims to ignore such threats and not give in to such extreme demands. This approach is much easier said than done. In most cases, business, with no other recourse, tend to just pay the ransom to retain their files so they could just go back to work. The department had to pay the attackers in Bitcoins so that they'd be given the correct key to decrypt their files. "The virus encrypted several files that could only be decrypted through the purchase of Bitcoins, an unregulated digital currency, to pay for the special decryption key" (Fraga). With the Swansea Massachusetts police department, they concluded that this issue would be best settled if the ransom was paid. Despite the department's belief that paying the attackers was the way to go, it certainly doesn't look good on their part considering that they're law enforcement and probably shouldn't give in to threats. The fact that the department went on to eventually pay the attackers just goes to show that sometimes involving law enforcement isn't the best choice, but rather one must ensure their computers protection with the proper anti-virus software.

References:

Online Safety. (n.d.). Retrieved April 13, 2015, from http://www.microsoft.com/security/resources/ransomware-whatis.aspx

The history of ransomware: From CryptoLocker to Onion. (2014, August 1). Retrieved April 13, 2015, from http://blog.trendmicro.com/the-history-of-ransomware-from-cryptolocker-to-onion/

Overton, David. "Ransomware with David Overton." Personal interview. 4 Mar. 2015.

Ragan, S. (2014, October 7). Ransomware attack knocks TV station off air. Retrieved April 12, 2015, from http://www.csoonline.com/article/2692614/malware-cybercrime/ransomware-attack-knocks-tv-station-off-air.html