CryptoLocker

A Siege is a tactical assault that surrounds a fortified place in a way to isolate it from help and supplies. Sieges involve taking key points to weaken the target in order to take over. In a way this is what the malicious ransomware; CryptoLocker does to any computer it infects. Just think that of your computer as the battleground, and your money as the target. "The word ransomware and the associated phenomenon appeared something like 3 years ago, around the year 2005. It shed light on a specific class of malwares which demand a payment in exchange for a stolen functionality." (Gazet 77-80). Ransomware usually comes in three different varieties, scareware, screen locking, and encryption. Scareware is just as the name says, and it used to scare someone into thinking that they have malware on your computer. Scareware, calms you have a problem, and ask that you pay a fee in order to remove the problem. They are the most common, and are usually just popup ads that you can just close. They may stop you from using the computer, but it really depends on what kind of Scareware infected your computer. The second type of ransomware is when malicious software locks up your screen and prevents you from using the computer or limiting your access. They way said that you have illegal material on your hard drive or that the FBI what to confiscate your computer. This types of malicious software can be difficult to remove, and may require a special removal software. However, most up the time if you can get your computer to boot into safe mode and run anti-virus software, then you can remove it. If that does not work then you would try a system restore to return system files and programs to the state they were before they got infected. The last type of ransomware is when you data become encrypted, and the keys to unlock it are unattainable. This type is the most severe, because your personal data may be lost forever. This type of ransomware will encrypt personal data when it infects a computer. Each of the different types will uses different

encryption methods, but they all asks for money in exchange for the keys or passwords to unlock the data. One of the newest and most effective ransomware is called CryptoLocker, and it will be the main focus of my paper.

CryptoLocker is a ransomware program that started to appear around September 2013 and effect all current version of Windows There are different reports on the exact number of people who have been infected by CryptoLocker since it releases. In November, over 35,000 computers were confirmed to have had a run in with CryptoLocker, and there are reports the numbers may be higher. The way CryptoLocker spread is through corrupted websites, and emails sent to company email addresses that pretend to be about issues from FedEx, UPS, and other shipping companies. The subject line of the emails would say that you have missed a package or that it was a payroll invoice or even a voice message. The emails would have zip file attachments that would infect the computer if they were downloaded, and open. In the zip files are executables files that are disguised as PDF files. They have a PDF icon that looks very convincing, and can be hard to misjudge as fake. Once they are open, it may use a Trojan called Zeus to connect to a bot control server to install CryptoLocker to avoid decoction. There are also reports that it can be passed by flash drives and can be found on file sharing site as of early this year. It being changed and re-engineered by the author so it may change again in the future.

When CryptoLocker is install on the computer, it become infected, and it will save itself as a random named filename to root of a directory .It then creates an auto start entry in the registry to start when you login. CryptoLocker then attempts to delete any shadow volume copies on the computer to prevent using them to recover data. Then it will connect to a live command and control sever that it gets the address from a domain generation algorithm. This is where it gets public and private keys. CryptoLocker uses an asymmetric encryption, which

means it uses the public key to encrypt data files, and the private key is used to decrypt the file. The public key is stored on the local computer in the registry text, and the private key is kept on the server. It then starts to encrypt certain files that are on the local machine. After getting the keys it CryptoLocker then scans and tries encrypt files associated with Open Office, Microsoft Office, and images. It does not scan system files that are critical for Windows' to function, only files that could be consider personal or work related It will also try to move to any network drives that are mounted to the network and try to encrypt them as well. After it scans, and encrypts the data, it will then display a message which offers to decrypt the data. It will ask a payment of $300 in Bitcoins or a Money Pack voucher within 72 hours, and it threatens to delete the private key if the deadline is met without a payment. You can extend the deadline if you change the clock in the BIOS settings in the computer, but the private key may still be delete. If the initial deadline is not met, the malware then offers again to decrypt data by directing you to an online service by the malware's authors. The cost becomes higher in Bitcoin, and current this is no way to decrypt the data without the private key, It's not recommend by security professional to pay for the private key, but the data cannot be access with the key. There have been reports of people paying and not receiving there private key, and people have been given the wrong key.

Removing CryptoLocker is not very difficult, and could be done it a few simple steps. Also, removing CryptoLocker will not decrypt any files that were encrypted, and will not prevent a future attack unless you change some policy setting. In order to remove CryptoLocker all you have to do is download the lasted version of Malewarebytes, and install. Then you should shut down your computer and run it in safe mode. From safe mode you would then open up Malewarebytes and run a quick scan. You should also unplug the Ethernet cored, and disable any

wireless communication on the computer. This will prevent it from going over to other drives on the network, and may interrupt some communication between the server, preventing any more files from being encrypted. Another way to remove CryptoLocker is to use a program called CryptoPrevent. When used, it will beef up a computer software restriction policy path rules to prevent another CryptoLocker attack. It will also remove the ransomware from the computer. There also may be a way to recover some of your lost data. CryptoLocker deletes shadow files that are used to restore files. For one reason or another, sometimes CryptoLocker will not be able to delete all of shadow files. This will allow you to uses a shadow copy snapshot to restore some files. A program called shadow explorer will help restore complete flooders that have been encrypted by CryptoLocker. When the program is open it will list the entire list shadow copy snapshots on your computer, and if it has any you can replace the encrypted file with the shadow copy. This method is not guaranteed to work, but it worth. The only truly way to prevent a CryptoLocker attack is to have an off side data back-up that can be put replace the encrypted files, and to have anit-virus software in place to help prevent an attack monetize

The damage cause by CryptoLocker can be very high, and hard to measure. Some things like family picture and other personal data are hard to monetize. About 250,000 users total have had to deal with CryptoLocker and at $300 to decrypt the data, it's estimated that the developers have made well over 27 million dollars. $300 hundred dollars is very steep for personal data, and it seem right now is the only way to get your data back. There is no way for a person to crack this type of encryption. It also seem like its development process is not slowing down. Unless the new variants have been seen by other then it would be impossible for you to protect self with anti-virus software. It takes a sometimes for anit-virus software to get the necessary updates to protect against the newest threats. Lucky we know how CryptoLocker spreads and thorough that

we can prevent computer becoming infected. Currently, the most common way that it is being spread is by fake email, and best way to protect against to be able to spot a CryptoLocker email. It's also a good idea to not open attachments from people you don't know, and don't open the email from about missed packages when you have not even place any kind of order. "Even sophisticated exploits may fall back on using tried-but-true techniques, like using spear-phishing and social-engineering tricks. "Even as technology evolves, the weakest link will always be the human operator in front of the keyboard," he says. "The majority of the advanced attacks in 2013 began because some user clicked on a link in an email or unintentionally visited a malicious website." (Epper 18-23) CryptoLocker does note exploit a hole in the security it just targets the weakest link, which is the user, so education about the issue would be the best defense.

CryptoLocker to me seems like one of the worse infection you can get on a computer. To me it likes a big taunt to know where you data is, and not be able to get to it. The developers of CryptoLocker are worst kinds of thieves. They target people, and business that are venerable to this attack and they hold their data hostage and demand money for it release. CryptoLocker is very preventable and it not difficult to get rid of, but it cost peoples millions of dollars and still causes major technical outages if company gets infected. I think the reason it does so well is going for irreplaceable information on the system, and it puts it just out of reach from our grasp. As long as the hardware is working you can re-instil operation systems and we can always change passwords or move account if they get hacked. But we can't do much about lost personal documents. They are the most important thing to the user on the computer, and will pay to get it back.

Reference

Gazet, Alexzander. "Comparative analysis of various ransomware viri." 6. (2010): 77-80. Print. <http://download.springer.com/static/pdf/16/art%3A10.1007%2Fs11416-008-0092-2.pdf?auth66=1397653171_f8aa242557ea2b2b6c3957583c62804b&ext=.pdf>.

Epper, Hofftman. "THE GROWING CYBER MENACE." *SC Magazine*. 25.2 (2014): 18-23. Print. <http://search.proquest.com.jproxy.lib.ecu.edu/docview/1500752464>.

http://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information

http://blog.malwarebytes.org/intelligence/2013/10/cryptolocker-ransomware-what-you-need-to-know/

http://www.microsoft.com/security/resources/ransomware-whatis.aspx

http://www.pcworld.com/article/2084002/how-to-rescue-your-pc-from-ransomware.html

http://www.cio.com/article/744937/Cryptolocker_Ransom_Trojan_Infected_250_000_PCs_Dell_Secureworks_Estimates

http://www.tomsguide.com/us/cryptolocker-evolves-worm,news-18066.html

http://www.zdnet.com/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin-7000024579/