A. Michele Parrish
Dr. Phil Lunsford
ICTN 6865
4 December 2015

Is your device being held hostage?

ABSTRACT

Ransomware could be a potential problem for users of electronic devices. This paper will examine ransomware. I will discuss what it is and how your device can be infected. I will explore the reasons why it is growing and the new devices it is infecting. I will also explain ways in which a normal user can protect themselves against ransomware.

INTRODUCTION

Malware is "software that enters a computer system without the user's knowledge or consent and then performs an unwanted and usually harmful action" (Ciampa 51). Ransomware, also known as cryptovirus, is a form of malware that takes control of a user's device or files until the user agrees to the hacker's demands. Usually those demands are monetary but they may ask for other forms of compensation (Luo,Liao 195). "Recently a new ransomware required the victim to purchase a specific amount of pharmaceutical drugs from a Russian online pharmacy to meet the ransom demand" (Fanning 11). It is just not the ransom fee, usually between $200 and $10,000 that the victim has to incur but also costs for "network mitigation, network countermeasures, loss of productivity, legal fees, IT services, and/or the purchase of credit monitoring services for employees or customers" (Cooney). Companies may also suffer loss of reputation and trust of stockholders.

One of the first documented examples of ransomware was in 1989 when an AIDS Info disk contained a Trojan named PC Cyborg. The disk was given to over 7,000 people and when it ran it would count the count the number of times the computer booted. After 90 boots, the ransomware hid and encrypted the files that were on the C: drive until users paid $378 to a post

office box (Bridges 18). In 1996 an article by A. Young and M. Young described potential ideas and scenarios where encryption of files could be used for extortion or denial of service attacks (Bridges 18). Ransomware is considered a Trojan, or also known as Trojan horse, because it disguises itself as a legitimate program or it hides inside other software. It cannot replicate itself and relies on a host (Luo,Liao 198). It is transferred from device to device via files and protocols. Ransomware is a federal crime so information technology companies and law enforcement are working together to try and stop the distribution of it (Fanning 11).

PC World's Eric Geier says there are three categories of ransomware; scareware, lock-screen viruses and encrypting malware (McDermott 35). "Scareware consists of bogus antivirus or clean-up tools that claim they've detected umpteen issues, and demand that you pay in order to fix them" (McDermott 35). Lock-screen viruses lock your computer so you can't use them. They usually display a message that looks like it's from the Federal Bureau of Investigation or the Department of Justice that warns you have broken the law and must pay a penalty (McDermott 35). Encrypting malware encrypts files on your device.

EXAMPLES

There has been many different examples of ransomware since the first documented case in 1989. In 2006 there were several including Trojan.Pluder.a, Arhiveus, Trojan.Randsoma.A, Trojan.Cryzip and Trojan.PGPCode (Luo,Liao 197). Most modern computer users were introduced to ransomware in September 2013 when CryptoLocker infected Windows computers. Users' files were encrypted when they clicked on links in emails that appeared to be tracking emails from FedEx and UPS (McDermott 35). The hackers demanded payment in Bitcoins. The IC3 believes that hackers use Bitcoin because it is "easy to use, fasts, publicly available, decentralized and provides a sense of heightened security/anonymity" (Cooney). According to Dell Secure Works CryptoLocker infected approximately 250,000 computers in the first 100 days and the hackers could have made anywhere from $380,000 to millions ("CryptoLocker success leads to more malware"). The mastermind behind the ransomware was Evgenly Mikhailovich Bogachev from Anapa, Russia (McDermott 35). The computers that ran the botnet, Gameover Zeus, which distributed CryptoLocker, were shut down by law enforcement in June 2014 (McDermott 35).

In mid-January of this year, 2015, CryptoWall 3.0 was discovered. It is more powerful than CryptoLocker and can be traced back to a hacker in Russia (McDermott 35). The Dickson's sheriff's office in Tennessee was one of the first victims of CryptoLocker. Employees' first clue that they had been affected was when messages popped up on their screen demanding a ransom in a certain amount of time or the files would not be recoverable. The department had backup copies of almost all their files but couldn't recover about 70,000 files. The sherrif's office paid the $572 ransom because the files that couldn't be recovered included "documents vital to … ongoing investigations, booking documents, records, records of issued equipment, documents related to current and past prosecutions and other non-replaceable documents" (19).

In early December of 2015, *Reader's Digest* website was one of the victims of a new instance of ransomware, called Angler, which is targeting Windows machines through websites that have not been secured properly (Goodin).

> The campaign is carried out by installing a cocktail of malware on the compromised PC. The first payload consists of the notorious data thief Pony, which systematically harvests all usable usernames and passwords from the infected system and sends them to a series of Control & Command servers controlled by the attackers (Goodin).
>
> The purpose of this action is to abuse legitimate access credentials to web servers and CMS systems used by websites and to inject the malicious script in these websites so that the campaign achieves the largest possible distribution (Goodin).
>
> In the second phase, the drive-by campaigns unfolds via the victim being moved from the legitimate website, which has been compromised, to a heap of dedicated domains which drop the infamous Angler exploit kit (Goodin).
>
> The Angler exploit kit will then scan for vulnerabilities in popular third-party software and in insecure Microsoft Windows processes, if the system hasn't been updated. Once

the security holes are identified, Angler will exploit them and force-feed CryptoWall 4.0 into the victim's system (Goodin).

Symantec recently discovered a revival of the scareware ransomware mentioned earlier in this paper. Users receive a pop-up message that alerts users that they have a problem with their computer and should call a number of download software to fix the problem (Kirk). Ransomware is then downloaded in the background as part of the software to fix the problem. Users have to pay for the technical support and the ransomware for their files that have been encrypted (Kirk). "On one tech support site seen by Symantec, an iframe hidden on the page redirected to the Nuclear exploit kit, a popular one used to spread malware" (Kirk). It is not clear if the people running the tech support scam are also responsible for the ransomware or if their website have been compromised and users are redirected to sites with the ransomware (Kirk).

It is not just personal computers that can be compromised by ransomware. Ransomware can also hold cell phones and smart tvs hostage. An updated version of Simplocker is affecting Android phones. It "masquerades on app stores and download(s) pages as a legitimate application and uses an open instant message protocol to connect to command and control servers" (Gallagher). Once the "app" is installed it asks for administrative privileges and announces to users that it was planted by the National Security Agency and that they will need to pay a fine to get control of their phone back (Gallagher). What makes this instance of ransomware new is that this is the first one to use Extensible Messaging and Presence Protocol (XMPP), an instant messaging protocol, to circumvent detection by anti-malware software (Gallagher). Check Point researchers thinks that there are tens of thousands of devices infected with this malware. They also found that approximately 10 percent of the users paid the ransom of between $200 and $500 (Gallagher). That equals out to $2,000 to $5,000 made by the hackers for every 10,000 infections (Gallagher).

There are also two more common ransomware attacks that are targeting Android phones. They are both applications that advertise themselves as adult video players. Adult Player does display the content it promised but takes a picture of the phone's user with the forward facing

camera (Brzezk). The attack locks the phone and blackmails the user by threatening to reveal the photos of the user (Brzezk). The other application is called Lockerpin and "it sets or changes the current PIN code and blocks access to the phone" (Brzezk).

Apple devices are not immune to ransomware. iOS phones have been compromised by lock-screen attacks. While it's not known exactly how hackers compromised the phone it is believed that they leveraged access to iCloud accounts to exploit the phones (McDermott 35). Macs have also been targeted by the scareware FBI ransomware (McDermott 36).

Symantec ran a successful experiment where it was able to compromise smart tvs that were running Alphabet's Android operating system (Ilascu). They said the experiment could be altered and be used against other operating systems used on smart tvs like Tizen, Web OS and Firefox OS (Ilascu). In the experiment they were able to "hijack(ed) the installation of a game app and replaced it with a version that looked just like the legitimate one. This one was repackaged with the malicious component, which deployed when the game launched " (Ilascu).

GROWTH

One of the reasons for the spread of ransomware is the profit that can be made by the hackers. As mentioned earlier ransomware is a federal crime but for the hacker the risk of being caught and charged with a crime is worth it. Security vendor Trustwave says that on average a hacker can get a 1,425% return on investment (Heun). They can purchase an exploit kit or ransomware scheme for one month for $5,900 and can turn it into a profit of approximately $90,000 (Heun). Cisco announced in October 2015 that it disabled a global ransomware operation that was distributing the Angler ransomware exploit kit. The hackers were making a profit of $60 million each year (Duffy).

An additional reason for the growth of ransomware and malware in general is the use of mobile devices in a company setting. This is commonly referred to as the BYOD (bring your own device) issue (Fanning 7). Each user brings their own device so there is no standardization for the device that is being used to access the company resources. Companies assume that users will follow the company's security policies. Either the user doesn't under the policy or the policy

may not even be in place (Fanning 7). These mobile devices are used to access the Internet more than they have been in the past. Users must use the Internet to access the company's resources (Fanning 8). This will continue to increase as more and more companies turn to the cloud for software and storage.

Lastly, vulnerabilities in applications are a problem. According to Trustware 98% of software application had at least one vulnerability in 2014 (Heun). They found that one application had 747 vulnerabilities and that the average number for an application was up 43% in 2014, up to 20 per application. The previous year the average was 14 (Heun). These vulnerabilities allow hackers to install ransomware on devices. As software is rushed to market there will be more vulnerabilities in the software.

PREVENTION

User education is a key to the prevention of ransomware. Users need to understand how ransomware can affect them personally and their company (Luo,Liao 201). When they understand how their actions can affect them and the business they are more likely to take the measures to prevent ransomware. They must also be educated about what ransomware is and steps they should take to avoid infecting their systems with it. Some simple steps that a user can take to prevent ransomware is to:

- Malicious software is spread via web browser pop ups. So that they are not accidentally clicked, block popups on your web browser (Cooney).
- Make sure you use strong passwords and have a different password for every login (Cooney).
- Don't open suspicious or unsolicited web links (Mustaca 19).
- Don't open email attachments that look suspicious even if they come from someone you know (Mustaca 19).
- If you receive a ransomware message immediately disconnect from the Internet (Cooney).

One of the most recommended ways to counteract ransomware is to make sure you backup your data. This way even if the hacker encrypts your data you will have a copy of it and you will not feel that you have to pay the ransom to get back control of your files. You will be able to disinfect your computer and then restore the unencrypted files from the backup copy (Mustaca 19). "According to Minneapolis-based company Kroll Ontrack, 65% of survey respondents last year had a backup solution in place sat time of data loss, up 5% from 2013. Of those respondents, 59% used an external hard drive, 15% had cloud backup, and 10% used a tape backup system. Additionally, 55% said they diligently backed up their data on a daily basis" (Drolet). No matter what method you use to back up your data the backup needs to be kept in a separate location from the pc itself" (Drolet).

Keep your operating system and applications patched will help protect your device from ransomware. You should also make sure that your anti-virus/malware programs are kept up to date. New viruses and malware are introduced every minute. If you detection programs are not updated the new strains may be able to infect your computer. Operating systems and applications have vulnerabilities and new one are discovered on an ongoing basis. Companies provide fixes to the vulnerabilities through patches and support packs. You should make sure that your system is set to update on a regular basis.

TO PAY OR NOT TO PAY

You should not pay the ransom. By paying the ransom you are encouraging the hackers to continue their criminal activity. If you pay the ransom you are not guaranteed that the hacker will release control of your device or send you the decryption key so you can unencrypt your data (McDermott 37). As mentioned earlier most ransoms are paid with Bitcoin. There has been a drop in the value of Bitcoin recently. It takes 2-3 days for a payment to be processed through Bitcoin and by the time it processes your payment may not have the value that was requested (McDermott 37).

CONCLUSION

Ransomware is not going away. It will continue to grow and adapt to circumvent detection programs. It will also expand to affect more devices. Next month it may attack your

network attached refrigerator or toilet. As users of network connected devices we have to educate ourselves so we can protect our devices as much as we can. It is up to us to minimize the effect that ransomware attacks have.

Works Cited

Brzezek, Pawel. "Ransomware Attacks against Android Phones - Kroll Ontrack UK Blog." *The Kroll Ontrack UK Blog*. Kroll Ontrack, 20 Nov. 2015. Web. 01 Dec. 2015.

*Bridges, Lloyd. "The Changing Face of Malware." *Network Security* 2008.1 (2008): 17-20. Web.

Ciampa, Mark. *Security Guide to Network Security Fundamentals*. 5th ed. CENGAGE Learning, 2015. Print.

Cooney, Michael. "FBI: CryptoWall ransomware plague rising." Network World. (June 24, 2015 Wednesday 08:33 AM EST): 1048 words. LexisNexis Academic. Web. 30 Nov 2015.

"CryptoLocker Success Leads to More Malware." *Network Security* 2014.1 (2014): 20. *ProQuest.* Web. 4 Dec. 2015.

Drolet, Michelle. "Don't be mad at ransomware attackers, be grateful." *Network World*. (July 7, 2015 Tuesday 07:52 AM EST): 835 words. LexisNexis Academic. Web. 30 Nov 2015.

Duffy, Jim. "Cisco Disrupts $60M Ransomware Biz." *Network World (Online)* (2015) *ProQuest.* Web. 4 Dec. 2015.

*Fanning, Kurt. "Minimizing the Cost of Malware." *J. Corp. Acct. Fin. Journal of Corporate Accounting & Finance* 26.3 (2015): 7-14. Web.

Gallagher, Sean. *Android Ransomware Uses XMPP Chat to Call Home, Claims it's from NSA*. New York: Condé Nast Publications, Inc, 2015. *ProQuest.* Web. 4 Dec. 2015.

Goodin, Dan. "New Ransomware Campaign Pilfers Passwords before Encrypting Gigabytes of Data." Arstechnica, 3 Dec. 2015. Web. 03 Dec. 2015.

Heun, David. "Hackers' Schemes Prove Extremely Profitable: Report." *Payments Source*. (June 9, 2015 Tuesday): 627 words. LexisNexis Academic. Web. 30 Nov 2015.

Ilascu, Ionut. "Ransomware Works on Smart TVs, Too!" *The Security Ledger*. Security Ledger, 27 Nov. 2015. Web. 30 Nov. 2015.

Luo, Xin, and Qinyu Liao. "Awareness Education as the Key to Ransomware Prevention." *Information Systems Security* 16.4 (2007): 195-202. *ProQuest.* Web. 4 Dec. 2015.

Kirk, Jeremy. "Ransomware and Scammy Tech Support Sites Team up for a Vicious One-two Punch." *PCWorld*. N.p., 2 Dec. 2015. Web. 03 Dec. 2015.

McDermott, Irene E. "Ransomware: Tales from the CryptoLocker." *Online Searcher* 39.3 (2015): 35-7. *ProQuest.* Web. 1 Dec. 2015.

*Mustaca, Sorin. "Are Your IT Professionals Prepared for the Challenges to Come?" *Computer Fraud &*

Security 2014.3 (2014): 18-20. Web.