David McConnell
COMP 116
12/07/17

The Current State of Ransomware in Today's World and Why the Future is Bleak

Abstract and Introduction:

Recently, Ransomware has become the topic of much conversation, especially due to the fairly well-known "WannaCry" attack that occurred in May of 2017. While WannaCry has been discussed at length, Ransomware has been growing steadily for several decades now. Many people have a rough idea of what ransomware is, but lack an understanding of the specifics. Through the discussion of the most common ransomware practices and the methods they exploit, several defensive strategies allowing for ransomware protection can be created and applied. The tactics that malicious entities use to install malware and methods to defend against these entities will be discussed. The more information there is about how to stop ransomware, the less successful these malicious entities will be.

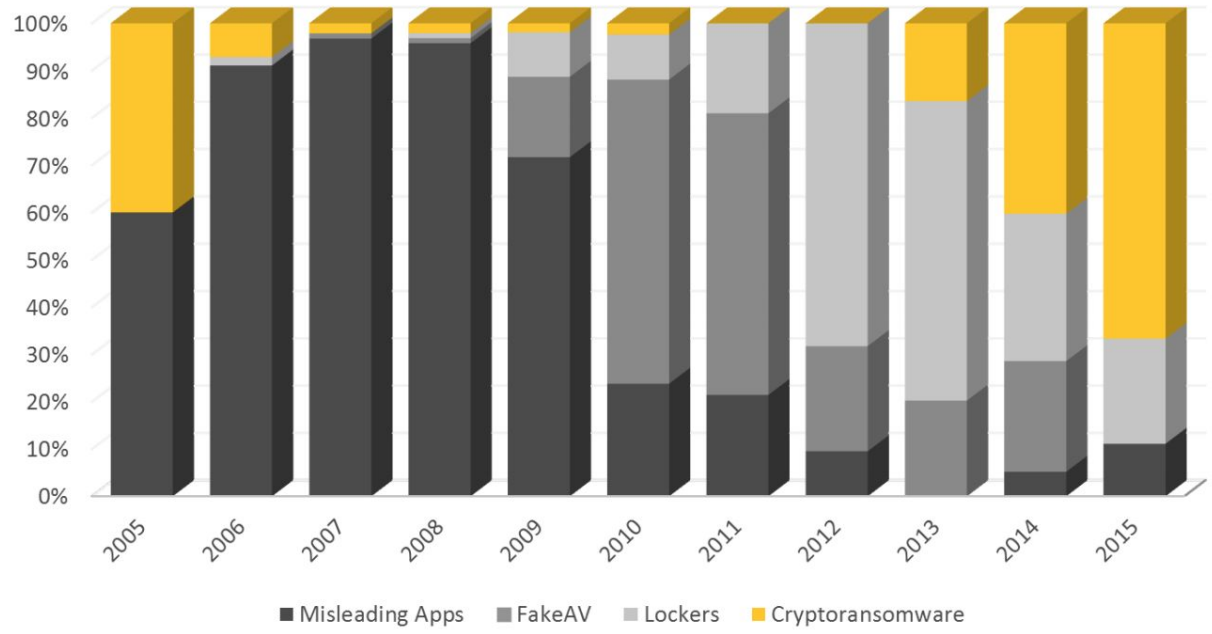


Figure 1: Percentage of new families of attacks from 2005-2015 (http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf)

In recent years, the percentage of attacks on users has been increasingly shifting towards mainly being Ransomware attacks, to the point that the majority of the attacks in recent years

have been some form of Ransomware (Savage, et al). The idea that is crucial to understand is that nothing has happened in recent years to make users particularly more susceptible to Ransomware attacks, despite this increase. Rather, attackers have slowly been coming to the realization that the majority of computer users are not protecting themselves against these types of attacks in any way, despite there being so many different methods of protection available. For this reason, it is absolutely imperative that information about Ransomware and protection against it be spread as much as possible, in a manner that is easy to follow for those individuals who are not particularly acquainted with methods to ensure their safety against these types of attacks. This being said, this information has been readily available for decades but Ransomware continues to become more and more prevalent, suggesting that we, as a society, are not as concerned as we should be.

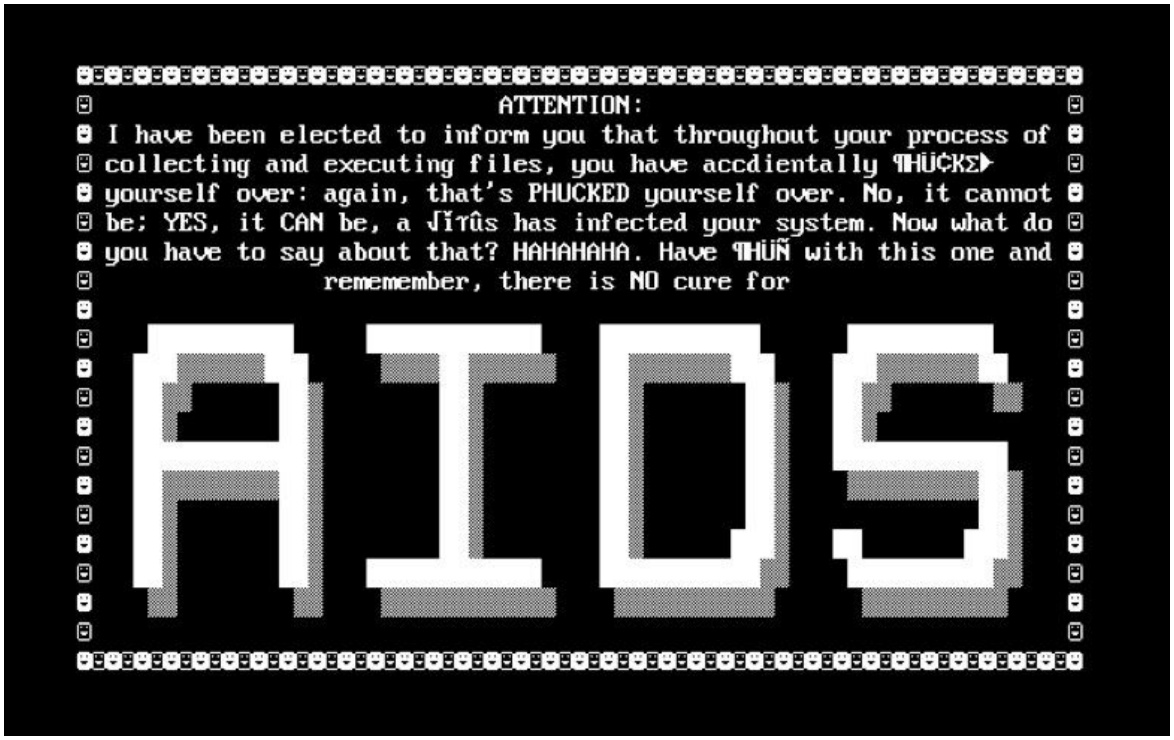
To the Community:

Ransomware attacks continue to occur on a regular basis. Although they might not receive as much new coverage as a relatively large-scale attack such as WannaCry, people are constantly being impacted by ransomware due to a lack of defence and prevention. In 2017, the total cost of ransomware attacks is estimated to be $5 billion (Cyber Security Ventures). The fact that so many of these sorts of attacks happen by exploiting vulnerable software for which a patch has already been released highlights the attitude of most computer users, in that they think they are perfectly safe and don't recognize the possible threats to security and privacy that exist, or they simply think that is won't impact them personally. The tricks that these malicious individuals and groups are using to take advantage of unsuspecting victims are *not* new tricks. They have been around for decades, but we as a society continue to allow ourselves to be taken advantage of as a result of this false sense of security. This attitude absolutely needs to change for any sort of positive change to happen. Understanding how Ransomware functions and what kind of individuals and groups are generally targeted, and spreading this information to everyone possible, is necessary to try and combat the people responsible for spreading Ransomware. Without significantly more of push for security awareness and training, this problem will only continue to worsen.

History And Classifications of Ransomware:

In order to understand how to make some sort of positive change in how we as a society protect ourselves against ransomware, it is extremely useful to understand exactly how the current state of ransomware in the world came to be. What is thought to be the first ransomware attack is known as the "AIDS Trojan," named such due to the surrounding scenario that allowed for the trojan to be spread. The AIDS Trojan was spread in 1989 by an individual named Joseph Popp, PhD, who was an AIDS researcher. Popp spread the attack by handing out roughly 20,000

floppy disks to AIDS researchers across the world (Lord). These disks supposedly determined an individual's risk of acquiring AIDS based on their answers to a questionnaire. However, along with the questionnaire, the disk also contained a trojan. This trojan would only activate after the user had booted their computer up 90 times, at which point a message was displayed demanding a payment of several hundred dollars for a software lease (Lord). While this attack was quite simple in terms of the methods that it used to take advantage of victims, it certainly laid the foundations for Ransomware attacks to grow into what they have become today.



<u>Figure 2</u>: Screen displayed on machines infected with the AIDS Trojan.
(www.knowbe4.com/aids-trojan)

One of the two most common types of Ransomware in recent years is Locker Ransomware. The first major instance of Locker Ransomware, which effectively "locks" users out of their system until a fee has been paid, was the Reveton Worm, which first released in 2012 (Rubens). Reveton essentially displayed a message in place of the normal login screen that a user might expect. This message was designed to look like an official message from a national police force, such as the FBI in the United States. The type of message that was displayed was based on the region in which the victim's computer was located, to make the message seem legitimate. Regardless of the region, the content of the message was something along the lines of requiring the victim to pay a fee for breaking some sort of law, with the result of not paying the fee being criminal prosecution. More recent versions of Reveton include password stealing software that will stay on the victim's machine, even if they pay the fee to be able to access their computer

again (Rubens). Reveton still exists today, and many different examples of Ransomware have followed Reveton by example and lock users out in a similar way.

Figure 3: Example of a message when infected with the Reveton Worm. (www.knowbe4.com/reveton-worm)

The other of the most common types of Ransomware in today's world is Crypto Ransomware. This type of ransomware encrypts many of the victim's files, demanding a fee to have them decrypted. While some examples exist from fairly early on, in 2013 and 2014 several instances of Crypto Ransomware, including but not certainly not limited to CryptoLocker, Xorist, CryptorBit, CryptoWall, and CTB-Locker began infecting systems and encrypting their victims' files (Lord). All of these types of Ransomware use some sort of encryption algorithm on the victim's files, although the exact type of encryption varies. Both symmetric and asymmetric encryption algorithms can be used, both with their respective advantages and disadvantages (Savage, et al). Symmetric algorithms tend to be much faster in terms of time than asymmetric algorithms, although files encrypted with a symmetric algorithm tend to be much easier to decrypt. Asymmetric algorithms, on the other hand, are generally slower, but it is much more difficult to decrypt any files that have been encrypted. When attackers decide the method to use, speed is very important, as the faster the files are encrypted, the less likely it is that a user might realize that their files are being maliciously encrypted. However, if the algorithm is simple and the files are easy to decrypt, chances are the user will simply find a method to decrypt the files themselves or with the help of a third party individual or group, rather than paying the demanded fee for decryption. Some of the more advanced instances of Crypto Ransomware will use some sort of combination of the two (Savage, et al).

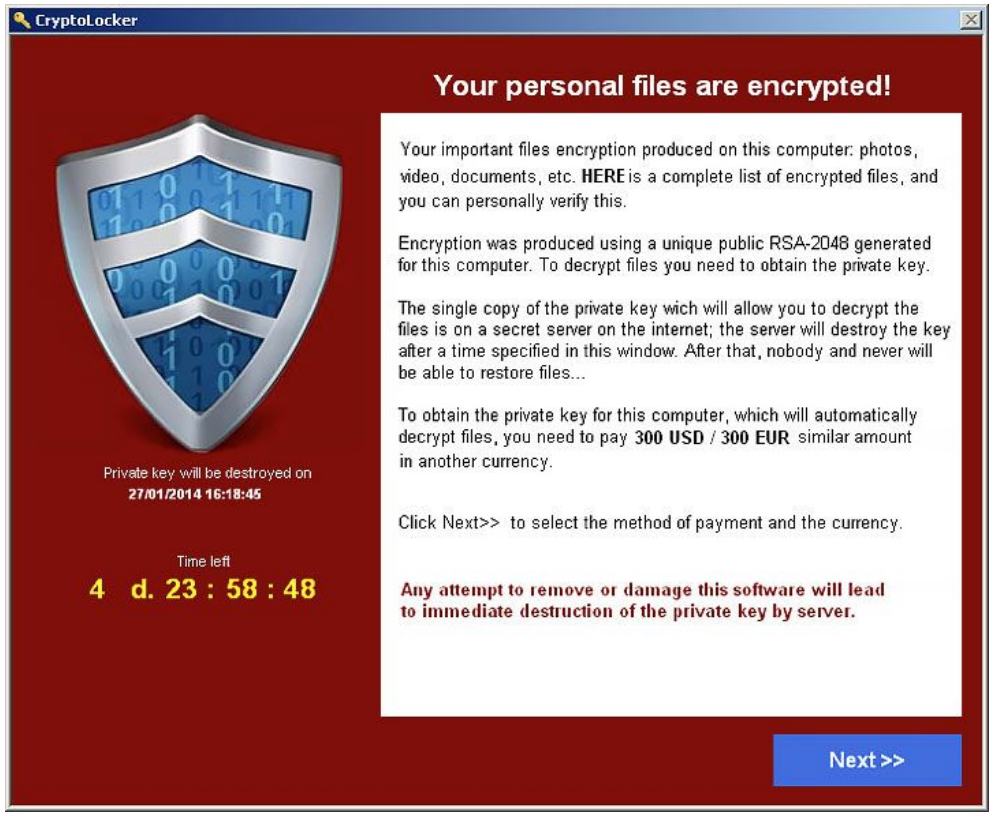


Figure 4: Screen displayed when infected with CryptoLocker 2.0. (www.knowbe4.com/cryptolocker-2)

How Ransomware is Transmitted to a Victim's Machine:

First, it is important to define who is generally targeted by Ransomware attacks. Many home users are victims of Ransomware, but several police departments, city councils, schools, hospitals, and other generally larger groups of individuals have been targeted by attackers as well. Several methods exist for infecting a single user's machine. One common approach is using email, generally done with phishing, either sending someone to a malicious site or telling them to download an attachment that is actually malicious (Gupta). Often times, downloads from "spam sites" are malicious and secretly install some sort of malware onto a user's machine. Examples of this include free versions of otherwise expensive software that have malicious code embedded in them, or telling a user visiting a website that their software is out of date and that they should update it with a file they can download, which secretly has malicious code (Gupta). Both of these sorts of methods directly involve user interaction, but methods that do not exist as well. Attackers are often able to exploit security vulnerabilities in software in order to install Ransomware. Generally speaking, the average user is reluctant to update their software to the most recent version, allowing attackers to exploit these vulnerabilities, even *after* a patch has

been released. Occasionally, legitimate websites might have malicious code injected into them in an attempt to make potential victims lower their guard and be less suspicious of any software they are downloading.

Perhaps the most frightening method of installing Ransomware on an individual's machine is using a different victim's already infected machine. A machine that is already infected is able to send the Ransomware to potential victims as a link or an attachment, causing these potential victims to severely lower their guard as the sender might be a friend or colleague. Another option is to abuse the same security vulnerability that was present on the initial victim's machine, if the machine was infected using some sort of vulnerability. This type of infection is repeatable, meaning that any infected machine might spread it to another uninfected machine, effectively creating a botnet from which the attacker benefits, with almost no input once the initial machine has been infected (Savage, et al). These are the main methods that are used to spread Ransomware to people in the same workplace.

What Can be Done Once a Machine is Infected:

There are a few different options for what can be done to unlock a computer or decrypt files that have been encrypted. The most obvious, although a potentially useless option, would be to simply pay the malicious attacker to unlock the computer or decrypt the files. However, there is *no* guarantee that the attackers will remove the Ransomware from a machine after a payment has been made. Several online guides are available for free, explaining how to remove the Ransomware from a machine if possible, although these guides should be followed with *extreme* caution, as they have the potential to be malicious in intent as well. For Crypto Ransomware, there is often a decryption algorithm available if it is not a new type of Ransomware, as long as symmetric encryption was being used. If asymmetric encryption was used, it could be potentially impossible to decrypt the encrypted files due to the lack of the private key that an attacker would have used. Often times this is in fact the case, which is why prevention is so much more important as a means of dealing with Ransomware as opposed acting only once a computer has been infected.

Defences - Ransomware Infection Prevention:

Infection Prevention is crucial to mitigating the potential impact of Ransomware. One of the easiest, yet least followed methods to prevent infection is to update software on a regular basis. The recent WannaCry attack relied *completely* on a security vulnerability for Windows software that had been released two months before the attack actually took place (Zaharia). Attackers took advantage of the fact that Microsoft only released a patch for support versions of Windows, and the fact that it was likely that several users simply wouldn't patch their software. The lack of individuals who update their software on a regular basis is extremely beneficial to

attackers, as the vulnerabilities that have been found have the potential to still be exploitable, even though the software creators have issued a fix.The attitude towards updating software needs to shift in order for these vulnerabilities to have any real chance of being mitigated.

Other methods of protection include being extremely cautious when downloading any type of software. Often times, software releases include an encryption checksum, allowing a user who downloads software to ensure that it is exactly what they think it is. Users should inspect any attachments they receive by email extremely carefully, and closely examine any links they receive by email as well. Several tools, such as VirusTotal, exist that allow a user to scan any files and URLs for potential malware. Another option is to install reliable antivirus software preventatively, so that if a user actually is infected, they have a chance of noticing before it is too late. One thing that should be noticed is that all of these methods require the *user* to take preventative measures in order to ensure protection against attackers. The unfortunate truth is that many users simply do not realize that they are even at risk or lack the knowledge to protect themselves against malicious intent.

One of the most effective methods for preventing Ransomware in general, but especially Crypt Ransomware, is to regularly backup data to an external disk (Savage, et al). If a user has a backup for all of their data, *it doesn't even matter* if they have their files encrypted, as they always have a backup copy they can rely on. With a backup, infected machines can be completely wiped clean, with the backup then being used to essentially "reset" the user's machine to state prior to being infected. Another option is to keep a backup on some sort of cloud storage. There are several different companies that offer online storage of files, many of which offer a decent amount of storage completely for free. By pushing backups of files to cloud storage, file encryption again becomes even less of a threat. Ideally, both of these methods being used in conjunction provides a huge amount of security for possible attacks. This again relies completely on the user taking initiative for protecting their machines from any possible threats, meaning that many people will either not know how or not think they have any reason to backup their data.

Conclusion:

One might be hopeful for the future when it comes to Ransomware protection, considering the vast number of different protection techniques that are fairly readily available for use. However, despite all of these methods, Ransomware continues to grow by exploiting the same kinds of vulnerabilities that have existed for decades. There needs to be a fundamental change in how we as a society treat protection against attacks that exploit the several vulnerabilities that exist, or things will just continue to get worse. It is up to the security community to effectively communicate these issues and how to prevent them so that users are able to better understand protection and take it more seriously.

References:

"Alert (TA14-295A)." *Crypto Ransomware | US-CERT*, 22 Oct. 2014, www.us-cert.gov/ncas/alerts/TA14-295A.

Gupta, Harshit. "Major Sources of Ransomware Attack in Computer System." *Protegent 360 Complete Security Software*, 31 May 2017, www.protegent360.com/blog/major-sources-of-ransomware-attack-in-computer-system/.

Lord, Nate. "A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time." *Digital Guardian*, 7 Dec. 2017, digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time.

"Ransomware Damage Costs $5 Billion in 2017, Up from $350 Million in 2015." *Cybersecurity Ventures*, 18 May 2017, cybersecurityventures.com/ransomware-damage-report-2017-5-billion/.

Rubens, Paul. "Common Types of Ransomware." *Types of Ransomware*, 2 Mar. 2017, www.esecurityplanet.com/malware/types-of-ransomware.html.

Savage, Kevin, et al. "The Evolution of Ransomware." *Symantec Security Center White Pages*, 6 Aug. 2015, www.symantec.com/content/dam/symantec/docs/security-center/white-papers/the-evolution-of-ransomware-15-en.pdf.

Zaharia, Andra. "What Is Ransomware - 15 Easy Steps To Protect Your System." *Heimdal Security Blog*, 11 Dec. 2017, heimdalsecurity.com/blog/what-is-ransomware-protection/.