2017

Insight into Ransomware

RYAN HAUG
KEANU MUNN
GARRETT TAYLOR

INTRODUCTION TO INFORMATION SECURITY COM-416

Abstract

In today's society virus's and malware are an increasingly growing threat to home users and businesses that range from independent owners to corporate giants of the world. In recent years a new type of virus has made waves across the globe because of its destructive nature, and its ability to hold organizations like world-trade banks at ransom for their information. Scholars have come to call this malicious virus Ransomware. The purpose of this paper is to discuss topics that deal with Ransomware. The findings and research are divided into three sections. The first section goes into detail about what Ransomware is and how it is different from most other viruses. The second section covers how to prevent and mitigate Ransomware using four fundamental steps, and why companies should be taking Ransomware as a very serious threat in modern times. Finally, the last topic gives an example of the most recent and viral form of Ransomware, WannaCry.

Introduction

The definition of ransomware is a malicious software that locks the user out of their computer until a sum of money is paid. Ransomware has cost businesses large and small billions of dollars, and the threat is only increasing. Ransomware is the type of malicious software that needs to be caught and contained quickly or else it will wreak havoc on user's systems. Ransomware has had a 26-year period of evolution, and has only grown exponentially more sophisticated as of 2011. The 26-year growth and recent increase of sophistication has been measured, and will show that ransomware usage is increasing. 2011 was the start of direct end user attacks by hackers, and it also fueled the growth of financial gain that hackers were seeing by using this type of software. The attraction that ransomware was producing has increased the amount of usage. No target is too small for this type of attack. If a user has data that they find to be valuable then it is at risk of a ransomware attack. The hacker will lock access to this data, and the user feels that they have little choice but to pay to retrieve their data. Ransomware has recently started to introduce cryptographic traits that make it increasingly more difficult to crack the lock that the software puts on the data. Cryptographic traits make it that much more important to catch the attack and contain it before it locks the data down. Today, ransomware no longer just blocks user's access to their devices, but instead encrypts an entire device's data. If a business were to be the subject of a ransomware attack, the consequences could be loss of revenue, loss of cliental, and an overall detriment to daily business functions. Preventing ransomware and implementing mitigation tactics against this disastrous virus is now a necessity to accommodate for the growing threats and risks that ransomware poses for businesses today.

Ransomware mitigation and prevention can be summarized in four steps: back up, avoid email links and attachments, patch and block, and drop-and-roll.

Back up is the concept of backing up data to either cloud servers or some sort of locally connected backup system; however, "[ransomware] encrypts files in the background, and those encrypted files are then placed into the current backup, preventing that backup from being used to restore unencrypted files", so multiple back-ups are necessary. The next step is to avoid email links and attachments that try to lure personnel into phishing traps. These types of attacks are very common for the spread of ransomware, so it's important for employees to be trained to be vigilant against spam and potential harmful emails. The third step is to patch and block, which is the idea of keeping operating systems, browsers, and security software up to date, and blocking programs that are necessary for business operations. The last step, and the final counter to ransomware attacks that are in progress, is the drop-and-roll method. If a machine is infected, it should be immediately turned off, and the network should be shut-down to prevent further spreading of the attack. WannaCry or WannaCrypt is a perfect example of a ransomware. It was able to infect hundreds of thousands of computers worldwide. It infected these computers in more than 150 countries. This version of a ransomware was extremely powerful as it could spread across an entire organizations network with ease. It was able to do this using a critical vulnerability in Windows. This vulnerability named Eternal Blue was released by a group known as the Shadow Brokers. They made the claim that they stole the data from a group called the Equation Cyber Espionage group. This ransomware was able to use TCP port 445 otherwise know as the SMB port to spread across networks and encrypt them. It then requested payment in the form of Bitcoin. This effect was felt not only on old systems running Windows XP but on

new systems running Windows 8.1. Ransomware is a big threat and this paper will prove that it has evolved, what current threats are present, and how to mitigate this threat.

Ransomware History

Ransomware is a type of malware that did not start to become popular until 2011. Before this there existed a time in the 1990's where almost all malware activity was being conducted by hobbyist hackers. Hackers that chose to attack people for reasons other than monetary gain. The attitude towards malware quickly changed in the early 2000's when hackers saw opportunities for financial gains. Most financial gains were seen through direct information theft, the use of botnets (a network of unknowing computers used for numerous malicious activities), and advertising revenue. Malware authors would also profit from finding information like banking credentials, or personal financial information. Direct user attacks did not start until 2011 era of "Fake Antivirus Software." Unsuspecting users would pay for fake antivirus software believing that their system had been compromised. Scams like the Fake Antivirus were quickly made obsolete by a harsh crackdown on the credit card company's facilities. The Fake Antivirus scam almost overnight was dealt with. Hackers then developed a more complex type of malware that used DOS (denial-of-service) tactics. Denial of service is a malicious attack that prevents an authorized user access from their computer network. The hacker would attack the boot operations of a machine essentially locking it until the user paid to have the attack stop. The file system remain virtually untouched, so security professionals created anti-virus recovery software that would compensate for the loss of access into the system by the user. The next evolution was for hackers to be able to encrypt disk data. (Hampton & Baig, 2015)

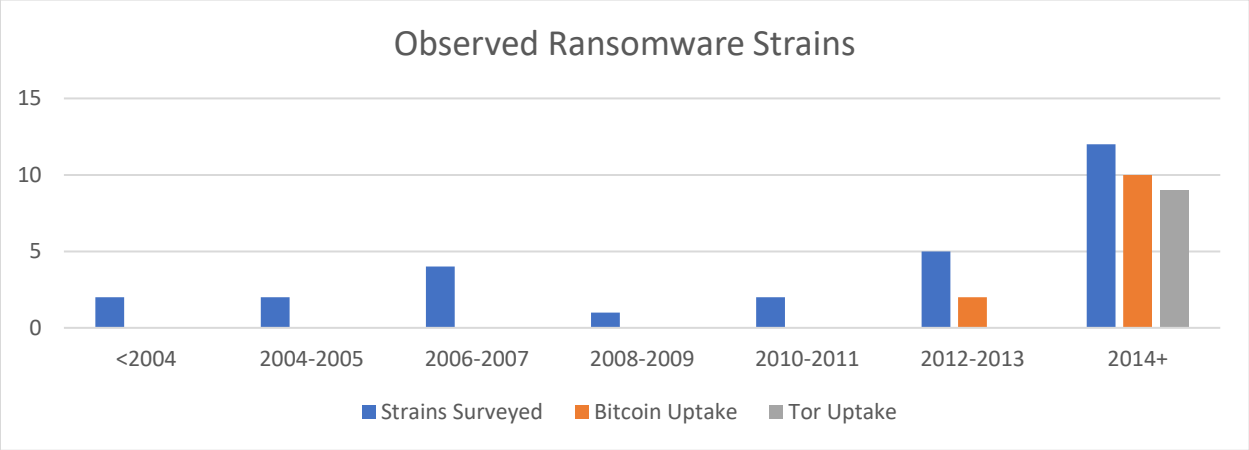
1.2 The Introduction of Cryptography

Adam Young and Moti Yung were cryptographers that created the concept of kleptography. Simply put a Kleptography attack was the use of asymmetric cryptography that was used to implement a cryptographic backdoor. The backdoor would require a private key to access it, and only the person that created the backdoor would know the private key. Young and Yung proposed the use of cryptography for strong encryption. The idea of using cryptography for a reverse denial of service attack did not gain any traction until 2005 with the introduction of PGPCoder/GPCode. The introduction of these two things brought the ideas by Young and Yung into real world implementation. PGPCoder/GPCode was used to encrypt disk content and the hacker would demand ransom payment to remove the lock. GPCode had a number of variants which created multiples of flaws. The early flaws of GPCode included: poor file deletion strategies, poorly implemented encryption routines, and insecure encryption keys. GPCode was ever evolving fixing these flaws and creating strong schemes of encryption and the key lengths also improved over this time. The invention of encrypting lockers for direct end-user ransom did not catch on for malware authors until a while later. The use of this malware required there to be many points of contact between the end user, gateway for payments, and the malware profiteer. The main problem was creating a third-party gateway that could accept the payment of the ransom. The theft of information or resource theft was still more profitable than risking using end-user extortion, so end-user extortion remained rarely used. End-user extortion needed to become less risky to make it more viable, and so three things ultimately aligned to make that possible. (Hampton & Baig, 2015)

1.3 CTB-Locker

The three things that were needed to make end-user extortion more viable were: a way of concealing the payment through an untraceable setup, a strong reversible encryption lock to use on user's files, and a system that could anonymously communicate the keys and decryption tools needed to place the lock and remove it after the ransom was paid. CTB-Locker was the first ransomware to be able to integrate these three things. CTB(Curve, TOR, Bitcoin)-Locker can be broken down into using three parts. Elliptic curve is a type of cryptography that created a fast secure encryption of the targeted system's file content. TOR is a protocol that is used in onion routing. The TOR (The Onion Routing) protocol created an anonymous way for the hacker to communicate with the target system. Finally bitcoin is an untraceable crypto-currency that the hacker could use to accept payment for the ransom. CTB-Locker had a few implementation flaws, but this was hardly a setback for the use of ransomware skyrocketed to a surprising 500% increase of usage between the years of 2012 and 2013. Newer evolutions of ransomware have created instances where the ransomware can infect multiple platforms at once including: remove media, network shares, and external hard disk backups. Ransomware is only evolving more and more as hackers are seeing a larger profit from the use of this type of malware. Large companies have started to institute constant updating of their security system, but smaller companies can not afford this type of luxury due to the increase of costs in securing systems for constantly evolving threats. The profit of ransomware shows that its use will only increase, and today's security can not deal with future iterations of ransomware, so there must be a way to effectively deal with ransomware. A way to be able to prevent or mitigate the damages caused by the use of this type of malware. Though ransomware can be seen as a scary threat; researchers are pointing to the history of malware and ransomware to show that with each evolution of these programs there are

flaws. The constant flaws or already seen performed actions can be detected, and ultimately prevented. (Hampton & Baig, 2015)



Ransomware Mitigation

Ransomware is becoming a growing threat to many businesses and industries across the world. If ransomware were to effectively infiltrate a business's infrastructure and infect the workstations, then daily business functions would come to an unexpected halt. The ability for a business to remain functional and have a near constant uptime is crucial for the business continuity of many businesses today; thus, many industries are implementing ransomware in their risk analyses as real threats that need to be mitigated and prevented. There are four steps an individual or a workplace should take to prevent ransomware: back up data, avoid email links and attachments, patch and block, and drop-and-roll.

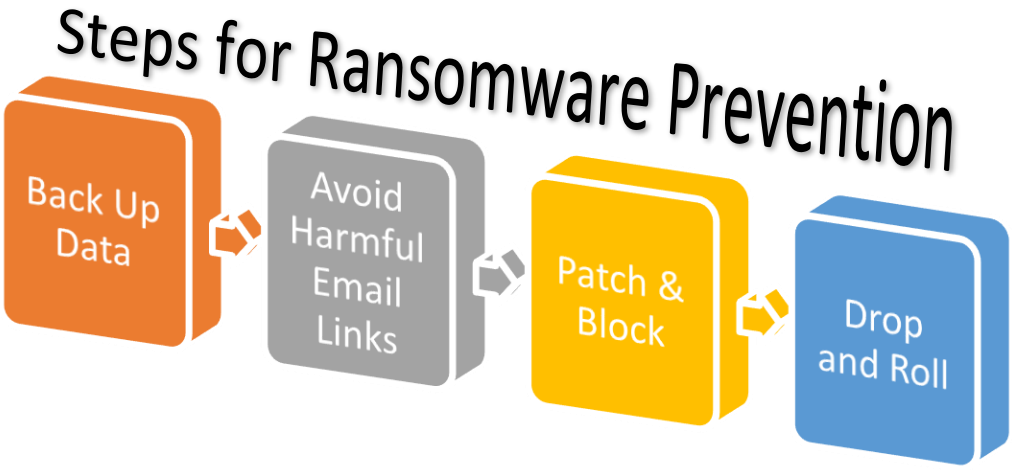


Diagram made by Keanu Munn

2.2 Back Up Data

Backing up data is an excellent way to mitigate a ransomware attack. Instead of paying money to attackers to unlock data, who might not even give the data back, or trying to decrypt the data yourself, having backups can recover the data if a good system is in place. There are many ways to back up data, but not all methods are cost-efficient and worth the time given the scale of a company. One way to backup data is through portable hard-disc drives. Most portable hard-drives are just simple plug-and-play, and suddenly a user has access to terabytes of unused storage. However, "some ransomware attempts to encrypt locally connected backup systems" (Richardson, North, 2017), so local portable hard drives may not be the best solution anymore. Another way to backup data is through CDs and DVDs. This method "has faster seeks times than tape, historically is less volatile and prone to degradation than tape, and is more portable than a SAN or a drive array" (Wells, Walker, Abarca, 2017). However, this form of media is not ideal for substantial amounts of data because of the limited size capacities of most modern CDs and DVDs. One of the best alternatives for backups and ensuring its safety from ransomware

encryption is cloud storage. Cloud storage relies on the usage of an offsite server, usually a hard disk and serviced by a third party, to store backups. This method is secure because the cloud storage is typically not on the same network as the point of attack, so the attack typically does not reach the cloud backups.

2.3 Avoid Email Links & Attachments

One of the most common ways to spread ransomware is through harmful links and attachments found in emails. Most of these emails are what experts call attempts at phishing, "a form of social engineering in which the attacker provides what appears to be a legitimate communication, but it contains hidden or embedded code that redirects the reply to a third-party site in an effort to extract personal or confidential information" (Whitman, Mattord, 2016). However, these phishing attacks are no longer used to just gain information, instead, they are being used to open attachments or click links that download ransomware on to the local machine. Companies are now trying to teach all employees on how to properly view and navigate email in a work environment. Additionally, popular email providers are implementing into their email services techniques to block malicious attachments that are suspected of carrying malware and ransomware. However, these safeguards are still not enough to prevent people from clicking on links and attachments in email, especially if they feel coerced by frightening pop-up messages notifying users that they have a harmful virus on their computer, when their system is perfectly fine, that can only go away by clicking on a link or downloading a virus remover.

2.4 Patch and Block

System and software updates should never be ignored or forgotten by a company. These updates typically are patches for security weaknesses in preexisting software, and if these patches are not addressed, then ransomware and other malware are more likely to use these

weaknesses to infiltrate a system. Additionally, unnecessary types of software and plug-ins, especially if they are provided from a third party, need to be blocked to reduce the chances of any malware infection. Many individuals and companies use antivirus software that runs as a background process on a local machine to check for and block suspicious software activities. However, most ransomware can bypass antivirus software, so a user should not solely rely on antivirus to monitor their computer for potential threats.

2.5 Drop-and-Roll

If a user or company practices the steps described above, then the potential for a ransomware attack/infection is significantly low. However, if a computer seems to be showing signs of an infection, the computer should be instantly turned off and unplugged. The faster the machine is powered down the more likely the files will not be damaged. Additionally, "if [the machine] is connected to a network, administrators should immediately shut down the network to minimize the propagation of the ransomware" (Richardson, North, 2017). Unfortunately, there is not much more a user can do when ransomware makes its way on a machine or network.

WannaCry

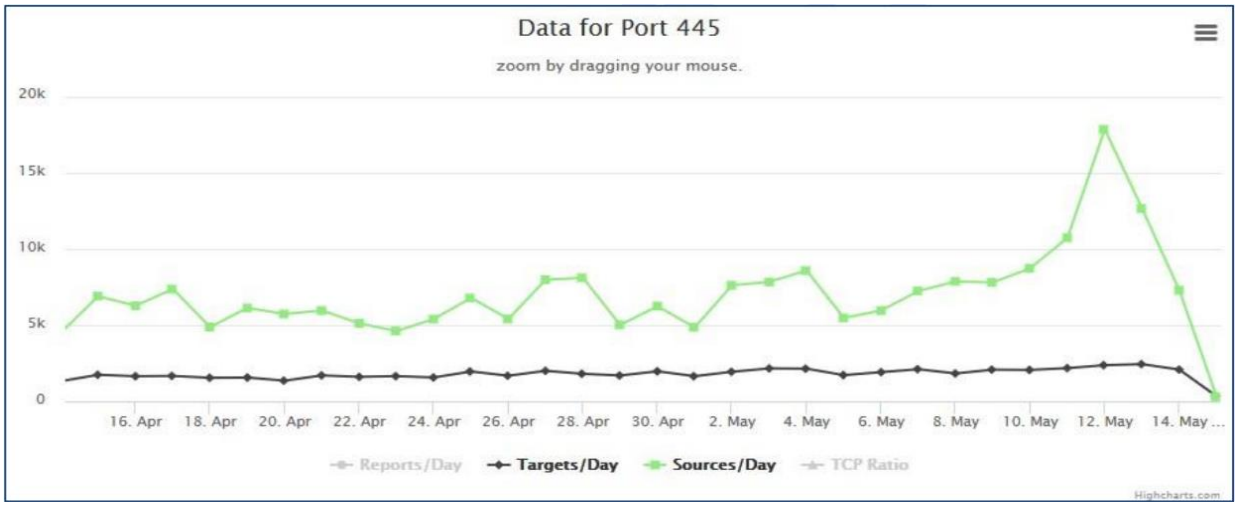
The WannaCry or WannaCrypt ransomware primarily affected windows systems from Windows XP through Windows 8.1. This ransomware used a release patch MS17-010 codenamed ETERNALBLUE. This patch was released on March 14th for newer systems and for the older systems on May 12th. The ransomware had 3 variants: .wcry, WCRY.WCRYT,

WNCRY.WNCRYT. This attack hit on a global level.

3.2 The Attack

The Attack origin is unknown. Microsoft suspected that it arrived through social engineering emails which would allow it to activate and spread through SMB (Server Message Block). The ransomware would create two threads once it was on a system. The first of the threads would scan for local hosts and the second thread would replicate itself 128 times and scan hosts across a wider range on the internet. It used the EternalBlue patch to attempt to take over the system with a 10-minute timeout. Cisco stated that it would make use of DOUBLEPULSAR which is a backdoor to execute its code. This backdoor is associated with an exploitation framework that is part of the Shadow Brokers cache. This framework was released to the public and is heavily analyzed by security professionals and hackers. The ransomware uses both the eternal blue method and the DoublePulsar method. The primary attack happened on

May 12th this coordinates perfectly with the complete release of the EternalBlue patch.



3.3 The Encryption

The encryption starts by extracting an embedded file into the same location as the installer. This file is a password protected zip file that contains everything that is used by the ransomware. The ransomware then downloads a TOR client. It uses this client to communicate with its various serves: x7ekbenv2riucmf.onion, 7g7spgrzlojinas.onion, xxlvbrloxvriy2c5.onion, 76jdd2ir2embyv47.onion, cwwnhwhlz52maqm7.onion. It then gives full permissions to everyone on the folder its installed in. It does this so that it has full control over the folder. it then kills all of the database connections and mail connections so that it can capture those as well. It then searches all of the drives associated with the computer for any of the following file types.

.der, .pfx, .key, .crt, .csr, .pem, .odt, .ott, .sxw, .stw, .uot, .max, .ods, .ots, .sxc, .stc, .dif, .slk, .odp, .otp, .sxd, .std, .uop, .odg, .otg, .sxm, .mml, .lay, .lay6, .asc, .sqlite3, .sqlitedb, .sql, .accdb, .mdb, .dbf, .odb, .frm, .myd, .myi, .ibd, .mdf, .ldf, .sln, .suo, .cpp, .pas, .asm, .cmd, .bat, .vbs, .dip, .dch, .sch, .brd, .jsp, .php, .asp, .java, .jar, .class, .wav, .swf, .fla, .wmv, .mpg, .vob, .mpeg, .asf, .avi,.mov, .mkv, .flv, .wma, .mid, .djvu, .svg, .psd, .nef, .tiff, .tif, .cgm, .raw, .gif, .png, .bmp, .jpg, .jpeg, .vcd, .iso, .backup, .zip, .rar, .tgz, .tar, .bak, .tbk, .PAQ, .ARC, .aes, .gpg, .vmx, .vmdk, .vdi, .sldm, .sldx, .sti, .sxi, .hwp, .snt, .onetoc2, .dwg, .pdf, .wks, .rtf, .csv, .txt, .vsdx, .vsd, .edb, .eml, .msg,.ost, .pst, .potm, .potx, .ppam, .ppsx, .ppsm, .pps, .pot, .pptm, .pptx, .ppt, .xltm, .xltx, .xlc, .xlm, .xlt, .xlw, .xlsb, .xlsm, .xlsx, .xls, .dotx, .dotm, .dot, .docm, .docb, .docx, .doc.

The ransomware applies a WANACRY! String to the beginning of the files it encrypts as well as a .WNCRY to tell the user just what they can't access. It then places an exe and txt file in every folder a file was encrypted in telling the user to pay up. The ransomware only accepted bitcoin for the files as it is untraceable.

3.4 The Infrastructure and Kill Switch

Cisco evaluated that the domain if the kill switch was created on May 12th. This domain was identified as human written and could reach a peak of 1400 queries on May 12th. The kill switch domain was www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com if the worm found

this domain it would destruct itself.

Conclusion

Ransomware is a serious threat to both businesses and users alike. History has shown that malware has evolved from a hobbyist hacker activity that started in the 1990's to a profiting enterprise enticing more and more hackers to use malware for profit today. Ransomware has become more popular since the risk of being caught has diminished due to the introduction of CTB-Locker. The combination of cryptography, an anonymous protocol, and a crypto-currency has created the perfect series software for use in Ransomware. People have jobs that are purely made for mitigating and preventing damage from Malware. The first step that was covered in this paper about prevention/mitigation of ransomware attacks is to regularly backup data. Data should be regularly backed up to ensure that the loss of data from an attack is lower. The next step is to avoid harmful web links that are sent via email or any other links. Personnel should be trained to identify potentially harmful links, and how they should handle disposing of those links.

The step that follows avoiding harmful links is to regularly patch and update software eliminating vulnerabilities. The last step is to be able to identify if the computer is running slow or exhibiting signs of being infected. At the point of recognizing a potential infection it is important for the user to unplug their machine, and have it quarantined. Ransomware is constantly evolving and being developed proof of that can be seen with the newest dangerous ransomware aptly named WannaCry. The WannaCry ransomware is proven to be powerful. Its real threat will come when other ransomware developers use similar exploits and techniques to create stronger ransomware.

References

April Wells, C. W. (2007). *Disaster Recovery Principles and Practices.* New Jersey: Pearson Education.

Hampton, N., & Baig, Z. A. (2015, December 2). Ransomware: Emergence of the Cyber-Extortion Menace. Retrieved September 1, 2017, from http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1179&context=ism

Michael Whitman, H. M. (2016). *Principles of Information Security.* Boston: Cengage Learning.

MU, C. (2017, May). The WannaCry Ransomware. Retrieved November 3, 2017, from http://cert-mu.govmu.org/English/Documents/White%20Papers/White%20Paper%20-%20The%20WannaCry%20Ransomware%20Attack.pdf

Ronny Richardson, M. N. (2017). Ransomware: Evolution, Mitigation and Prevention. Kennesaw, Georgia, United States of America: Kennesaw State University.