Ransomware

How did WannaCry infect the world?

Essay Networks and Network Security

Marit Beerepoot - 10983430
Jessy Bosman - 11056045
Vincent Damen - 11034734
Sander van Wickeren - 11060999

Introduction

Ransomware is the nightmare of every computer-, server- and systemuser. It is a type of malware that blocks the access to data or a whole system until a ransom is paid. The infector encrypts the device with a specific key and demands money for decrypting the data. If the money is not paid in a given time limit, the infector destroys the key which will make it (nearly) impossible to crack the encryption and to use the data or system again. Sometimes the infector threatens to publish the data publicly. Although paying might seem like the only option, it's uncertain if the user will ever get the key from the infector (O'Gorman & McDonald, 2012).

Last May one of the biggest ransomware attacks so far occurred. Worldwide computers were infected with the *WannaCry* ransomware *cryptoworm*. WannaCry used *EternalBlue* to propagate, which is an exploit of Windows' SMB (the application-layer network protocol widely used in windows). Microsoft actually found the vulnerability months before the attack, but still the virus spread quickly, because not every computer had the latest (security) patches installed. It is estimated that around 200.000 computers across 150 countries were infected. WannaCry demanded $300 per computer in bitcoins to decrypt all computers (Mohurle & Patil, 2017; Symantec Security Response, 2017b). The goal of this paper is to analyze how ransomware works and how it can be prevented or detected. WannaCry is used as example to explain the main concept of ransomware in more detail.

How does it work?

The setup of ransomware is realized in a couple of steps, according to Brewer (2016). First of all, before a device can be 'infected', a malicious file containing the virus must be opened and ran on the device. Most often, these are spread by simply sending e-mails to unexpecting users, sending malicious files as attachment. In some cases security holes of software are used, for example in adobe flash player or, in case with '*Cryptolocker*', Internet Explorer.

After initial infection of the malware, all required files are send to the virus to properly function in taking over devices. A Secure Socket Layer (SSL) is used rather than the Hypertext Transfer Protocol (HTTP), so that the connection is secure, because SSL also provides encryption, to avoid detection and suspicion, and endpoint authentication (Kurose & Ross, 2017).

Now that the ransomware is able to function properly, the malware starts to target the last thing that is still able to save your device; backups. Backups located on the hard drives are removed, making it impossible for the user to restore the device without something like backup cd's. It is rather unique for malware to target backups, making ransomware an exception.

When the backups are gone the malware can start to encrypt the device. The encryption information is acquired from a specific server, stating how to encrypt the files on local system. A unique identifier is used to encrypt the files to make sure that each 'victim' can be distinguished for one another. The problem that this entails is that each encryption is unique for each user, which ensures that each encryption is different each time. This makes it almost impossible to crack. Encryption of simple devices usually only takes a couple of minutes, which is quite fast. The exact way that the files and filenames are encoded is dependant on the version and distribution of the ransomware.

At this point the whole setup is complete and the ransomware is ready for which it was created; to extort money from the victim. The instruction can be given through different methods: for example a simple text file on the desktop, or a full screen pop-up blocking any further interaction with the device. To unlock the computer and decrypt the files a ransom, in the form of a sum of money, must be paid, hence the name 'Ransomware'. Online currency/crypto currency like *bitcoins* are increasingly used for these transactions. Although with bitcoin all transactions can be viewed, it's hard to connect a certain bitcoin address to an user. After the required amount is paid, the device is released. The ransomware clean sweeps the malware files, making sure no trace of the malware is left. This way there is no evidence left of the ransomware and it cannot be traced back to the source (Kharraz et al., 2015).

Case study: WannaCry:

The first infection of the WannaCry ransomware was, in contrast to most infections, likely through the vulnerable SMB port in Windows. After an user was infected with the malware, the worm spread through the SMB, also known as Common Internet File System (CIFS), the file sharing protocol used in windows to transfer files between computers. This was possible because of EternalBlue, an exploit in the SMB which made it possible to remotely execute code. The NSA informed Microsoft about the vulnerability and Microsoft did update their SMB, but lots of computers didn't execute the update. Computers that have not yet updated the application-layer network protocol are still vulnerable and able to spread the malware to other connected computers of the network. Windows quickly responded with emergency updates which were automatically downloaded and installed on every Windows device connected to the internet, which made it harder for WannaCry to spread (Smith, 2017; ESET, 2017)

Another cause of stopping the spreading was something that was later called the 'Kill switch'. The Wannacry software tried to connect to an unregistered domain. If it could connect, the software thinks it is in a sandbox (a 'shielded' space in which software can be executed without disturbing other processes), because in some sandbox environments there is a reply to all URL lookups, including unregistered domains. It is not sure why the software was made this way, but probably to avoid it running on sandboxed or quarantined machines used by researchers, so that it would be harder to analyze the code and stop the attack. When the software can't connect to the domain, it executes the remaining ransom software. An employee of MalwareTech found this domain and registered it into a DNS sinkhole (a DNS sinkhole is a server that captures malicious traffic and makes it possible to prevent remote control of computers infected with malicious software). This prevented new infections, because after registering the domain the malware always thinks it is in a sandbox and exits, instead of running the remaining ransom software. This gave Microsoft time to spread the emergency updates, before the attackers spreaded their new software with a different domain (MalwareTech, 2017).

When a device is infected, it first tries to spread to through the SMB port. WannaCry ransomware then generates a RSA 2048 bit asymmetric encryption key (which would take approximately 6,4 quadrillion years to crack (Digicert.com, 2017)) and saves this unique key in a file (asymmetric encryption is an encryption method where one (public) key is used for encryption and another (private) key is used for decryption). The WannaCry malware has two hardcoded public keys. It uses one of the public keys, the demo key, to encrypt files smaller than a defined limit. These files are later used to show that the attacker can decrypt the files. The other public key is used to encrypt the file with the generated RSA key. Every other file will be encrypted with another generated key, but this one is symmetric (the encryption and decryption can thus be done with the same key) and unique for every file. After that every file is encrypted together with the generated symmetric key, with the unique RSA key generated at the beginning. Finally, it displays the ransom information and uses the demo key to decrypt some of the files (Symantec Security Response, 2017a).

Detection and prevention

Malware is hard to detect, but certain things can be monitored. Some ransomware, for example, always use the same folder to work from in a root directory, or always create the same file extension (e.g. a .locky). By monitoring these type of events the malware can be detected before it it too late to stop it or to limit the damage (Brewer, 2016).

Another very important damage reduction measure is to immediately disconnect an infected endpoint from the network. This prevents that the malware is spread through the complete network, making the damage significantly worse. The most important thing to do to be protected against ransomware is keeping your system up to date. Always have the latest patches installed for your operating system, antivirus and all the other software you've installed. This way, ransomware using vulnerabilities and patches like these are less likely to succeed. External and offline backups are important to restore the system if something goes wrong, so regular back-ups are advised. To be on the safe side, it is better to replace a former infected device than to simply clean it, to avoid that the malware is still lurking in the software waiting to strike again (Brewer, 2016).

Some other preventive measure can be disabling remote services, disable file sharing and switch off unused wireless connections (including bluetooth). Another important point is to make sure to not open spam messages, never open EXEs or harmful links in emails. Especially in companies it is important to make employees aware of the dangers of ransomware (Mohurle & Patil, 2017). Even though preventive measures can be taken, it is nearly impossible to completely protect yourself against it. Pay attention or pay the price.

References:

Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. Network Security, 2016(9), 5-9. http://www.sciencedirect.com/science/article/pii/S1353485816300861

Digicert.com. (2017). Just How Strong is 2048-bit SSL Certificate Encryption? Accessed 15th of October 2017. Retrieved from: https://www.digicert.com/TimeTravel/math.htm

ESET (2017). Vulnerability CVE-2017-0144 in SMB exploited by WannaCryptor ransomware to spread over LAN. Accessed on 14th of October 2017. Retrieved from: https://support.eset.com/ca6443/?locale=en_US&viewlocale=en_US

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015, July). Cutting the gordian knot: A look under the hood of ransomware attacks. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 3-24). Springer, Cham.

Kurose, J. F., & Ross, K. W. (2017). *Computer networking: a top-down approach* (Vol. 7).

MalwareTech (2017). How to accidentally stop a global cyber attack. Accessed on 14th of October 2017. Retrieved from: https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html

Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. International Journal, 8(5).

O'Gorman, G., & McDonald, G. (2012). Ransomware: A growing menace. Symantec Corporation.

Smith, B (2017). The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack. Accessed on 14th of October 2017. Retrieved from: https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#sm.0001gnysbhjsod01z7q11hvz0xg2d

Symantec Security Response (2017a). Can files locked by WannaCry be decrypted: A technical analysis. Accessed on 14th of October 2017. Retrieved from:https://medium.com/threat-intel/wannacry-ransomware-decryption-821c7e3f0a2b

Symantec Security Response (2017b). What you need to know about the WannaCry Ransomware. Accessed on 14th of October 2017. Retrieved from: https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware