An Exploration of Ransomware

Technical Report by Reese Pearsall, Logan Pappas, Dallas LeGrande, Chris Cooper

Introduction

In the spring of 2017, Erie County Medical Center in Buffalo, New York was a victim of a cyber attack. The attacker encrypted all the files on the hospital's network so that employees could not access them. The attacker requested money in order to decrypt and release their files. The hospital did not comply with the request and did not send money to their attacker. Erie County Medical Center ended up getting access to their files later, but have spent around ten million dollars recovering from the attacker. This was just one of thousands of cyber attacks happening around the world where a "ransom" was required to be paid during the attack. These destructive and heinous computer viruses are known as ransomware. Ransomware is defined as "a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid." [2]

This particular type of malware is differentiated from an ordinary virus in that it creates leverage for an attacker to coerce the victim to trade money in exchange for the attacker to give up that leverage. The attacker usually encrypts the files on the victim's system and offers the decryption code after receiving money. In most cases, ransomware is spread through phishing emails or from a victim visiting an infected and malicious website. Ransomware attacks usually take a "shotgun" approach, which means that attacks target a large group of people instead of just targeting a single individual.

Purpose and Harm of Ransomware

Ransomware is a type of digital extortion,thus its main purpose is to extort some form of money from the victim. Ransomware is a rather unsophisticated type of malware, which makes it more appealing to both rookie and veteran cyber criminals. The ability for ransomware to attack and spread throughout a company also makes it an enticing option to cyber criminals who want to attack larger companies with multiple computers across a network.

Ransomware can be an incredibly crippling attack on a business, especially if they lack security response procedures and security infrastructure. First off, it can cause significant financial damage if the ransom is paid and also if the ransom is not paid.If a ransom is paid, there is no guarantee that the victim will receive back the decryption key, so the victim will have lost thousands of dollars and their files will still be encrypted. Secondly, if the ransom is not paid, it may lead to all important files getting deleted, which can be crippling for many businesses. In most cases, the largest portion of the financial cost comes after the encryption has been done. Companies will spend thousands trying to decrypt the files themselves, recovering files, and replacing infected equipment. Ransomware has been enough to entirely wipe out small businesses and make people quit their own jobs. When a small hearing center in Michigan was victim to a ransomware attack, all files were wiped after a $6,500 ransom was not paid.[6] This caused the doctors to close their business and quit their jobs.

Background and History

The first known ransomware virus was created in 1989 by Joseph L. Popp. This virus was known as the AIDS Trojan and the PC Cyborg, this virus sent 20,000 infected diskettes labeled “AIDS information - introductory Diskettes” to attendees of the world health organization during its international AIDS conference. This trojan used simple symmetric cryptography and was easy to stop but has evolved rapidly since then. In mid 2011, the first large scale ransomware outbreak began when anonymous payment services became more available. With these anonymous payment services such as Bitcoin, ransomware became a great method to extort money from its victims. In the first half of 2011 there were around 30,000 new samples of ransomware detected and that number doubled in the second half of the year. Ransomware made a big advancement in 2013 when it evolved and started to infect both android and IOS smartphones. With ransomware’s rapid advancement over the past 30 years, it is estimated that in 2019 a business will fall victim to ransomware every 14 seconds and by 2021 this number will go down to every 11 seconds.

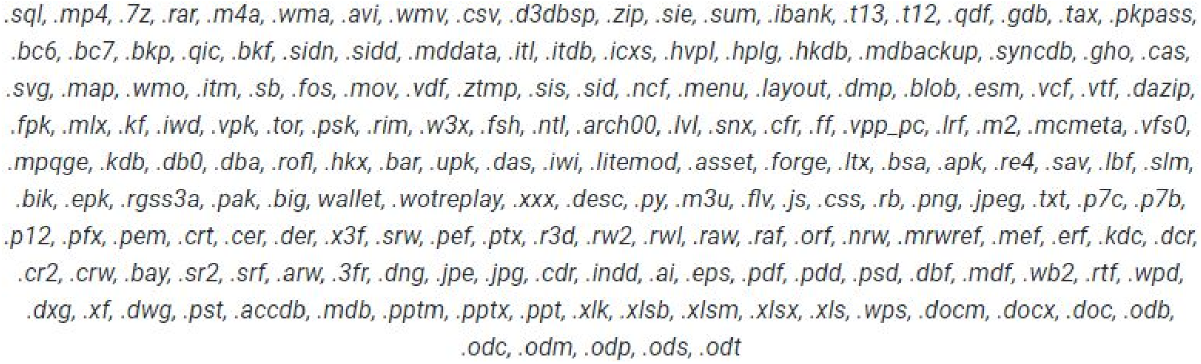
After ransomware became more viral in 2011, ransomware has cost business’s lots of money no matter the size of the business. Most ransomware attacks on small businesses go unreported but there are still millions of reports each year. In 2018 ransomware was estimated to cost businesses more than 8 billion dollars, up from just one billion in 2016. The average cost of a ransomware attack on businesses is $133,000 and overall has a minimum global revenue of 1 billion USD every year and rising.

What types of ransomware exist

There are two main types of ransomware: crypto ransomware and locker ransomware. The main purpose of crypto ransomware is to encrypt files on a victims computers or servers to deny access to them. Then demanding a specific amount of money, usually through an anonymous online currency like bitcoin, to unlock the victims files. There are multiple different types of crypt ransomwares that have different encryptions and different methods of execution but in general all use the same concept. Locker ransomware is different than crypto ransomware in the way that instead of using encryption this type of program locks the victims devices as a whole instead of encrypting what's inside. Similarly to crypto ransomware it forces the victim to pay an “unlock fee” to regain access to their device through anonymous payment services.

Encryption Implementation

The encryption scheme used in modern ransomware attacks if often a hybrid between different kinds of encryption. It uses both symmetric and asymmetric encryption, and does not require an internet connection for the encryption. The ransomware will generate a client public key and client private key for each computer during the infection. It will also have a server public key that will be hardcoded into the ransomware. The server public key will encrypt the client private key. When the encryption routine begins using an advanced encryption standard (AES) algorithm, all files will be encrypted and all AES keys will be encrypted using the client public key. For the files to be decrypted, the victim would need all the AES keys that were used during encryption. However, to get the AES keys, they will need the client private key, which is encrypted by the server public key. The server private key is what the victim will need to decrypt the file, which only the criminal has access to on the server. The list below includes the many different file extensions that can get encrypted by ransomware



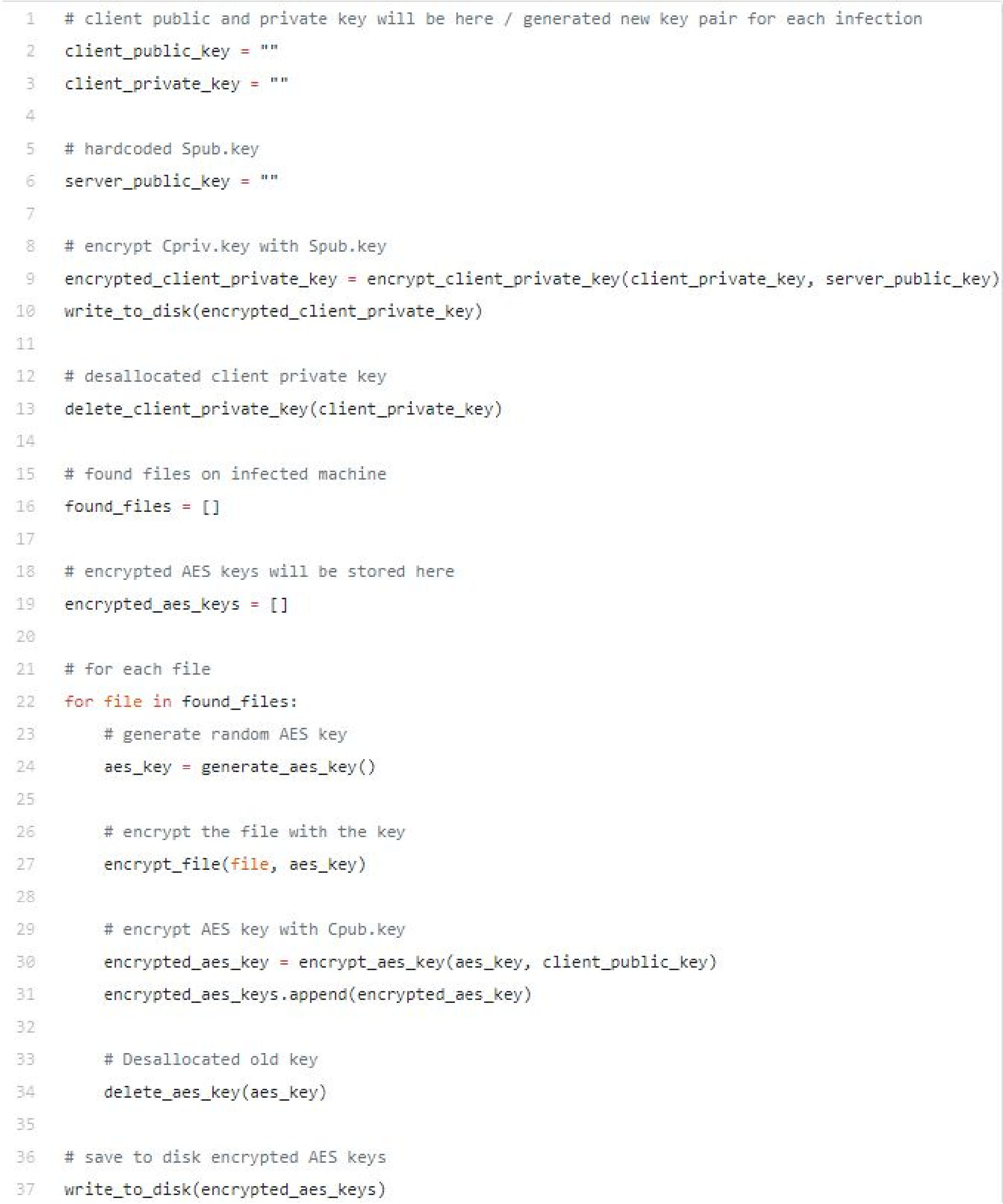
.sql, .mp4, .7z, .rar, .m4a, .wma, .avi, .wmv, .csv, .d3dbsp, .zip, .sie, .sum, .ibank, .t13, .t12, .qdf, .gdb, .tax, .pkpass,
.bc6, .bc7, .bkp, .qic, .bkf, .sidn, .sidd, .mddata, .itl, .itdb, .icxs, .hvpl, .hplg, .hkdb, .mdbackup, .syncdb, .gho, .cas,
.svg, .map, .wmo, .itm, .sb, .fos, .mov, .vdf, .ztmp, .sis, .sid, .ncf, .menu, .layout, .dmp, .blob, .esm, .vcf, .vtf, .dazip,
.fpk, .mlx, .kf, .iwd, .vpk, .tor, .psk, .rim, .w3x, .fsh, .ntl, .arch00, .lvl, .snx, .cfr, .ff, .vpp_pc, .lrf, .m2, .mcmeta, .vfs0,
.mpqge, .kdb, .db0, .dba, .rofl, .hkx, .bar, .upk, .das, .iwi, .litemod, .asset, .forge, .ltx, .bsa, .apk, .re4, .sav, .lbf, .slm,
.bik, .epk, .rgss3a, .pak, .big, wallet, .wotreplay, .xxx, .desc, .py, .m3u, .flv, .js, .css, .rb, .png, .jpeg, .txt, .p7c, .p7b,
.p12, .pfx, .pem, .crt, .cer, .der, .x3f, .srw, .pef, .ptx, .r3d, .rw2, .rwl, .raw, .raf, .orf, .nrw, .mrwref, .mef, .erf, .kdc, .dcr,
.cr2, .crw, .bay, .sr2, .srf, .arw, .3fr, .dng, .jpe, .jpg, .cdr, .indd, .ai, .eps, .pdf, .pdd, .psd, .dbf, .mdf, .wb2, .rtf, .wpd,
.dxg, .xf, .dwg, .pst, .accdb, .mdb, .pptm, .pptx, .ppt, .xlk, .xlsb, .xlsm, .xlsx, .xls, .wps, .docm, .docx, .doc, .odb,
.odc, .odm, .odp, .ods, .odt

List of File Extensions that get Encrypted during Ransomware [8]

Ransomware Code Analysis

One of the most prevalent examples of ransomware created was WannaCry. It was terribly efficient, compared to previous types of ransomware, because it used tools released from the NSA. WannaCry in particular affected windows machines after being run by the user on a machine, or finding an open RDP session on a machine with open RDP to the internet (a dangerous thing to do). Then, it created a service under the guise of “Microsoft Security Service 2.0” and starts the service. Within seconds, it has every file on the system encrypted. It then runs additional binaries hidden within the original program that run to delete all the original files off the system and finally display a message to the user. The user must then pay a bitcoin payment and the virus must be able to check in on the internet to verify the payment has been received.

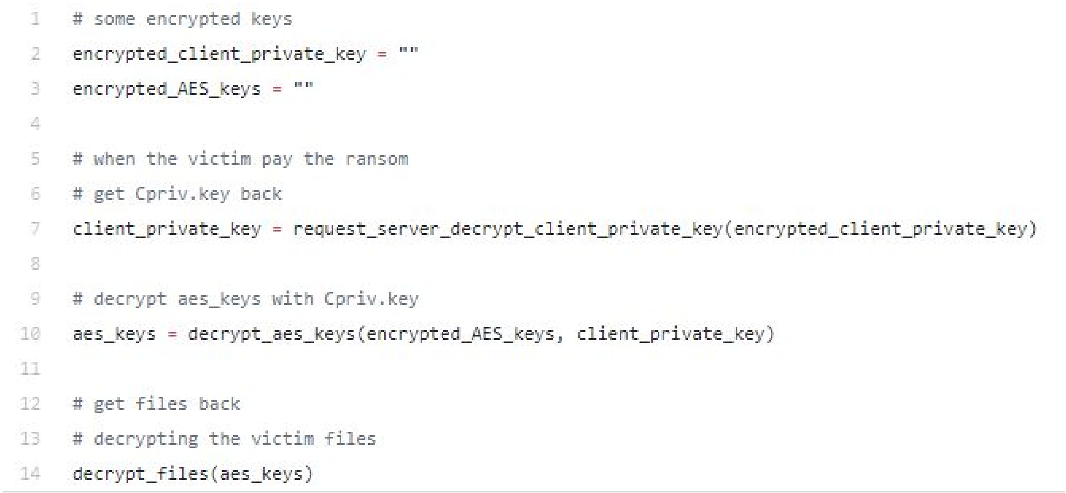
The encryption algorithm for ransomware can vary depending on when and who created the ransomware. The following code snippet below shows python pseudocode for how the encryption routine works during a typical ransomware infection



```
# client public and private key will be here / generated new key pair for each infection
client_public_key = ""
client_private_key = ""

# hardcoded Spub.key
server_public_key = ""

# encrypt Cpriv.key with Spub.key
encrypted_client_private_key = encrypt_client_private_key(client_private_key, server_public_key)
write_to_disk(encrypted_client_private_key)

# desallocated client private key
delete_client_private_key(client_private_key)

# found files on infected machine
found_files = []

# encrypted AES keys will be stored here
encrypted_aes_keys = []

# for each file
for file in found_files:
    # generate random AES key
    aes_key = generate_aes_key()

    # encrypt the file with the key
    encrypt_file(file, aes_key)

    # encrypt AES key with Cpub.key
    encrypted_aes_key = encrypt_aes_key(aes_key, client_public_key)
    encrypted_aes_keys.append(encrypted_aes_key)

    # Desallocated old key
    delete_aes_key(aes_key)

# save to disk encrypted AES keys
write_to_disk(encrypted_aes_keys)
```

Python Pseudocode for Ransomware Encryption Routine[8]

The code above follows the routine as explained in the previous section. It encrypts all files with AES keys and the AES keys get encrypted with the client public key, which needs the server private key, which only the criminal has access to. Next is how files will be decrypted if the ransom is paid.



```
# some encrypted keys
encrypted_client_private_key = ""
encrypted_AES_keys = ""

# when the victim pay the ransom
# get Cpriv.key back
client_private_key = request_server_decrypt_client_private_key(encrypted_client_private_key)

# decrypt aes_keys with Cpriv.key
aes_keys = decrypt_aes_keys(encrypted_AES_keys, client_private_key)

# get files back
# decrypting the victim files
decrypt_files(aes_keys)
```

Python Pseudocode for Decryption Routine[8]

The code retrieves the client private key to decrypt the AES keys. It retrieves it through the `request_server_client_private_key` function.

Solutions to Ransomware

The number one touted solution to ransomware is backups. Selecting the proper kind of backup depends on the needs of each business. An offline backup solution allows a business to maintain and secure their own information, without relying on a third party. If an offline backup is setup for a weekly rotation, this is the safest and easiest way to protect your computer or network from ransomware. The other option is a cloud solution for backups. This provides more security by entrusting a third party to protect against ransomware with backup revisions. Unfortunately, privacy can become an issue for companies with proprietary information—and you are restricted to the network bandwidth for backing up.

There are lots of companies and programs that provide ransomware protection and patching vulnerabilities is still a higher priority than even having the protection programs. One such protection program is called CrytoDrop [4]. CryptoDrop works by monitoring your files and looking for signs of ransomware. When ransomware is detected the program goes into lockdown mode which blocks all file access. You are then able to click a button to turn off lockdown mode if the program running is ok to run. It is recommended to do a backup at the time of lockdown to ensure that your files are safe if it is actually ransomware that is affecting your computer.

More techniques for combating ransomware include training employees to not click on email attachments or open emails from unrecognized people, good secure passwords [1] and ad blockers that keep users from clicking on click bait [3]. Attackers have been using the same techniques as advertisers in that they have some interesting video or story blurb that entices users to click on their links. Once the links are clicked the user is directed to a site where malware can be placed on their computer. This type of attack is called social engineering and is harder to prevent against since it targets users that are uneducated on malware and ransomware.

If you do get infected with ransomware and see that your files are being decrypted, you should unplug your network cable to ensure that the ransomware does not spread out into the internet. Ransomware tries to send itself out onto a users network and/or into the internet to be able to create the most havoc possible. Experts and the FBI say not to pay the ransom because paying the ransom tells the hackers that what they are doing is profitable and that they should continue doing it. Another reason not to pay the ransom is that there is no guarantee that the hacker will unlock your files after you pay them. Another option for combating ransomware once your computer is infected is to go to nomoreransom.org [5] where they have decryptors for some ransomware and will try to decrypt your particular ransomware if they do not have a decryptor already available.

Future of Ransomware

As the decade comes to an end, we have learned a lot about how existing malware propagates through a system and have created mitigations to prevent an infection from taking place and reducing the damage if it does happen. Most ransomware attacks are all untargeted attacks that are designed to cast a wide net against many different systems. Unfortunately, the future holds great potential for attackers to make more ransomware more efficiently. A.I. has already been used to defend networks against ransomware attacks, but that exact same software could be used by an attacker to penetrate an otherwise well-defended network. A.I. can adapt dynamically to different situations and find a unique weakness rather than try the exact same exploits with every system it comes across—making it harder to detect and much more efficient.

In addition, the IoT movement provides more potential security risks for every additional device added to the network. Without constant patches of all devices and vigilance from IT services, any device could be used as a pivot point for an attacker to breach a network. This could be a national security risk if, like WannaCry, the attackers are state sponsored hackers from Korea, China, or Russia. The future is an arms race, not of nuclear weapons, but of software that can control others.

References

[1] https://www.smarttech247.com/news/cryptodrop-can-stop-ransomware/

[2] https://www.us-cert.gov/Ransomware

[3] https://blog.malwarebytes.com/101/2016/01/hacking-your-head-how-cybercriminals-use-social-engineering/

[4] http://cryptodrop.findmysoft.com/

[5] https://www.nomoreransom.org/

[6] http://www.startribune.com/all-of-records-erased-doctor-s-office-closes-after-ransomware-attack/508180992/

[7] https://medium.com/@tarcisioma/ransomware-encryption-techniques-696531d07bb9

[8] https://malwaretips.com/blogs/remove-your-personal-files-are-encrypted-virus/