Authors:

- Matteo Di Fabio: 264339
- Luca Genovese: 264364

What is a Ransomware

The word ransomware indicates a class of malware that makes the data of infected computers inaccessible and asks for the payment of a ransom to restore them. Technically they are cryptographic Trojan horses (worm malware) and have as their sole purpose the extortion of money, through a "seizure of files", through the encryption that, in practice, makes the PC unusable. In exchange for a password that can unlock all content, it intends to pay a fairly high sum of money: generally the currency used is bitcoin (because is more difficult to track). The aim of the attackers is therefore to make money.

The most sophisticated ransomware uses hybrid encryption systems (which do not require sharing of keys between the two users) on the victim's documents, adopting a random private key and a fixed public key. The author of the malware is the only one who knows the private decryption key.

If the attackers don't give you the decryption key, you may be unable to regain access to your data or device.

How do you get ransomware

One of the main channels for spreading ransomware are the advertising banners of sites with adult content. But emails are also used (in a very similar way to phishing emails) that invite us to click on a certain link or download a certain file: email that is masked so that it is sent by someone we trust, for example a business colleague. Furthermore, cybercriminals rarely exploit vulnerabilities in various programs - such as Java, Adobe Flash and Adobe Acrobat - or in different operating systems. In the latter case, the malicious software propagates autonomously without the user having to perform any action.

The infection ways used by ransomware are basically the same as those used for other types of malware attacks.

The most common method is phishing emails (it work very well and is very simple): through this technique, which takes advantage of social engineering, over 75% of ransomware are conveyed. All of us will have happened to receive emails from shippers, or with false bills attached. They are obviously phishing emails, but statistics tell us that in 30% of cases these messages are opened by users and even in more than 10% of the cases the attachments or links in the emails are also clicked, thus allowing the infiltration of malware!

Another way is by browsing on compromised sites: the so-called "drive-by download" from sites where exploit kits have been introduced (by hackers who managed to violate the site) that exploit vulnerabilities of browsers, Adobe Flash Player, Java or others. They present themselves, for example, as advertising banners or buttons that invite us to click. At that point we will be directed to malicious sites, other than the original, where the malware download will take place.

Within (bundled) other software that is downloaded: for example, free programs that promise us to "crack" expensive software to use them without paying. It is a practice that has become very dangerous today, because the crack we are going to download will be an executable (.exe) inside which there could also be a bad surprise.

Finally exist also attacks through the remote desktop (RDP: remote desktop protocol, usually on port 3389): they are attacks with theft of credentials (usually of the "brute force" type) to access servers and take control of them.

Types of ransomware

Ransomware attacks can be deployed in different forms. Some variants may be more harmful than others, but they all have one thing in common: a ransom. Here are seven common types of ransomware.

- **Crypto malware**. This form of ransomware can cause a lot of damage because it encrypts things like your files, folders, and hard-drives. One of the most familiar examples is the destructive 2017 WannaCry ransomware attack. It targeted thousands of computer systems around the world that were running Windows OS and spread itself within corporate networks globally. Victims were asked to pay ransom in Bitcoin to retrieve their data.

- **Lockers**. Locker-ransomware is known for infecting your operating system to completely lock you out of your computer or devices, making it impossible to access any of your files or applications. This type of ransomware is most often Android-based.

- **Scareware**. Scareware is fake software that acts like an antivirus or a cleaning tool. Scareware often claims to have found issues on your computer, demanding money to resolve the problems. Some types of scareware lock your computer. Others flood your screen with annoying alerts and pop-up messages.

- **Doxware**. Commonly referred to as leakware or extortionware, doxware threatens to publish your stolen information online if you don't pay the ransom. As more people store sensitive files and personal photos on their computers, it's understandable that some people panic and pay the ransom when their files have been hijacked.

- **RaaS**. Otherwise known as "Ransomware as a service," RaaS is a type of malware hosted anonymously by a hacker. These cybercriminals handle everything from distributing the ransomware and collecting payments to managing decryptors — software that restores data access — in exchange for their percetage of the ransom.

- **Mac ransomware**. Mac operating systems were infiltrated by their first ransomware in 2016. Known as KeRanger, this malicious software infected Apple user systems through an app called Transmission, which was able to encrypt its victims' files after being launched.

- **Ransomware on mobile devices**. Ransomware began infiltrating mobile devices on a larger scale in 2014. What happens? Mobile ransomware often is delivered via a malicious app, which leaves a message on your device that says it has been locked due to illegal activity.

The origins and evolution of ransomware

- How did ransomware get started? While initially targeting individuals, later ransomware attacks have been tailored toward larger groups like businesses with the intent of yielding bigger payouts. Here are some notable dates on the ransomware timeline that show how it got its start, how it progressed, and which is the state of the art today.

- **PC Cyborg, also known as the AIDS Trojan, in the late 1980s**. This was the first ransomware, released by AIDS researcher Joseph Popp. Popp carried out his attack by distributing 20,000 floppy disks to other AIDS researchers. The researchers didn't know, these disks contained malware that would encrypt their C: directory files after 90 reboots and demand payment. Since PC Cyborg used symmetric encryption, it wasn't long before someone created a way to recover files. This ransomware is a Trojan horse that replaces the AUTOEXEC.BAT file, which would then be used by AIDS to count the number of times the computer has booted. Once this boot count reaches 90, AIDS hides directories and encrypts the names of all files on drive C: (rendering the system unusable), at which time the user is asked to 'renew the license' and contact PC Cyborg Corporation for payment .

- **GpCode in 2004**. This threat implemented a weak form of RSA encryption on victims' personal files until they paid the ransom. Using a 660-Bit RSA public key to encrypt or lock victims files, GPCode ransomware would prevent victims from accessing everything in the MyDocuments directory. GPCode required victims to pay a fee or ransom and in return a code or key would be delivered to the victims; which they would used to unlock their files. This version of ransomware is especially nasty because it can leave a backdoor open to other hackers. Furthermore, this gateway allows hackers to access important information such as secure documents, social security number, bank account numbers and credit card information.
- **Archievus in 2006.** Archievus targeted Windows users' "My Documents" folder, and used RSA encryption to ensure there was no easy way back. Victims had to make purchases from specific online sellers before being given the key to decrypt their data. As it turns out, the password was not unique to each victim, and once this was discovered the password was widely published, helping victims to recover their data.
- **WinLock in 2007**. WinLock was spread by another ransomware worm that imitated the Windows Product Activation notice. Rather than encrypting files, this form of ransomware locked its victims out of their desktops and then displayed pornographic images on their screens. In order to remove the images, victims had to pay a ransom with a paid SMS.
- **Reveton in 2012**. Based on the Citadel trojan (which was in turn based on the Zeus trojan), its payload showed a warning that appeared to be coming from the federal police (hence the name "police trojan"), stating that the computer had been used for illegal activities. The notice informed the user that to unlock their system, he would have to pay a fine using an anonymous prepaid credit service voucher. To heighten the illusion that the computer was under federal police control, the screen also showed the IP address of the car, and some versions even showed footage of the PC's webcam to make it appear that the user was also taken by the police.

  The attack begins with the victim being lured to a drive-by download website. Here, a dropper installs the Citadel malware on the target machine, which retrieves the ransomware DLL from its command-and-control center. Once installed on the victim's computer, the ransomware locks up the targeted machine and, as said above, displays a warning message notifying the user he or she has violated U.S. federal law (for example).
- **CryptoLocker in 2013**. This encrypted ransomware worm appeared in September 2013: it generated a pair of 2048-bit RSA keys, uploaded them to a command-and-control server and encrypted files with extensions contained in a particular whitelist. The malware then threatened to delete the private key if a payment had not been made via Bitcoin or prepaid vouchers within three days of the infection. Even after the deadline, the private key could still be obtained using an online tool (the price, however, had increased). CryptoLocker was isolated following the annihilation of the Gameover ZeuS botnet, officially announced by the US Department of Justice on June 2, 2014.

  CryptoLocker generally spreads as an apparently lawful and harmless e-mail attachment that appears to come from legitimate institutions, or is uploaded to a computer already part of a botnet. A ZIP file attached to the email contains an executable file with an icon and a pdf extension, making use of the fact that recent Windows systems do not show file extensions by default. Some variants of the malware may instead contain the Zeus Trojan, which in turn installs CryptoLocker. The first time the software is installed, it is installed in the Documents and Settings folder (or "Users" in the most recent Windows operating systems) with a random name and adds a key to the registry that puts it into automatic startup. He then tries to connect to one of the command and control servers. Once connected the server generates a 2048 bit RSA key and sends the public key to the infected computer. The command and control server can be a local proxy and pass through others, often occurring in different countries so as to make tracking difficult. The malware then begins to encrypt the files of the hard disk and network shares mapped locally with the public key by saving each encrypted file in a registry key. The process only encrypts data with some extensions, among them: Microsoft Office, Open document and other documents, images and Autocad files. The software then informs the user that it has encrypted the files and requests a payment with an anonymous and prepaid voucher, or using Bitcoin, to decrypt the files. The payment of the ransom allows the user to download a decryption software with the user's private key already preloaded.

- **TorrentLocker in 2014.** Another kind of cryptolocker malware is TorrentLocker. released around the end of August 2014 that targets all versions of Windows including Windows XP, Windows Vista, Windows 7, and Windows 8. When you are first infected with TorrentLocker it will scan your computer for data files and encrypt them using AES encryption so they are no longer able to be opened. Once the infection has encrypted the data files on all of your computer drive letters it will display a window that contains the ransom note and instructions on how to get your files back. TorrentLocker is distributed via emails that pretend to be shipping notifications, driving or speeding violations, or other corporate/government correspondence. Some emails will contain the malware installer as ZIP attachments or Word documents, while others will contain a link that will bring you to the associated fake site that will prompt you to enter a 5 digit code in order to download the shipping notification or violation notice. When you enter the code it will download a ZIP file that contain an executable that are disguised as PDF files. When the fake PDF files are opened they will infect your computer with the TorrentLocker infection and install malware files in the %AppData%, %Temp%, or %WinDir% folders. Once infected the installer will start to scan your computer's drive letters for data files. When TorrentLocker detects a supported data file it will encrypt it and then append .encrypted to the filename.

- **CryptoWall in 2014.** In September 2014, a new wave of the cryptolocker malware developed known as "CryptoWall", which mainly affected users in Australia. The worm spread through fraudulent emails, which showed themselves as notifications of non-delivery of parcels by the post company Australia Post; to avoid being identified by automatic scanners that check if the links on a page lead to malware, this variant required the user to visit a page and type a CAPTCHA code before downloading the payload

- **Locky in 2016**. So-called Locky ransomware used social engineering to deliver itself via email. When it was first released, potential victims were enticed to click on an attached Microsoft Word document, thinking the attachment was an invoice that needed to be paid. But the attachment contained malicious macros that will infect the computer encrypting files. More recent Locky ransomware has evolved into the use of JavaScript files, which are smaller files that can more easily evade anti-malware products.
  When Locky is first installed iit will connect to a remote Command & Control server that is under the Locky developer's control and send it the ID associated with the victim's infection. This ID is generated by taking the first 16 characters of a MD5 hash of the GUID for the storage volume that Windows is installed on. Once it sends the ID, Locky will respond with an RSA key that will be used during the encryption process. Locky will then create a Windows registry key that it will use to store configuration information. Locky will now scan the computer's local, removable, mapped drives, and unmapped network shares for file types that it targets for encryption. When a file is encrypted it will generate a new AES encryption key and encrypt the file with it. This AES encryption key is then further encrypted by the RSA key that was retrieved from the Command & Control server. This RSA encrypted AES key will then be stored in the encrypted file. When a file is encrypted it will be renamed to different formats depending on the version of Locky. Many of these extensions are named after gods from Norse and Egyption mythology.

- **Petya in 2016.** Petya is a family of encrypting ransomware that was first discovered in 2016. The malware targets Microsoft Windows–based systems, infecting the master boot record to execute a payload that encrypts a hard drive's file system table and prevents Windows from booting. It subsequently demands that the user make a payment in Bitcoin in order to regain access to the system. Petya's payload infects the computer's master boot record (MBR), overwrites the Windows bootloader, and triggers a restart. Upon startup, the payload encrypts the Master File Table of the NTFS file system, and then displays the ransom message demanding a payment made in Bitcoin. Meanwhile, the computer's screen displays text purportedly output by chkdsk, Windows' file system scanner, suggesting that the hard drive's sectors are being repaired. In essence, your files are still there and still unencrypted, but the computer can't access the part of the filesystem that tells it where they are, so they might as well be lost. At this point, the ransomware demands a Bitcoin payment in order to decrypt the hard drive.

- **WannaCry in 2017**. WannaCry, is a ransomware-type worm, responsible for a large-scale epidemic that occurred in May 2017 on computers with Microsoft Windows. Europol called it the biggest ransomware attack ever. WannaCry's attack did not spread via email like the previous ones, but took advantage of a Windows exploit developed by the NSA and called EternalBlue. This exploit was stolen and released to the wild. The attack targets vulnerabilities in the Windows SMB protocol. After it is installed on a computer, it begins to infect other systems on the same network and vulnerable ones exposed to the internet, which are infected without any user intervention. When it infects a computer, WannaCry encrypts the files by blocking their access and adds the .WCRY extension; it also prevents the system from restarting. At that point, in a file called @ Please_Read_Me @ there is a ransom note which the user must pay in bitcoin to unlock the files. The WannaCry ransomware encrypts all files stored on the affected machine. The encryption uses the AES 128-bit encryption algorithms, which are extremely difficult to break.

  It encrypts the following file types: .doc, .docx, .docb, .docm, .dot, .dotm, .dotx, .xls, .xlsx, .xlsm, .xlsb, .xlw, .xlt, .xlm, .xlc, .xltx, .xltm, .ppt, .pptx, .pptm, .pot, .pps, .ppsm, .ppsx, .ppam, .potx, .potm, .pst, .ost, .msg, .eml, .edb, .vsd, .vsdx, .txt, .csv, .rtf, .123, .wks, .wk1, .pdf, .dwg, .onetoc2, .snt, .hwp, .602, .sxi, .sti, .sldx, .sldm, .sldm, .vdi, .vmdk, .vmx, .gpg, .aes, .ARC, .PAQ, .bz2, .tbk, .bak, .tar, .tgz, .gz, .7z, .rar, .zip, .backup, .iso, .vcd, .jpeg, .jpg, .bmp, .png, .gif, .raw, .cgm, .tif, .tiff, .nef, .psd, .ai, .svg, .djvu, .m4u, .m3u, .mid, .wma, .flv, .3g2, .mkv, .3gp, .mp4, .mov, .avi, .asf, .mpeg, .vob, .mpg, .wmv, .fla, .swf, .wav, .mp3, .sh, .class, .jar, .java, .rb, .asp, .php, .jsp, .brd, .sch, .dch, .dip, .pl, .vb, .vbs, .ps1, .bat, .cmd, .js, .asm, .h, .pas, .cpp, .c, .cs, .suo, .sln, .ldf, .mdf, .ibd, .myi, .myd, .frm, .odb, .dbf, .db, .mdb, .accdb, .sql, .sqlitedb, .sqlite3, .asc, .lay6, .lay, .mml, .sxm, .otg, .odg, .uop, .std, .sxd, .otp, .odp, .wb2, .slk, .dif, .stc, .sxc, .ots, .ods, .3dm, .max, .3ds, .uot, .stw, .sxw, .ott, .odt, .pem, .p12, .csr, .crt, .key, .pfx, .der

- **NotPetya in 2017.** In June 2017, a new variant of Petya was used for a global cyberattack. The new variant propagates via the EternalBlue exploit, which is generally believed to have been developed by the U.S. National Security Agency (NSA), and was used earlier in the year by the WannaCry ransomware. The malware harvests passwords and uses other techniques to spread to other computers on the same network, and uses those passwords in conjunction with PSExec to run code on other local computers. Additionally, although it still purports to be ransomware, the encryption routine was modified so that the malware could not technically revert its changes. This characteristic, along with other unusual signs in comparison to WannaCry, prompted researchers to speculate that this attack was not intended to be a profit-generating venture, but to damage devices quickly.

- **Sodinokibi in 2019**. Ransomware remains a popular means of attack, and continues to evolve as new ransomware families are discovered. Sodinokibi encrypts a user’s files and can gain administrative access by exploiting a vulnerability in Oracle WebLogic (CVE-2019-2725). Sodinokibi starts by building a dynamic import table and ensuring that this is the only instance running currently on the system with the help of mutexes. Once the mutex check is passed, it decrypts the JSON config stored within the binary using RC4 and checks for the Boolean key value “exp”. If it is set to “true” Sodinokibi tries to run an exploit. In our case, the value of “exp” key is set to true so it proceeds to run the exploitation function. Before encrypting user files, Sodinokibi searches the entire file system and network shares for all directories named “backup” and wipes it out. Interestingly, before wiping all the files inside this directory it overwrites the content with random bytes to make file recovery impossible. Sodinokibi uses an Elliptic-curve Diffie–Hellman (ECDH) key generation and exchange algorithm to generate a private-public key pair. It uses this to generate a shared secret, which will be used as the key for symmetric encryption algorithms AES and Salsa20 which are used to encrypt different kinds of data. AES encryption is used to encrypt the private keys of the private-public key pair, which is generated locally on the user’s machine as well as the data sent over the network. Salsa20, on the other hand, is used for encrypting user files. Sodinokibi is shipped with two different public keys, one as part of JSON configuration and another embedded in the binary itself. These public keys will be used to encrypt the locally-generated private key.

Conclusion

To prevent this type of attack some simples actions can be taken: install and keep updater a professional antivirus, don’t click on unknown links, suspicious banner and advice. Don’t open untrusted mail and messages, even if the message is from a people that we know very well, but is a bit strange received from him. And finally another action that could be taken could be do periodic backup and check them, doing simulations of the attacks, trying to recover files from the backup periodically. This is very important as the last version of ransomware, remain silent for a long period (that could vary from the situation and the victim), search for an existing backup and encrypt it. Then when a new backup is created the ransomware encrypt even the new backup and so on, for periods that could last even months or year. At a certain point the ransomware reveal it’s presence, encrypting the file on the victim machine and ask for a ransom. The victim (that usually is a company in these case) thought to have valid backup, but doesn’t know that even all their backup are encrypted.

As we have seen all the ransomware encrypt different file, folder or part of the operating system, making the victim’s PC unusable. With the years more or less the strategy and the steps of attack are always the same, but as we notice the encryption algorithms become more and more complex, the key become more and more long (a greater number of bits used) in order to avoid to break the encrypt using brute force. In fact the algorithms become more complex while the computational power increase with years (it is a constant challenge between encryption algorithms and computation power to do brute force). So for example for the last discovered ransomware: *Sodinokibi* that use Elliptic-curve Diffie–Hellman (ECDH) key generation, it’s pretty impossible to break using brute force, as this algorithm is designed to resist to quantic processor brute force attack. This is due to the fact that ransomware can exist while the victim (or government) can’t force the encryption using brute force, otherwise the attacker can’t ask a ransom, because the victim, in this case, using a very big computational power can decrypt the files. So imagine that the government (or a private company) has a super computer that in few days can find the key and decrypt the files of a victim, at this point the victim don’t pay the ransom to unlock the file and the ransomware attack would no longer make sense. For this reason the encryption algorithms become more and more complex with years, to face the increasing hardware technology development.

Another aspect to consider is also that even if you pay the ransom after an attack, you don’t have the assurance to recover your files because if the criminal is very bad he doesn’t unlock your file even if the victim pays, but this is not good for him, because in this way he lost credibility, he create a damage to people, but then they won’t want to pay him anymore because it is useless as the criminal does not respect the agreements.

Finally ransomware business is very complex: the criminals have to do a lot of analysis on the value of ransom in fact this is the main point of this kind of attack.

We will, therefore, assume that the objective of the cyber-criminals is to maximize profit. Given that it is relatively costless to attack victims and there is little chance of being caught, the main variable the criminals can control is the size of ransom. This will, therefore, be the focus of our analysis. Note that in taking this approach, our analysis is best suited to randomly distributed attacks, such as Cryptolocker , that is designed to infect as many computers as possible, and where the criminal has very limited information about victims before the attack. In this setting, the criminals maximize profit, as we shall see shortly, by setting a ransom based on ‘average’ WTP (willing to pay) a ransom across the population. Our approach is less well suited to precisely targeted attacks in which a particular organization or firm is targeted for extortion (such as a university or health trust). In this setting, the criminals are likely to have more precise information on the ransom the victim may be willing to pay.

The profit that criminals can make largely depends on the willingness of those attacked to pay the ransom. This, in turn, will depend on various components—how important the files are to the victim, whether they have a recent backup, how much liquid money they have available, the extent to which they trust the criminals to honor their word, willingness to give money to criminals, etc. From the criminal's perspective, however, it is irrelevant why people are, or are not, willing to pay a ransom. All that matters is the maximum amount a particular victim is willing to pay to recover their files. Different people will naturally have a different WTP, and so we denote by vi the WTP of person i. For instance, a victim who values her files at $500, has no recent backup, and trusts the criminals will return her files would have vi = 500 while a victim who values her files at $1000 but has a recent backup, or does not trust the criminals and dislikes interacting with criminals may have vi = 0.

The revenue of the criminals can then be summarized as:

$$\Pi=\sum i=1N(pi-c)1i-F$$

where N is the number of people attacked, pi is the ransom asked of person i, c is the cost of dealing with any ransom money and providing a service to victims, 1i is an indicator variable that takes value 1 if pi ≤ vi and 0 otherwise, and F is the fixed cost of operating the malware. In the following, we shall abstract away from considering N and simply take it as given that the criminals will target as many people as possible. Our focus will, thus, be on deriving the optimal ransom to charge victims. Note that we also abstract away from dimensions other than money, such as the amount of time and effort a victim would be willing to devote to dealing with the criminals, obtaining Bitcoin, etc.

Survey estimates suggest that anything up to 40% of victims paid the ransom and around two-thirds of those recovered their files after paying the ransom. While the precise proportion of victims who paid ransoms is unknown, it is clear that enough people paid the ransom to generate a large amount of money. Conservative estimates on the amount of ransom received by the criminals range from $300 000 to over $1 000 000. We also know that a single Bitcoin address connected with cryptolocker received a total of 346 102 BTC at the time of its last transaction in February 2014. This was a significant proportion of the total number of Bitcoins in circulation (approx. 12 million) and would have had a valuation in excess of $200 m.

Bitcoin allows for relatively easy money transfers and, although by no means untraceable or completely anonymous, it is considered to be secure enough to provide a good degree of anonymity. These characteristics provide cyber-criminals with a very powerful tool for profiting from their crimes, and one that law enforcement is not that accustomed to. They can use Bitcoin to defeat the classical control measures already put in place to trace, follow and stop other, better-known payment methods such as bank transfers.

According to Cybersecurity Ventures research in 2017, in every 40 s, a business falls prey to a ransomware attack and the rate is predicted to rise to 14 s by 2019. Business organizations have had to pay cyber criminals even up to $1 million in a single attack, while others have incurred losses in hundreds of millions of dollars.

Below we can see an estimation on the turnover of ransomware: the table shows the top 15 ransomware types by total payment received between 2013 and mid-2017; a conservative estimate of the size of the ransomware market was at $12,768,536.

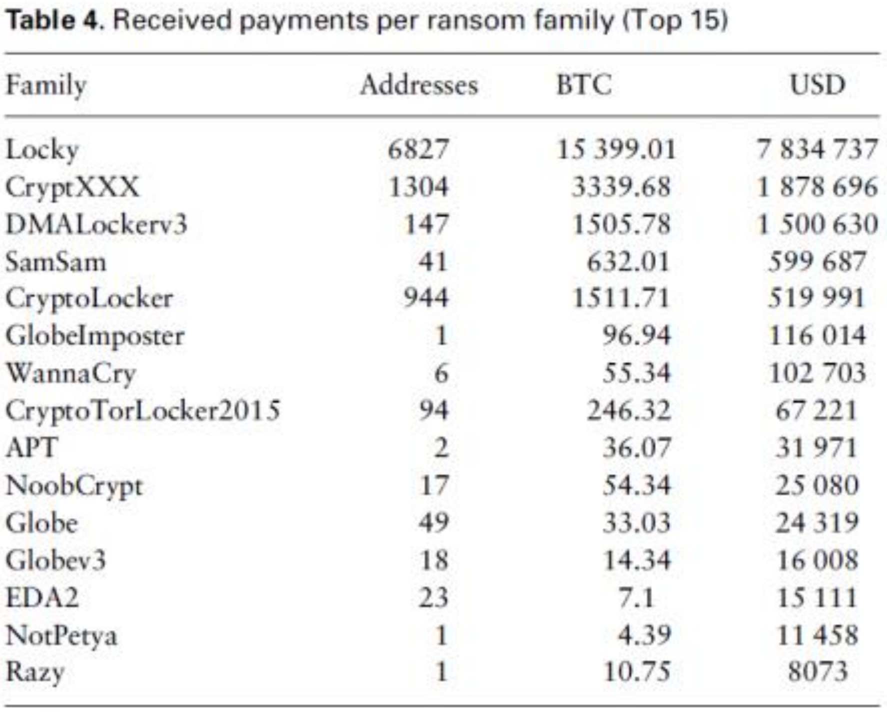

Table 4. Received payments per ransom family (Top 15)

Family	Addresses	BTC	USD
Locky	6827	15 399.01	7 834 737
CryptXXX	1304	3339.68	1 878 696
DMALockerv3	147	1505.78	1 500 630
SamSam	41	632.01	599 687
CryptoLocker	944	1511.71	519 991
GlobeImposter	1	96.94	116 014
WannaCry	6	55.34	102 703
CryptoTorLocker2015	94	246.32	67 221
APT	2	36.07	31 971
NoobCrypt	17	54.34	25 080
Globe	49	33.03	24 319
Globev3	18	14.34	16 008
EDA2	23	7.1	15 111
NotPetya	1	4.39	11 458
Razy	1	10.75	8073

(Paquet-Clouston, M., Haslhofer, B., & Dupont, B. 2019)