New directions in the ransomware phenomenon

Mihai-Andrei Costandache[1], Marian-Ștefan Mihalache[1], and Emil Simion[2]

[1] Faculty of Computer Science, Alexandru Ioan Cuza University of Iași:
{mihai.costandache, marian.mihalache}@info.uaic.ro
[2] Politehnica University of Bucharest: emil.simion@upb.ro

Abstract. Ransomware is a type of malware that blocks an user's access to files and requests him/her a ransom. The main approach of an attacker is to encrypt the user's files and give him/her the decrypting tool only after he/she pays the requested amount of money. The payment is usually done in difficult to trace currencies. In this paper, we provide a review of the ransomware phenomenon, making a clear distinction between the threats before and after WannaCry (which appeared in May 2017). Initially, we give two taxonomy examples from the literature and one designed by us. The first two taxonomies use "Platform", "Cryptosystem"/"Crypto", "Severity", "Attack" and "Target" as criteria (the terms appear in one of them or both), but we have chosen "Target Zone", "Propagation", "Payment" and "Weakness". We further describe/compare ransomware programs, taking into account several aspects including how they work (e.g., encryption methods), whom they target (e.g., individuals/organizations), what impact they have and what weaknesses can be used to provide countermeasures (besides the general prevention techniques that we mention briefly).

Keywords: cyberattack · ransomware · encryption · AES · RSA

1 Introduction

Over the years more and more cyberattacks have been focusing on capturing the users' data for malicious purposes like using it without consent, deleting it or even harassing the users with the captured data. This paper approaches the ransomware phenomenon, that covers all these purposes (especially the harassing part). The analysis provides many ransomware threats examples, in order to illustrate our findings. It is worth mentioning that the examples have their appearance date specified, between parentheses, as the chronological aspect is very important. We have structured the presentation as follows: 1. Introduction - the current part, 2. Ransomware taxonomies - presents two existing taxonomies plus ours, 3. Ransomware before WannaCry - presents an analysis over the existing ransomware appeared before WannaCry (we discuss implementation methods, targets, infection methods, ransom retrieval, impact and countermeasures), 4. WannaCry - provides an overview of this threat, as it is a reference point for our research, 5. The new directions of ransomware after WannaCry - exposes an analysis of the new generation of ransomware following the same path from the section concerning the older threats, 6. Conclusions - has some remarks regarding the new directions in the ransomware phenomenon, Appendix A - presents the dataset standing at the base of this paper, ransomware threats ordered by appearance time.

2 Ransomware taxonomies

In order to understand the evolution of ransomware, we must analyze from multiple criteria the threats encountered over the years in this domain. Taxonomies help us identify the relevant criteria. Several taxonomies exist in the literature, two examples are in [1] and [2], that can be seen in Fig. 1 and in Fig. 2, respectively. These two taxonomies have small differences. There are certain nuances regarding the "Cryptosystem" and "Severity" criteria from the former and the "Severity", that includes "Crypto", criterion from the latter, but the main ideas are the same. Also, the first taxonomy describes the "Attack" technique, while the second taxonomy introduces the "Target" criterion.

Fig. 3 shows our taxonomy, that focuses on other aspects than what we have presented so far.

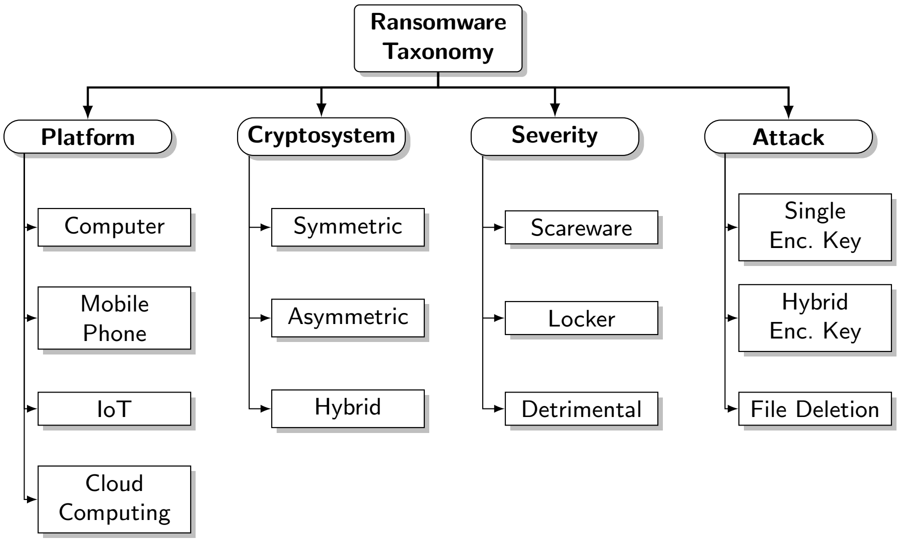

Fig. 1. Existing Ransomware Taxonomy 1

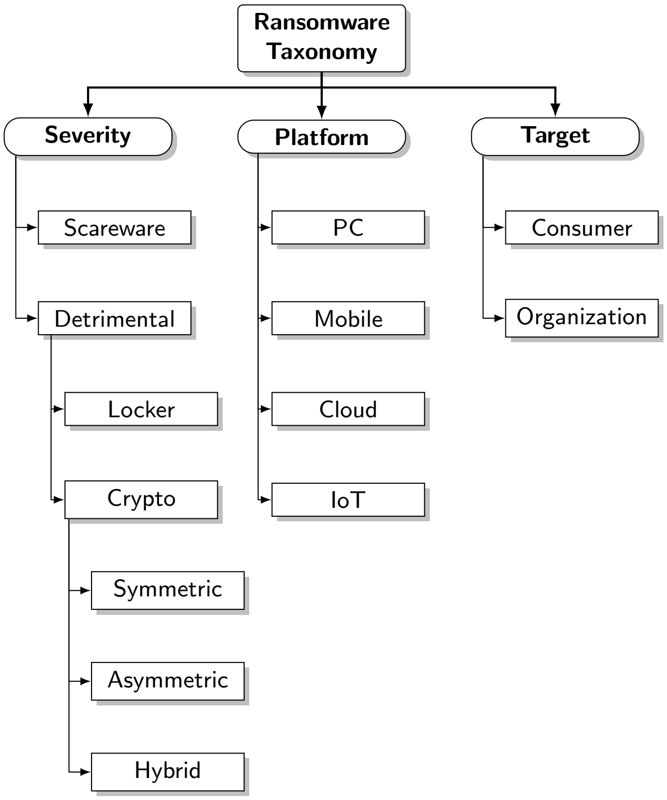

Fig. 2. Existing Ransomware Taxonomy 2

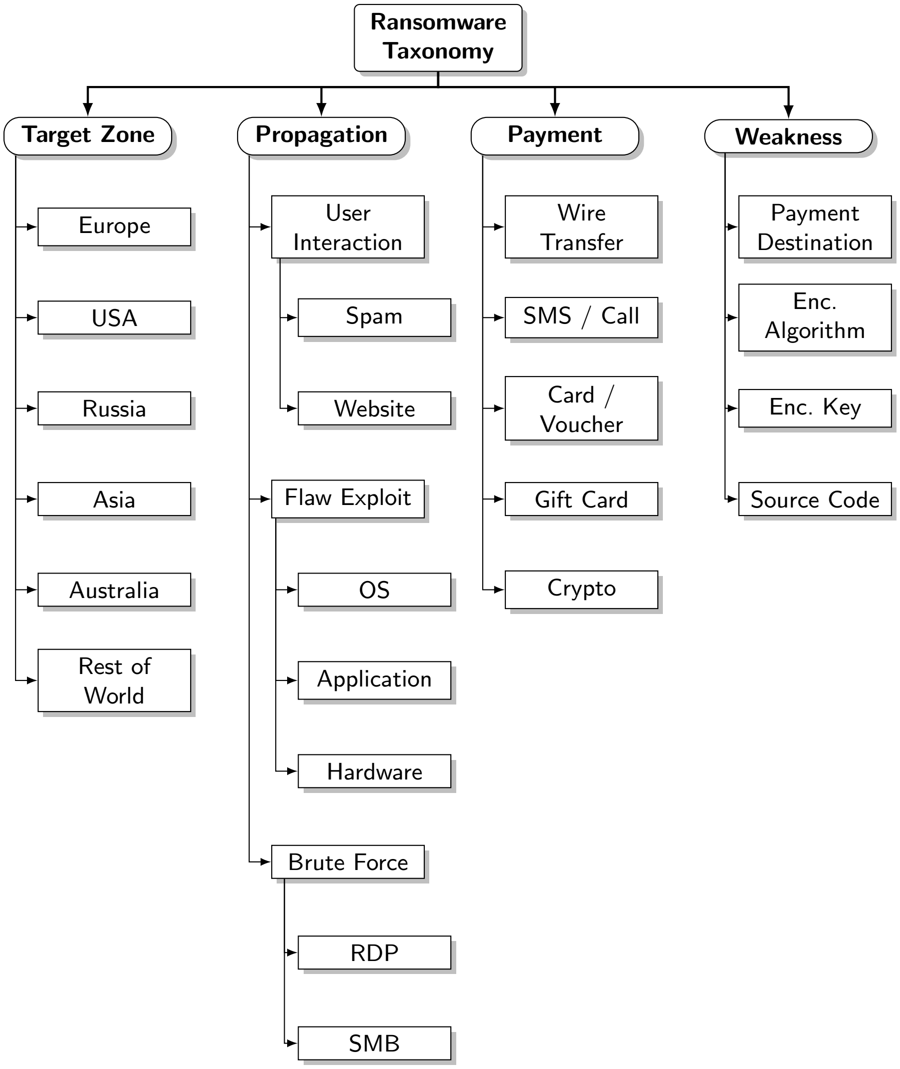

Fig. 3. Our Ransomware Taxonomy

3 Ransomware before WannaCry

3.1 Overview

WannaCry was a large scale attack that brought to our attention the ransomware threat. However, the ransomware danger had appeared a long time ago and it had targeted a lot of regular users and organizations. We present how the ransomware threats worked before WannaCry, by answering some important questions.

In order to understand the context, we provide a short description of the first ransomware threat. This description covers the ransomware analysis from multiple points of view, but in the following subsections, we answer each of the relevant questions separately.

The first ransomware is considered to be AIDS Trojan [7], launched in December 1989. Dr. Joseph L. Popp obtained the mail subscriber lists to World Health Organization AIDS conference and PC World Magazine. He then sent his victims infected floppy disks, disguised as survey programs about the AIDS virus. Each disk contained two files written in QuickBasic 3.0 - the survey and the installer for the malware. The malware altered the names of all the files (not the files themselves) within the C: drive using symmetrical encryption. The files were prevented from being executable, as the extension name had been modified. The user was told that his/her lease for software from the PC Cyborg Corporation had expired and he/she must renew it. Popp asked his victims to send their payments to a post office box in Panama. The unusual payment method contributed to the failure of the attack regarding the income. However, the attack produced a lot of damage, as several users deleted their files. The malware was easy to remove and a month after its appearance, softs for malware removal and files decryption were available.

3.2 How were the threats implemented?

There were various implementation methods. For the encrypting ransomware attacks, the encryption algorithms and keys were important aspects too.

Gpcode [8], a trojan which appeared in May 2005, created a startup key for its file in Windows Registry and used a simple encryption technique. Gpcode.AG [9], from June 2006, used RSA, with a 660-bit encryption key. Among other ransomware threats using RSA were two from 2013, CryptoLocker [24] and CryptoLocker 2.0 [26], with a 2048-bit and 1024-bit key pair, respectively. Different algorithms than RSA were also used. For example, Curve-Tor-Bitcoin Locker [27], discovered in midsummer 2014, used elliptic curve cryptography (hence the first part of the name). Locky [33] and Zepto [34], both launched in 2016, used AES with keys encrypted with RSA. Zepto used the same methods of spreading and redemption (but with a higher demand) as Locky, appearing to be created by the same team of hackers.

Krotten [16], a non-encrypting threat from September 2005, modified the Windows System Registry. Therefore, it disabled the registry editor, Control Panel and Windows Task Manager, prevented the user from closing Internet

Explorer and from accessing file and folder configuration, modified the Start Menu, etc. Other non-encrypting threats are those which ”scammed” or ”scared” users. In 2011, there was reported a trojan imitating the Windows Product Activation notice [20]. Some attacks consisted in accusing the victims of doing something illegal. FBI MoneyPak Ransomware [23] (March 2012, also known as Reveton) brought charges of pirated software or illegal pornography and ”fined” the victims. OS-X Trojan [22] (July 2013) acted in a similar way. The notices usually locked the users out of their computers.

According to [45], ransomware threats can be paired together with Advanced Persistent Threats (APTs), even though there are important differences between them, in terms of their targets, intention of alerting the victims of their presence or not and purposes. APTs have certain targets, stay undetected for a significant time period on the infected computers, launch the attacks at the right moments and usually steal information (e.g., accounts, passwords). DynA-Crypt [45,46] (February 2017) was the first-of-its-kind malware that used both the APTs and ransomware approaches. It encrypted, stole and/or deleted files from the victims' computers and even spied the users (e.g., by recording system sounds and logging typed commands). DynA-Crypt left files and processes running (the APT component) on the hit systems, allowing the attack to continue at any time. Generally speaking, APTs are harder to detect if they run on a schedule. The APTs may not be running at the time of analysis with forensic tools and therefore, may not be detected.

3.3 Who were the targets?

The victims were individuals and organizations. From what we have found, targeting individuals was the most popular choice and only in the more recent years of the time period studied in this section, some ransomware attacks directed towards organizations took place. According to [3], in the 2015-2016 time period among the victims were three Greek banks, Hollywood Presbyterian Medical Center, Ottawa Hospital, Kentucky Methodist Hospital, Chino Valley Medical Center, Desert Valley Hospital and San Francisco Municipal Transportation Agency.

A part of the ransomware authors focused on certain countries when choosing the victims, as most attacks were reported in particular locations. Gpcode.AG [9], Krotten [16], WinLock [18] (August 2010) targeted Russia, while Locky [33], on the contrary, did not attack the systems using Russian language. Cryzip [14] (March 2006) attacked people in U.S.A, MayArchive [14] (May 2006, a Cryzip variant) attacked people in U.K, while CryptoDefense [29] (February 2014) targeted both. It is worth mentioning that there was another threat, called Archiveus [15], that seemed to use some parts of Cryzip (and also appeared in the same year).

3.4 How were the victims infected?

During our research, we have noticed that most of the attacks involved user interaction. Basically, the ransomware infection files were ”carried” by spam emails and websites. The user had to download, open and/or execute the files in order for the attack to take place. CryptoLocker [24] spread by downloads from compromised websites and email attachments sent via a botnet called GameOver ZeuS. Locky [33] was based on emails having attached a Word document which used macros or a ZIP file containing a Javascript installer. Opening/executing the files triggered the attack. However, Locky did not always need user interaction, as it could also attack through hacked sites with an exploit kit on them. The exploit kit used vulnerable programs on the victims' computers without their knowledge. Spora [35] (January 2017) used email attachments in the form of a ZIP file that contained HTML Application (HTA) files. The files had double extensions, therefore the users sometimes saw only the first extensions (e.g., PDF) and opened the files. Opening any of the files started the ransomware process.

Ransomware also spread by exploiting security flaws and/or brute-forcing the user credentials. SamSam [43] appeared in 2016 and exploited at first a vulnerability in JBoss host servers. In 2018 (not in the time period analyzed in the current section), other infection channels, consisting of more flaws and the use of brute-force, appeared for this threat.

3.5 How did the criminals get the ransom?

The success of the attack was strongly connected to the inability to seize the ”place” where the ransoms were collected or to the trace the authors.

The trojan which imitated the Windows Product Activation notice [20] asked the user to call a phone number, as if it were from Microsoft. The call was billed at a high rate, even though the user was told the call was free of charge. Similarly, other early ransomware threats had a premium-rate SMS approach.

Another method to collect the ransom back then was to use pre-paid cards, vouchers or gift cards. CryptoLocker [24] and FBI MoneyPak Ransomware [23] accepted payments using Ukash, Paysafe and MoneyPak.

The anonymous online network Tor and the cryptocurrencies led to a better, almost untraceable way of getting paid for the attackers. Among the more recent threats, this combination was the most popular choice. CryptoLocker [24], mentioned earlier, accepted Bitcoin too. Curve-Tor-Bitcoin Locker [27], SynoLocker [23] (August 2014) and Spora [35] are only some other examples.

3.6 What was the impact?

Even before WannaCry, the ransomware phenomenon had a great impact. The first ransomware attack, which may seem ”primitive” now, still caused a lot of damage. The threats in the following years got more advanced and therefore more dangerous.

The following items are some key stats [3]:

- Between September and December 2013, the CryptoLocker strain hit more than 250,000 systems. The attackers earned more than $3 million before the Gameover ZeuS botnet was taken down.
- From April 2014 through early 2016, CryptoWall and its variants attacked hundreds of thousands of users. By mid-2015, CryptoWall had collected over $18 million.
- Attackers demanded more money from large companies/organizations. For example, in 2015 three Greek banks were supposed to pay $7 million each but they refused.

3.7 What were the countermeasures?

Generally speaking, users should not open/execute any suspect files and should regularly take backups and update software (as security patches are provided). According to [4], the users who get infected should not pay the ransom, as paying does not guarantee the files recovery, it encourages the criminals to continue their attacks and some ransomware threats can be defeated by decryption tools. We consider that these recommendations should also be followed in the present.

In some cases, security experts could exploit mistakes made by the attackers. Payment destinations not chosen properly were seized by the law enforcement agencies (and criminals most likely captured), "weak" encryption algorithms and key(s) led to relatively easy decryptions (e.g., by brute-force) and unusual programming decisions sometimes ruined the whole attacks. For example, CryptoDefense [29] used the Windows CryptoAPI to produce its key pair on the infected system. The decryption key, sent to the attacker's server, remained on the victim's computer and security experts used this flaw in their advantage.

3.8 What did we learn?

The attacks were primitive at first, yet effective. The victims were most of the time individuals. Some of them were convinced to pay the ransom, while others were not. Many users lost their files, with or without paying, as following the instructions from the attackers did not guarantee the recovery of the files (even though the victims were not told that). Therefore, the damage was done. Since the ransomware threats first appeared, their impact kept growing and countermeasures were more and more needed. Users were encouraged not to trust certain emails or websites and not to pay the ransom.

It is worth mentioning that some ransomware attacks were similar (parts of code were reused, the spreading technique was the same, etc.).

4 WannaCry

WannaCry, the reference point for our research, was a ransomware threat most people have heard of. However, we consider that a brief description, based on the article in [39], is needed in order to understand the context of the paper.

WannaCry, an encrypting threat, appeared in May 2017 and targeted Microsoft Windows users (both individuals and organizations). Older Microsoft Windows versions had a certain weakness that made them vulnerable to a hack, known as Eternal Blue. Before the WannaCry attack, a group of hackers called the Shadow Brokers made it public. Allegedly, the Eternal Blue hack was developed by the NSA (United States National Security Agency). A backdoor called DoublePulsar [40] was also involved in the attack and exactly as in the case of Eternal Blue, it was made public by the Shadow Brokers and allegedly created by the NSA. Microsoft had released a patch addressing the exploit two months before the attack began, but many users did not update their systems, therefore they were vulnerable.

The payment method chosen by the attackers was by the Bitcoin cryptocurrency. Victims were told that unless they paid the ransom within three days, their files would be lost. One of the reasons it is recommended not to pay the ransom is that the recovery of the files is not guaranteed and WannaCry is a great example of this principle. According to the code, there was no association between a victim and his/her payment. There is still no consensus about whether some victims got their files back or not.

The impact of WannaCry is illustrated by the following facts:

- It hit around 230,000 computers, in 150 countries.
- One of its victims was the United Kingdom National Health Service (NHS). It was estimated that the cancellation of 19,000 appointments costed the NHS £92 million.
- It caused $4 billion in losses globally.

WannaCry was one the biggest cyberattacks and has caused a great evolution of the ransomware phenomenon. Therefore, we consider that WannaCry is an excellent reference point for the history of ransomware.

5 The new directions of ransomware after WannaCry

5.1 Overview

WannaCry had a great impact at the time of its launch and has led to more dangerous ransomware, in terms of the number of targets and the obtained money. We present how ransomware has evolved, considering the questions from the analogous section. Multiple changes can be noticed. For example, organizations are more targeted than they were before and for collecting the ransom (both from individuals and organizations) other methods than by cryptocurrencies seem to be barely used.

5.2 How are the threats implemented?

There are diverse implementation techniques and, most importantly, the Ransomware as a Service (RaaS) model, which allows the customization of threats under various aspects, has been getting more and more popular. The main idea of the RaaS model [52] is that ransomware developers offer creator kits to other people. Even those with no technical knowledge can easily make their own versions of threats (with particular redemption note language, ransom value, etc.), as the attackers provide a web-based interface, 24-hour support, call center assistance, documentation and tutorials. In the recent years, the developers who offer these services have changed their approach to making money: instead of requesting payments before giving the creator kits, they ask for a part (e.g., 30%) of the ransom earnings made by the clients.

BitPaymer [51] (August 2017) used 128-bit RC4 to encrypt the files and 1024-bit RSA to encrypt the keys, but newer versions used 256-bit AES to encrypt the files and 4096-bit RSA to encrypt the keys. Sekhmet [54] (June 2020) used a combination of RSA-2048 and ChaCha encryption algorithms. Interestingly, some threats present similarities. DopplePaymer [51] (April 2019), a threat related to BitPaymer, used 256-bit AES and 2048-bit RSA to encrypt the files and keys, respectively and also shared significant code parts. According to CrowdStrike, Bad Rabbit and NotPetya's dynamic link library (DLL) shared 67% of the same code [42]. Nephilim and Nemty had similar code, design and attitude and they threatened the victim that they will publish sensitive data [54].

5.3 Who are the targets?

The targets are still individuals and organizations, like it was presented in the analogous section. However, attacks towards organizations are more popular than they were before. Ryuk [50] (August 2018, operated by the group Wizard Spider), GandCrab [52] (January 2018), CLOP (February 2019), Maze [54] (May 2019), Tycoon (at least December 2019), Nephilim (2019), NetWalker (2019/2020, also known as Mailto) and Sekhmet (June 2020) (all but the first two threat mentions are based on [54]) are only some examples. Sometimes, the ransoms are open for negotiations. Also, there are cases in which organizations do not just have their files encrypted, they are also threatened that their data will be disclosed.

The geographical location remains after WannaCry a factor in choosing the victims. For example, CLOP [55] did not attack users from the Commonwealth of Independent States (CIS), which includes countries such as Russia and Kazakhstan.

5.4 How are the victims infected?

The customization of threats made possible by the RaaS model has led to diverse ransomware spreading methods. For example, the attackers who purchased Nemty [54] (summer 2019) created their own versions of the threat and also chose their own infection techniques. Nemty developers obtained 30% of the paid ransoms.

Most of the attacks require the user's interaction with infected files, attached to spam emails or hosted on websites, or his/her visit of websites with exploit kits on them. According to [52], GandCrab mostly spread by spam emails and popular web-based exploit kits, such as RIG and GrandSoft. The same source states that, in addition, some ransomware threats (including GandCrab) use botnets. NetWalker [54] propagated by coronavirus phishing emails and executable files spreading through networks. Maze [54] used the exploit tools called Fallout and Spelvo.

Exploiting security flaws and brute-forcing the user credentials are other infection methods. Modified Petya [37] (June 2017) used the same EternalBlue exploit as WannaCry and Sodinokibi [58] (Sept 2019) propagated at first by exploiting a vulnerability in the servers of Oracle Weblogic. GandCrab [52] used brute-force sometimes.

5.5 How do the criminals get the ransom?

After WannaCry, given the increasing popularity and number of options of cryptocurrencies, other payment methods seem to be barely used. Actually, during our research, we have not found examples of attackers collecting ransoms in more traditional ways. Bitcoin is the most popular among the cryptocurrencies (around 98% of payments) [5]. According to [52], GandCrab also accepted Dash, a forked Bitcoin protocol with faster transactions that are untraceable. By studying the ways of collecting the ransom, relationships between ransomware threats may be identified. The association between BitPaymer and DoppelPaymer, two related threats mentioned in another subsection, is a good example. The note warning the user about the redemption requested by DoppelPaymer was similar to those used by the original BitPaymer in 2018 and the payment portal was almost identical [51].

5.6 What is the impact?

The ransomware attacks cause many lost and/or leaked files and huge financial losses. As the number of Internet users keeps growing and new payment methods appear, it is obvious that the number of ransomware threats, the number of victims and the incomes increase.

The following stats show why individuals and organizations need to worry about the phenomenon:

- In a recent study, SonicWall identified more than 153,000 new ransomware variants [6].
- A Barracuda report from recent years stated that 47% of UK businesses have been affected by ransomware attacks at some stage [6].
- BBC wrote that Danish company Demant lost around $85 million due to a ransomware attack, as the company lost access to 22,000 computers in 40 countries and the employees had to use pen and paper until the problem was resolved [5].
- Cybersecurity Ventures predicted ransomware financial damage will be $6 trillion annually by 2021 and that an attack will take place every 11 seconds on average [5].

5.7 What are the countermeasures?

Even against the latest ransomware threats, good practices such as not opening/executing files if they are not from trusted sources and regularly taking backups and updating software, are usually still effective. Organizations should also invest in security solutions in order to avoid breaches in their IT infrastructure and employees should be instructed on how to use the systems properly. These approaches may protect the organizations against other threats as well, not just ransomware.

Ransomware attacks are getting more professional these days. Their progress is partly due to the RaaS model, as some attackers purchase already well developed programs (they may be also customized), created by hacker groups. Even if they become more advanced, ransomware threats may still have the flaws indicated in the section concerning the older attacks. For example, the source code of CLOP [55] made the security experts think the attackers were not experienced programmers. The code that was in charge of deleting the ransomware from the disk did not wait for it to finish. As the ransomware was still running, it could not be deleted. A timeout command would have solved the issue. Another weird decision was the use of a .BAT file for certain actions, as the external file could have been found and removed. Also, it was unusual that the ransomware checked the names of the folders/files against hardcoded hashes, considering that later, for the resources that were files and not folders, it checked the names and extensions against hardcoded items that were in plain text, not in hash format. However, CLOP and other ransomware threats with coding flaws are still dangerous.

5.8 What do we learn?

The ransomware phenomenon is more and more dangerous. Not even large businesses or governmental institutions are safe. In their case, ransoms are much higher and the confidential data leaks increase the impact of the attacks. Organizations should have large scale protection systems, in order to avoid malware programs spreading in their networks.

The tendency of the criminals to develop similar attacks, mentioned in the analogous section, is still present and also, because of the RaaS model, the same threats can be customized and used by different authors.

6 Conclusions

Ransomware threats will continue to appear as long as we grow in storing and using data. As at the moment of writing the authors believe that we cannot stop this phenomenon, but we must understand it as understanding facilitates our protection against these threats.

References

1. Aaron Zimba, Mumbi Chishimba, Sipiwe Chihana: A Ransomware Classification Framework Based on File-Deletion and File-Encryption Attack Structures. In: 2nd IEEE-International Conference in Information and Communication Technologies, June 2019, https://www.researchgate.net/publication/333966134_A_Ransomware_Classification_Framework_Based_on_File-Deletion_and_File-Encryption_Attack_Structures. Last accessed 5 Dec 2020
2. Bander Ali Saleh Al-rimy, Mohd Aizaini Maarof, Syed Zainudeen Mohd Shaid: Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. In: Computers & Security Journal, volume 74, pages 144-166, May 2018, https://www.sciencedirect.com/science/article/pii/S016740481830004X. Last accessed 5 Dec 2020
3. Digital Guardian, A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time, https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time. Last accessed 7 Dec 2020
4. Emsisoft, Spotlight on ransomware: Ransomware payment methods, https://blog.emsisoft.com/en/28256/ransomware-payment-methods/. Last accessed 8 Dec 2020
5. Comparitech, 2018-2020 Ransomware statistics and facts, https://www.comparitech.com/antivirus/ransomware-statistics/. Last accessed 10 Dec 2020
6. Pure Cloud Solutions, Ransomware statistics: Cyber threats in numbers, https://www.purecloudsolutions.co.uk/ransomware-statistics-cyber-threats-in-numbers/. Last accessed 10 Dec 2020
7. SDX Central, Case Study: AIDS Trojan Ransomware, https://www.sdxcentral.com/security/definitions/case-study-aids-trojan-ransomware/. Last accessed 5 Dec 2020
8. F Secure, Trojan:W32/Gpcode, https://www.f-secure.com/v-descs/gpcode.shtml. Last accessed 5 Dec 2020
9. Secure List, Blackmailer: the story of Gpcode, https://securelist.com/blackmailer-the-story-of-gpcode/36089/. Last accessed 5 Dec 2020
10. F Secure, Virus:W32/Gpcode.AK, https://www.f-secure.com/v-descs/virus_w32_gpcode_ak.shtml. Last accessed 5 Dec 2020
11. Sophos, Troj/Ransom-A, https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Ransom-A/detailed-analysis.aspx. Last accessed 5 Dec 2020
12. News Softpedia, Troj/Ransom-A Displays Pornographic Images and Asks for A Ransom, https://news.softpedia.com/news/Troj-Ransom-A-Displays-Pornographic-Images-and-Asks-for-a-Ransom-22504.shtml. Last accessed 5 Dec 2020
13. Secureworks, Cryzip Ransomware Trojan Analysis, https://www.secureworks.com/research/cryzip. Last accessed 7 Dec 2020
14. Securelist, Malware evolution: April – June 2006, https://securelist.com/malware-evolution-april-june-2006/36094/. Last accessed 7 Dec 2020
15. BBC News, Extortion virus code gets cracked, http://news.bbc.co.uk/2/hi/technology/5038330.stm. Last accessed 7 Dec 2020
16. Securelist, Malware Evolution: October – December 2005, https://securelist.com/malware-evolution-october-december-2005/36069/. Last accessed 7 Dec 2020

17. Securelist, Krotten source traced – for the moment, https://securelist.com/krotten-source-traced-for-the-moment/30086/. Last accessed 7 Dec 2020
18. The Register, Russian cops cuff 10 ransomware Trojan suspects, https://www.theregister.com/2010/09/01/ransomware_trojan_suspects_cuffed/. Last accessed 7 Dec 2020
19. PCWorld, Alleged Ransomware Gang Investigated by Moscow Police, https://www.pcworld.com/article/204577/article.html. Last accessed 7 Dec 2020
20. Computerworld, Ransomware squeezes users with bogus Windows activation demand, https://www.computerworld.com/article/2507340/ransomware-squeezes-users-with-bogus-windows-activation-demand.html. Last accessed 7 Dec 2020
21. The Next Web, Criminals push ransomware hosted on GitHub and SourceForge pages by spamming 'fake nude pics' of celebrities, https://thenextweb.com/insider/2013/02/07/criminals-push-ransomware-hosted-on-github-and-sourceforge-pages-by-spamming-fake-nude-pics-of-celebrities/. Last accessed 7 Dec 2020
22. The Next Web, New OS X malware holds Macs for ransom, demands $300 fine to the FBI for 'viewing or distributing' porn, https://thenextweb.com/apple/2013/07/16/new-os-x-malware-holds-macs-for-ransom-demands-300-fine-to-the-fbi-for-viewing-or-distributing-porn/. Last accessed 7 Dec 2020
23. TechBeacon, Ransomware on the rise: The evolution of a cyberattack, https://techbeacon.com/security/ransomware-rise-evolution-cyberattack. Last accessed 7 Dec 2020
24. KnowBe4, CryptoLocker Ransomware, https://www.knowbe4.com/cryptolocker-ransomware. Last accessed 7 Dec 2020
25. Avast Academy, What is CryptoLocker Ransomware and How to Remove it, https://www.avast.com/c-cryptolocker. Last accessed 7 Dec 2020
26. KnowBe4, CryptoLocker 2.0 Ransomware, https://www.knowbe4.com/cryptolocker-2. Last accessed 7 Dec 2020
27. SecurityAlliance, Know Your Ransomware: CTB-Locker, https://www.secalliance.com/blog/ransomware-ctb-locker/. Last accessed 7 Dec 2020
28. 360 Total Security, What is TeslaCrypt ransomware and how to remove it?, https://blog.360totalsecurity.com/en/remove-teslacrypt-ransomware/. Last accessed 7 Dec 2020
29. KnowBe4, CryptoDefense Ransomware, https://www.knowbe4.com/cryptodefense-ransomware. Last accessed 7 Dec 2020
30. PCWorld, Malvertising campaign delivers digitally signed CryptoWall ransomware, https://www.pcworld.com/article/2688992/malvertising-campaign-delivers-digitally-signed-cryptowall-ransomware.html. Last accessed 7 Dec 2020
31. TrendMicro, CryptoWall 3.0 Ransomware Partners With FAREIT Spyware, https://blog.trendmicro.com/trendlabs-security-intelligence/cryptowall-3-0-ransomware-partners-with-fareit-spyware/. Last accessed 7 Dec 2020
32. Heimdal Security, Security Alert: CryptoWall 4.0 – new, enhanced and more difficult to detect, https://heimdalsecurity.com/blog/security-alert-cryptowall-4-0-new-enhanced-and-more-difficult-to-detect/. Last accessed 7 Dec 2020

33. BleepingComputer, Locky Ransomware Information, Help Guide, and FAQ, https://www.bleepingcomputer.com/virus-removal/locky-ransomware-information-help. Last accessed 7 Dec 2020
34. Avast Academy, Zepto ransomware now introduces new features to better encrypt your files, https://blog.avast.com/zepto-ransomware-now-introduces-new-features-to-better-encrypt-your-files. Last accessed 7 Dec 2020
35. BleepingComputer, Spora Ransomware Works Offline, Has the Most Sophisticated Payment Site as of Yet, https://www.bleepingcomputer.com/news/security/spora-ransomware-works-offline-has-the-most-sophisticated-payment-site-as-of-yet/. Last accessed 7 Dec 2020
36. Networkworld, Petya ransomware is now double the trouble, https://www.networkworld.com/article/3069990/petya-ransomware-is-now-double-the-trouble.html. Last accessed 7 Dec 2020
37. ZDNet, Petya ransomware attack: What it is, and why this is happening again, https://www.zdnet.com/article/petya-ransomware-attack-what-it-is-and-why-this-is-happening-again/. Last accessed 7 Dec 2020
38. Kaspersky, What are the different types of ransomware?, https://usa.kaspersky.com/resource-center/threats/ransomware-examples. Last accessed 7 Dec 2020
39. Kaspersky, What is WannaCry ransomware?, https://www.kaspersky.com/resource-center/threats/ransomware-wannacry. Last accessed 7 Dec 2020
40. Ars Technica, >10,000 Windows computers may be infected by advanced NSA backdoor, https://arstechnica.com/information-technology/2017/04/10000-windows-computers-may-be-infected-by-advanced-nsa-backdoor/. Last accessed 28 Dec 2020
41. Malware Bytes Labs, BadRabbit: a closer look at the new version of Petya/NotPetya, https://blog.malwarebytes.com/threat-analysis/2017/10/badrabbit-closer-look-new-version-petyanotpetya/. Last accessed 7 Dec 2020
42. ZDNet, Bad Rabbit: Ten things you need to know about the latest ransomware outbreak, https://www.zdnet.com/article/bad-rabbit-ten-things-you-need-to-know-about-the-latest-ransomware-outbreak/. Last accessed 7 Dec 2020
43. Malware Bytes Labs, SamSam ransomware: what you need to know, https://blog.malwarebytes.com/cybercrime/2018/05/samsam-ransomware-need-know/. Last accessed 8 Dec 2020
44. WeLiveSecurity, New Mac ransomware appears: KeRanger, spread via Transmission app, https://www.welivesecurity.com/2016/03/07/new-mac-ransomware-appears-keranger-spread-via-transmission-app/. Last accessed 8 Dec 2020
45. CryptoStopper, Advanced Persistent Threats and Ransomware, https://blog.getcryptostopper.com/advanced-persistent-threats-and-ransomware. Last accessed 28 Dec 2020
46. CryptoStopper, DynA-Crypt - Encrypts AND Steals Your Data, https://blog.getcryptostopper.com/dyna-crypt-encrypts-and-steals-your-data. Last accessed 28 Dec 2020
47. PCrisk, Virus Hermes Ransomware, https://www.pcrisk.com/removal-guides/15123-virus-hermes-ransomware. Last accessed 8 Dec 2020
48. EnigmaSoft, Hermes Ransomware, https://www.enigmasoftware.com/hermesransomware-removal/. Last accessed 8 Dec 2020
49. Microsoft, Syskey.exe utility is no longer supported in Windows 10, Windows Server 2016, and later versions, https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/syskey-exe-utility-is-no-longer-supported. Last accessed 8 Dec 2020

50. CrowdStrike, Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware, https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/. Last accessed 8 Dec 2020
51. CrowdStrike, BitPaymer Source Code Fork: Meet DoppelPaymer Ransomware and Dridex 2.0, https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/. Last accessed 8 Dec 2020
52. Bitdefender, GandCrab: The Most Popular Multi-Million Dollar Ransomware of the Year, https://labs.bitdefender.com/2018/10/gandcrab-the-most-popular-multi-million-dollar-ransomware-of-the-year/. Last accessed 8 Dec 2020
53. BleepingComputer, Thanatos Ransomware Is First to Use Bitcoin Cash. Messes Up Encryption, https://www.bleepingcomputer.com/news/security/thanatos-ransomware-is-first-to-use-bitcoin-cash-messes-up-encryption/. Last accessed 8 Dec 2020
54. KeepNet Labs, Top 11 Ransomware Attacks in 2020-2021, https://www.keepnetlabs.com/top-11-ransomware-attacks-in-2020-2021/. Last accessed 8 Dec 2020
55. McAfee, Clop Ransomware, https://www.mcafee.com/blogs/other-blogs/mcafee-labs/clop-ransomware/. Last accessed 8 Dec 2020
56. SecurityIntelligence, Ransomware 2020: Attack Trends Affecting Organizations Worldwide, https://securityintelligence.com/posts/ransomware-2020-attack-trends-new-techniques-affecting-organizations-worldwide/. Last accessed 8 Dec 2020
57. CSO, REvil ransomware explained: A widespread extortion operation, https://www.csoonline.com/article/3597298/revil-ransomware-explained-a-widespread-extortion-operation.html. Last accessed 8 Dec 2020
58. InfraData, What is REvil ransomware? Sodinokibi aka REvil Ransomware explained, https://www.infradata.com/resources/what-is-revil-ransomware/. Last accessed 8 Dec 2020
59. BlackBerry ThreatVector Blog, Threat Spotlight: Tycoon Ransomware Targets Education and Software Sectors, https://blogs.blackberry.com/en/2020/06/threat-spotlight-tycoon-ransomware-targets-education-and-software-sectors. Last accessed 9 Dec 2020

7 Appendix A

Table 1. Chronological list of ransomware threats

Name	Appearance	Overview
AIDS Trojan	Dec 1989	Weak malware; easy removable; has infected the victim through mailed floppy disks
Gpcode	May 2005	Creates a startup key for its file in Windows Registry; uses simple encryption
Krotten	Sep 2005	Disables the registry editor, control panel and Windows task manager; prevents the user from closing Internet Explorer windows and from accessing file and folder configuration; modifies the Start Menu; was disguised as a code generator to top up mobile phones; target Russia

Cryzip	Mar 2006	Uses a commercial zip library in order to store files inside an encrypted zip; delete the original files; target U.S.A
TROJ.RANSOM.A	May 2006	Deletes files and displays a pornographic picture with a message every time the victim opens the computer
Archiveus	May 2006	Swaps files found in the "My Documents" folder; a single file protected by a 30-digit password; victims are required to buy drugs from one of three online pharmacies
MayArchive	May 2006	A new Cryzip variant; target UK
Gpcode.AG	Jun 2006	660-bit key; target Russia
Gpcode.AK	Jun 2008	Encrypts with RSA and renames the files with a ._CRYPT extension and deletes the original files
WinLock	Aug 2010	Non-encrypting ransomware; pornographic content; main-target Russia
Trojan-Windows Product Activation notice	2011	Non-encrypting ransomware; Call-Scam; imitates the Windows Product Activation notice; the user is redirected to call a fictitious phone number from Microsoft, in order to reactivate his Windows, where are kept on hold, racking up long-distance charges
FBI MoneyPak Ransomware (Reveton)	Mar 2012	Non-encrypting ransomware; charges of pirated software or child pornography; a window is displayed to the user informing him that he has been fined; Ukash, Paysafe, or MoneyPak - payment method
Trojan based on the Stamp.EK exploit kit	Feb 2013	Non-encrypting ransomware; distributed via SourceForge and GitHub, offer "fake nude pics" of celebrities
OS-X Trojan	Jul 2013	Non-encrypting ransomware, a web page that accuses the user of illegally accessing or downloading pornography
CryptoLocker	Sep 2013	First cryptographic malware spread by downloads from a compromised website or via infected email attachments and existing Gameover ZeuS botnet; uses an asymmetric encryption method to encrypted files; Bitcoin, CashU, Ukash, Paysafecard, MoneyPak or pre-paid cash vouchers - payment method

CryptoLocker 2.0	Dec 2013	Uses 1024 bit RSA key pair; encrypt or lock more file types than CryptoLocker and delete the originals; delete the private key or increase the ransom, if the payment is not received in three days; Bitcoin - payment method
CryptoDefense	Feb 2014	Uses Tor and Bitcoin for anonymity and 2048-bit encryption; spread via spear phishing email campaigns like CryptoLocker; CryptoLocker produces its RSA key pair on the command and control server and CryptoDefense uses the Windows CryptoAPI; target US and UK
CryptoWall	Apr 2014	Is an improved version of CryptoDefense; is, like CryptoLocker 2.0, unrelated to the original CryptoLocker; CryptoDefense required the user to open an infected attachment, CryptoWall uses a Java vulnerability
Curve-Tor-Bitcoin Locker	midsummer 2014	Curve - elliptic curve cryptography usage; Tor - was one of the first ransomware to use Tor to hide its C2 infrastructure and subsequently evade detection and blocking; Bitcoin - payment method
SynoLocker	Aug 2014	Targeting NAS devices produced by Synology; encrypts files one by one; users must go to an address on the Tor network to unlock the files; Bitcoin - payment method
CryptoWall 3.0	2014	Uses a payload written in JavaScript as part of an email attachment, which downloads executables disguised as JPG images; installs spyware that steals passwords and Bitcoin wallets
TeslaCrypt	Feb 2015	Originally affected game files, later other file types were also targeted; similar to CryptoLocker although they are not related
CryptoWall 4.0	Nov 2015	Spreads via drive-by attacks and spam mails, enhanced its code to avoid antivirus detection; encrypts not only the data in files but also the file names; changes in the text message; Cryptoware creators act like they run software companies

Locky	Feb 2016	The ransomware process is started by a Word document (with macros enabled) or a Javascript installer; checks if the computer uses Russian, and if so, it does not encrypt it
Petya	Mar 2016	Infect the master boot record; encrypts the file tables of the NTFS file system; blocking the system from booting into Windows
KeRanger	Mar 2016	Targets Apple OS X and spreads through a vulnerable version of Transmission – a BitTorrent client
Zepto	2016	Related to Locky; uses the same methods to spread as Locky; the only difference between Locky and Zepto is the ransom demand, much higher for Zepto
SamSam	2016	Targets JBoss servers; uses a Remote Desktop Protocol brute-force attack to guess weak passwords
Spora	Jan 2017	Running HTML Application (HTA) files starts the ransomware process; ability to work offline; a very well put together ransom payment site; via spam emails
DynA-Crypt	Feb 2017	The first-of-its-kind malware that uses both the APTs and ransomware approaches. It encrypts, steals and/or deletes files from the victims' computers and even spies the users (e.g., by recording system sounds and logging typed commands); leaves files and processes running (the APT component) on the hit systems, allowing the attack to continue at any time
Hermes	Feb 2017	Uses document macros; based on an open-source ransomware project called Hidden Tear; changes the desktop wallpaper, with ”HOW TO DECRYPT FILES.txt”
Syskey	removed from Windows in 2017	Windows feature; tool to encrypt the user account database used as ransomware during technical support scams
WannaCry	May 2017	Uses the EternalBlue hack, based on a vulnerability of some Windows versions; a global epidemic of attacks; Bitcoin - payment method
Modified Petya	Jun 2017	Used for a global cyberattack primarily targeting Ukraine

BitPaymer	Aug 2017	used 256-bit AES and 4096-bit RSA to encrypt the files and keys, respectively; older versions used 128-bit RC4 and 1024-bit RSA to encrypt the files and keys, respectively; uses a TOR-based payment portal
Bad Rabbit	Oct 2017	Similar pattern to WannaCry and Petya; Bitcoin- payment method; Bad Rabbit's code has many overlapping and analogical elements to the code of Petya/NotPetya
GoldenEye	2017	A new version of Petya; hit over 2,000 targets, including prominent oil producers in Russia and several banks; forced workers at the Chernobyl nuclear plant to check radiation levels manually as they had been locked out of their Windows PCs
GandCrab	Jan 2018	Customizes the ransom notes; for the payments, it accepts Bitcoin as well as Dash, a forked Bitcoin protocol with faster transactions that are untraceable
Thanatos	Feb 2018	The keys are not saved anywhere so decryption may be possible only by brute force; the first ransomware to accept Bitcoin Cash
Ryuk	Aug 2018	Derived from Hermes ransomware; targets large companies and government agencies; operated by the group Wizard Spider
CLOP	Feb 2019	Attacks companies and organizations; requires negotiations for ransom; encrypts files and leaks them; it checks language settings in order not to attack users from the Commonwealth of Independent States (CIS) which includes countries such as Russia and Kazakhstan; it has some programming mistakes/weird decisions
DoppelPaymer	Apr 2019	Related to BitPaymer; used 256-bit AES and 2048-bit RSA to encrypt the files and keys, respectively
REvil	2019	Besides functioning like a regular ransomware; it was also used for stealing data from the victims (e.g., Grubman Shire Meiselas & Sacks, Robert de Niro, Rod Stewart, Mariah Carey)

Sodinokibi	Sep 2019	A type of REvil ransomware propagated at first by exploiting a vulnerability in the servers of Oracle Weblogic, afterwards it began to propagate in any possible way, due to the Ransomware-as-a-Service (RaaS) model; may be related to GandCrab; linked to organized crime group ITG14 (for delivery)
Maze	May 2019	Attacks organizations; encrypts files and leaks them; uses the exploit tools called Fallout and Spelvo
Nemty	summer 2019	Ransomware service; in the beginning it was advertised on Russian pirated forum websites
EKANS	Dec 2019	Is able to kill several critical processes on a victim device, including some processes directly related to industrial control system (ICS) operations
Tycoon	at least Dec 2019	Attacks organisations in the education and software industry; written in Java; triggered by executing a shell script (there are both Windows and Linux versions) that runs the Main function of the malicious Java module using the java -m command
Nephilim	2019	Similar to Nemty; usually targets big organizations and companies
NetWalker (Mailto)	2019/2020	The targets are governmental agencies, healthcare organisations, corporations, remote employees; it propagates by coronavirus phishing emails and executable files spreading through networks
Sekhmet	Jun 2020	Attacks companies; encrypts files and leaks them; uses a combination of RSA-2048 and ChaCha encryption algorithms