Ransomware Appeared in 2020

Dr. Abdalla Eldow
Information Technology Department
Alsalama College of Science and Technology – Sudan
Mobile: 0096891260780 Email: abdalllaeldaw2021@gmail.com

Abstract
Ransomware is a collection of malicious software used by cyber security criminals to extort victims to pay a specified ransom at a specific time. In addition, ransomware attacks represent a modern challenge for all countries, companies, and organizations.A part of the results in this paper includes the timeline for the most ransomware that appeared in 2020, such that the paper listed eight ransomware this year, started by (Ragnar Locker) which appeared in January 2020, and ended by (Egregor) which appeared in September from the same year. In addition, the study found that: most ransomware uses a combination of three algorithms, like Nefilim and RansomExx, which use (RSA-2048, RSA-4096, and AES-256) algorithms, while most of the ransomware jointly uses the RSA & AES algorithms. In addition, the paper pointed out that: Egregor and Conti have the largest amount of ransoms, which is ($35 and $25) million respectively, instead (ProLock) which has the lowest ransom which is ($40000). Also, the amount ransoms of Nefilim and RansomExx is not determined. While Avaddon, Conti, and Nefilim are the most dangerous ransomware in 2020, because of their wide separation and attacks in many countries and companies.
Keywords: Cyberattack, Ransomware, Ransom, Encryption, AES, RSA, RC4
DOI: 10.7176/CEIS/14-3-02
Publication date: August 31st 2023

1. Introduction

In the year 2020, the pandemic in the world was twofold, the first hand the Covid-19 pandemic, and the second hand the pandemic of ransomware. Therefore, it may not be a coincidence that the health field will be the most targeted in the year 2020.

This study will offer some information about the ransomware that appeared in 2020, giving special significance to the types that represent a big threat like Nefilim and Conti. The paper also will offer information about the historical development of these ransomware, and the date of appearance of each one.

The study also shed light on the types of algorithms used by each type. In addition to the amount of ransom required for each ransomware.

2. Background

The following two sections will include the definition of ransomware, and the results of ransomware attack.

2.1. Ransomware

Ransomware is a collection of malicious software used by cyber security criminals to extort victims to pay a specified ransom at a specific time [1]. While (C. Simoiu, et al, 2019) referred that: Ransomware is a type of malware that encrypts victim data and demands payment of a ransom for decryption [2].

2.2. Results of Ransomware Attack

Many actions may happened when your company attacked by ransomware, these include:

Many actions may happen when your company attacked by ransomware, these include:

a- Lost of sensitive information.
b- Leak of your information.
c- Sell your information to other companies
d- Publication of the employee's records into cyberspace.
e-Publication of patient records in the case of medical institutions extortion
f- Paralysis of the company or institution and its complete inactivity
g- Damaging the reputation of the institution

In addition, (A. Imaji, 2019) ensured that "It can result in loss of sensitive information, regular operations' disruption and harm to an organization's reputation" [3].

3. The Ransomware Trends in 2020

In 2020, the ransomware continued with the same trends that appeared in 2019, like:
a- Increasing cyber-attacks compared with the previous years.

b- Incremental in the operations of the encryption, which take different forms.
c- Increasing of Ransoms amount.
d- Increasing of attacks incidents in the healthcare sector for some reasons: First: The ransoms fetched from this sector, second the sensitive information of the patient records, thirdly the information related to the Covid-19 pandemic medicines.
e- Using of new algorithms by cyber criminals.

4. Types of Ransomware in 2020

There are many types of ransomware, and this study found that the history of Ransomware started in 1989 and increased day after day. Ransomware uses different encryption algorithms with differences in extortion and ransom payments. The following sections will display the main types of ransomware that appeared in the year 2020.

4.1. Ragnar Locker Ransomware

4.1.1. Ragnar Locker Ransomware Description

Ragnar Locker appeared in January 2020 to attack large organizations and demand large amounts of ransom from it is victims [4]. While (PentaSecurity, 2020) referred that this ransomware was founded in Oracle VM VirtualBox, which uses the Windows XP operating system. Also ensured that it targeted the cloud storage for the victim's companies [5]. In addition, Ragnar Locker obtains language information of the infected PC by using GetLocaleInfo, and if the result matches one of the pre-defined languages, then it finally terminates its process [6].

4.1.2. The attacked Countries, Organizations, or Companies by Ragnar Locker

4.1.2. The attacked Countries, Organizations, or Companies by Ragnar Locker
(C., Brook, 2020) in his article on (the digital guardian website) referred that Ragnar Locker attacked many countries and companies, including France, Estonia, Sri Lanka, Turkey, Thailand, the U.S., Malaysia, and Hong Kong. [7]

4.1.3. Ragnar Locker Encryption Algorithms

Ragnar Locker ransomware uses the Salsa20 encryption algorithm (which is too strong to decrypt using brute-force methods) for file encryption and RSA-2048 to encrypt file keys. It generates two key data arrays of 40 bytes and 32 bytes for use by the Salsa20 cipher, and these keys are encrypted by the master RSA-2048 public key and added to the footer of a file [8].

4.1.4. Ragnar Locker Ransom Demand

The amount of ransom demanded from Ragnar's locker is $15 million [9]. In addition, (Covrr, 2021) referred that the travel company CWT paid $4.5 as a ransom to Ragnar's locker, in addition to another ransom ($4.4) (in the same year) requested by the gang after she attacks the Colonial Pipeline company[10]. While (Documentcloud, 2020) website referred that Ragnar Locker attacked many companies, and threaten to publish 10TB of data if the demanded ransom ($11 million) was not paid [11].

From the above paragraphs, we found that: there are many ransoms of different amounts from several companies requested by Ragnar Locker.

4.2. Nefilim Ransomware

4.2.1. Nefilim Description

(J. Agcaoili and B. Gelera, 2021), referred that Nefilim appeared in March 2020. It is a development of Nemty ransomware, and like other types, Nefilim threatens to publish the encrypted and stolen data, if the ransom is not paid. Nefilim uses the vulnerability (CVE-2019-19781), unsecured (RDP), and other programs like (Mimikatz, LaZagne, and NirSoft's NetPass), which also provides loopholes to enter the victims' computers. [12]

4.2.2. The attacked Countries, Organizations, or Companies by Nefilim

According to a report published by (Kaspersky, 2020) referred that Nefilim targeted the Toll Group Company (Australia), so the attackers encrypted the company files and they were stealing about 20 GB of data. However, on May 29, Toll Group restored all of its information systems and logistics operations [13]. In addition, Nefilim operators attacked France Orange Telecom in July 2020, and then the attackers threatened to publish the customers' records if the required ransom was not paid [14]. In addition, Nefilim ransomware attacked the SPIE group in Europe, which is a multi-technical services company and includes about (47200) employees [15].

4.2.3. Nefilim Encryption Algorithms

Nefilim uses AES-128 encryption to lock files and appends (.NEFILIM) with encrypted files and then appends AES encrypted key with each file. An RSA-2048 public key will then encrypt this AES encryption key. [16]

4.2.4. Nefilim Ransom Demand

In her article posted on (the ZDnet website), (C. Osborne, 2021) referred that Nefilim always targeted organizations with annual revenue of One billion dollars or more. [17]

4.3. ProLock Ransomware

4.3.1. ProLock Description

ProLock activities appeared in March 2020 and is a development of the ransomware called PwndLocker that appeared in 2019. ProLock embeds a code called ShellCode in AVI video files, as well as ProLock representatives steal the victim's files and encrypt them before the required ransom [18]. While (Enigma software, 2021) refereed that ProLock exploiters exploit the Windows variability CVE-2019-0859[19].

4.3.2. The attacked Countries, Organizations, or Companies by ProLock

ProLock attacked Diebold Nixdorf, which is a big company in ATM manufacturing, the city of Novi Sad in Serbia, and Lasalle County in Illinois, in addition to other companies and countries [20].

4.3.3. ProLock Encryption Algorithms

ProLock uses the RSA-2048 algorithm to encrypt victims' files and generates a ransom note. Then it will append the "ProLock" extension to all the encrypted filenames [21].

4.3.4. ProLock Ransom Demand

(C. Cimpanu, 2020) referred that based on (ZDnet) ProLock attackers demanded $2.3 million as a ransom to decrypt the encrypted files. Moreover, this amount of ransom ensured by other sources [22].

4.4. RansomExx Ransomware

4.4.1. RansomExx Ransomware Description

It appeared in June 2020, through several cyber-attacks, most notably on the Department of Transportation in the US state of Texas, and one of the most prominent features of this ransomware program is the leaking of information stolen from victims or selling it on the black internet [23].

4.4.2. The attacked Countries, Organizations, or Companies by RansomExx

RansomExx attacked the Japanese Technology company (Konica Minolta) which include about 40000 employees. In addition, the attack of Embraer, which is one of the world's largest airplane manufacturers company and Taiwanese computer hardware manufacturer Gigabyte, company [24].

4.4.3. RansomExx Encryption Algorithms

RansomExx encrypts the victim's server with a file called (svc-new). AES algorithm used to generate a 256-bit key and how long is this key encrypted by the RSA-4096 algorithm [25].

4.4.4. RansomExx Ransom Demand

There is no available information about the amount of ransom demanded by this ransomware.

4.5. Avaddon Ransomware

4.5.1. Avaddon Description

(Javier, Y., and Sergio, P., 2021) referred that Avaddon appeared on June 2020 in a Russian underground forum, only accessible by invitation or after the payment of a registration fee. It has allegedly infected and leaked full dump data from 20 companies (totaling 574.46 GB of data), and other 23 organizations in addition to the Denial of Service. [26]

4.5.2. The attacked Countries, Organizations, or Companies by Avaddon

Avaddon ransomware targets many public and private international organizations and many countries including Germany (Glasbau Wiedmann Gbh), Australia (Schepisi Communications), Brazil (CJ Selecta), Canada (Cathar Games), US (Capital Medical Center), Italia (Mipharm), Japan (Exedy Corporation), Czech Republic (Municipality of Olomouc) and UK (Logixal) [27]. In addition, the (Australian Cyber Security Centre (ACSC)), referred that Avaddon Targeted many countries and sectors, including Australia, Brazil, China, Czech Republic, Germany, Indonesia, Jordon, Poland, Spain, the UK, USA, UAE, Canada, France, Italy, and other countries. In addition to many sectors like Health, Government, Academia, Construction, Equipment, Freight and transport, Information Technology, Law Enforcement, and other sectors [28].

4.5.3. Avaddon Encryption Algorithms Used

Avaddon uses a combination of two algorithms, AES-256 and RSA-2048, and each file has a footer appended that contains the session key used to encrypt the file. The key can be extracted with the private RSA key [29]. While (Acronis, 2020) referred to that, the encryption is done after complicated encryption operations, which will start by Generating two master keys: RSA-2048 and AES – CBC 256 keys, then generating the AES-CBC-256 key that is added to the AES master keys. Then encrypts the victims' files with the AES key encrypted with the RSA-2048 key to the end of every encrypted file [30].

4.5.4. Avaddon Ransom Demand

(E. Georgescu, 2022) referred that Avaddon attackers demand ransom payment via Bitcoin, with an average demand of about $40,000 in exchange for a decryption tool [31].

4.6. Conti Ransomware

4.6.1. Conti Description

Conti ransomware started it is activities in July 2020, and it makes double extortion for the victims, in addition to the changing Windows version before the encryption operations for the network files. [32]. In addition, (PRODAFT, 2021) referred that Conti ransomware is a malicious program that infects networks and thus makes the network unavailable, and can spread in the victim's network and encrypt their data. [33]

4.6.2. The attacked Countries, Organizations, or Companies by Conti

Conti ransomware attacks different organizations and sectors, which include Energy (Colonial Pipeline), Transportation (NYC Subway system), Chemical (Brenntag), Information Technology (Acer), Food & Agriculture (BS), Healthcare, and Public Health (Health Service Executive), Emergency Services (Washington DC Metropolitan Police Department Financial Services [34]. While (Healthcare.com, 2021) ensured that Conti attacked the Irish Systems and about 16 American medical centers, in addition to about 400 organizations in different locations in the world, two-thirds of these organizations are from the USA [35].

4.6.3. Conti Encryption Algorithms Used

Conti ransomware uses the AES-256 algorithm to encrypt the victims' files and gives an independent key for each file, and then it uses the RSA-4096 algorithm to encrypt the pre-encrypted file with the AES algorithm. It also uses two types of ports, SMB-445 and SMB-139, and the purpose of these ports is to propagate in the network and access the computers associated with it[36].

4.6.4. Conti Ransom Demand

The ransom demanded by Conti ransomware is about $25 Million [37].

4.7. DarkSide Ransomware

4.7.1. DarkSide Description

Appeared in August 2020, as RaaS (Ransomware-as-a-Service). They have gained a reputation for their professional operations and huge ransoms since then. Before attacking, they give victims web chat support; develop complex data leak storage systems with redundancy [38]. In addition, this ransomware uses the vulnerabilities CVE-2019-5544 and CVE-2020-3992. Both vulnerabilities have widely available patches, but attackers are targeting organizations using unpatched or older versions of the software [39].

4.7.2. The attacked Countries, Organizations, or Companies by DarkSide

According to (Trend Micro Research, 2021) DarkSide targeted one of the biggest companies in the USA, which is the Colonial Pipeline company, and the stores of gasoline, diesel, home heating oil, and jet fuel, so the government declared a state of emergency in 18 states to help with the shortages [40].

Also (Speechreading, 2021) referred that this ransomware targeted Canadian discount cars and Truck Rentals and stole about 120GB of data [41]. While (C. Osborne, 2021) referred that Toshiba Tec Corp was targeted by DarkSide ransomware [42].

4.7.3. DarkSide Encryption Algorithms Used

DarkSide ransomware uses the Salsa20 encryption algorithm with an RSA-1024 public key [43].

4.7.4. DarkSide Ransom Demand

The Colonial Pipeline Company paid- the DarkSide- $4.4 million for a key to unlock its files [44]. While (NETdepot, 2020) referred that the DarkSide ransomware demands a ransom between $200,000 and $1,000,000 [45]. Instead, (Acronis, 2020) ensured that the ransom demanded falls in the range of between $200,000 and $2,000,000 (US) [46].

From the above paragraphs, it is clear that there is a difference in the required ransom, but more than one source confirmed that the required ransom is between $200,000 and $100,000. Because of the importance of this company (Colonial Pipeline) in American life and economics, the government has announced a sum of $10000000 for anyone who provides information about DarkSide ransomware.

According to the (U.S. Department of State, 2021), it will be offering a reward of up to $10,000,000 for information leading to the identification or location of any individual (s) who hold a key leadership position in the DarkSide ransomware. This reward is certainly a result of the importance of (the Colonial Pipeline) in American economic life [47]. However, the strange thing is that the DarkSide attackers' donated $20000 to the victims [48]. In this donation, the attackers claimed that they were Robin Hood collecting money from the rich to distribute to the poor's, but we noticed that the amount of donated money is very small compared to the money obtained from extortion.

4.8. Egregor Ransomware

4.8.1. Egregor Ransomware Description

It appeared in September 2020, and many researchers believe that the members of Maze ransomware are affiliated with Egregor after it has been closed. In addition, some security researchers agree that it was rapidly developed [49]. While (Edward, K., 2022) pointed out: the term Egregor is a term in Western magic, and it means (the collective energy of a group of people united around a common goal) [50]. In addition, (Morphisec, 2021), referred that Egregor is considered to be one of the most prolific ransomware threat groups. Yet it gained this reputation in a very short time due to its uncompromising double extortion methodology [51].

4.8.2. The attacked Countries, Organizations, or Companies by Egregor

Egregor attacked over than150 companies in Europe and US [52]. While (bleeping computer, 2021) referred that Egregore ransomware targeted Crytek company after the confirmation of the attack from the company itself [53].

4.8.3. Egregor Encryption Algorithms Used

(Comparitech, 2021) ensured that this ransomware uses ChaCha20 and RSA encryption, which is the same combination used by Maze and Sekhmet ransomware [54]. In addition, (cert, 2021) ensured that Egregor, Maze, and Sekhmet use the same encryption algorithms (ChaCha20 and RSA-2048) in addition they use similar ransom notes [55].

4.8.4. Egregor Ransom Demand

(Security Intelligence, 2021) conducted a chat with Egregor attackers, and after the recorded negotiations, it ensured the ransom demanded ranged between $10000 and $35 million [56].

5. Ransomware Information

5.1. Ransomware General Information

The following table includes information about the ransomware appearance, the action for each one, ransoms and algorithms used:

Table (1) Ransomware Time Line in 2020

I	Month	Name	Ransomware Action	Ransom	Algorithm (s)
1	January	Ragnar Locker	It attacks a large number of organizations and demands a large amount of ransom from the victims.	$15 Million	RSA(2048)+ Salsa20
2	March	Nefilim	Nefilim threatens to publish the encrypted and stolen data if the ransom is not paid	Not determined	RSA (2048)+ AES (128bit)
3	March	ProLock	ProLock embeds a code called ShellCode in AVI video files, as well as ProLock representatives steal the victim's files and encrypt them before the required ransom	$2.3 Million	RSA (2048)
4	June	RansomExx	The most prominent features of this ransomware program is the leaking of information stolen from victims or selling it on the black internet	Not determined	RSA (2096)+AES (256 bit)
5	June	Avaddon	Steal and leak information	$40000	RSA (2048)+AES (256 bit)
6	July	Conti	Infects networks and makes them unavailable, in addition to the encryption of victims' data	$25 Million	RSA (1024)+AES (256 bit)
7	August	DarkSide	Steal and leak of information	$4.4 Million	RSA(1024)+ Salsa20
8	September	Egregor	Considered one of the most prolific ransomware threat groups.	$35 Million	RSA + ChCha20

5.2. Ransomware: countries, companies, and organizations infection

The following table includes information about the ransomware infection of countries, companies, and organizations:

Table (2) Countries and Companies attached by 2020 ransomware

I	Name	Country/ Company/ Organization
1	Ragnar Locker	France, Estonia, Sri Lanka, Turkey, Thailand, the U.S., Malaysia, and Hong Kong
2	Nefilim	Australia: Toll G. Company France: Orange Company Europe: SPIER
3	ProLock	Diebold Nixdorf, which is a big company in ATM manufacturing, the city of Novi Sad in Serbia, and Lasalle County in Illinois
4	RansomExx	Japanese Technology company (Konica Minolta) which includes about 40000 employees. In addition, to the attack of Embraer which is one of the world's largest airplane manufacturers company and Taiwanese computer hardware manufacturer Gigabyte company
5	Avaddon	Australia, Brazil, China, Germany, Indonesia, Jordan, Spain, Belgium, France, India, Peru, Italy, Portugal, UAE, and USA Energy, Health, marketing, Governmental, and IT
6	Conti	Energy (Colonial Pipeline), Transportation (NYC Subway system), Chemical (Brenntag), Information Technology (Acer), Food & Agriculture (BS), Healthcare and Public Health (Health Service Executive), Emergency Services (Washington DC Metropolitan Police Department o Financial Services, Irish Healthcare Systems, 16 US organizations, more than 1000 organizations around the world and Costa Rica
7	DarkSide	USA: Colonial Pipeline company Canada: Canadian discount car Japan: Toshiba
8	Egregor	Over than150 companies in Europe and US

6. Results

6.1. Ransomware Timeline 2020

From Table (1) we noticed that Ragnar Locker Ransomware is the first ransomware that appeared in 2020, which appeared in January, and Egregor is the last ransomware that appeared in 2020, which appeared in September 2020. Figure (1) shows the ransomware timeline in 2020:

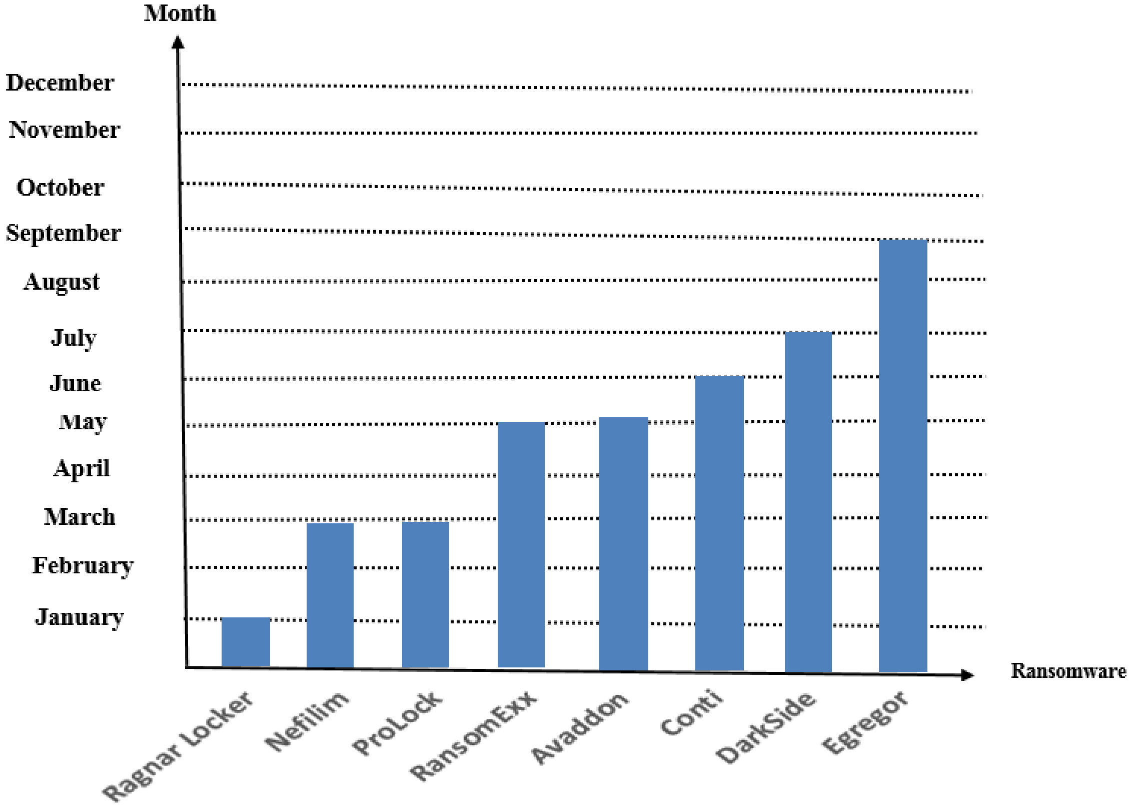

Figure (1) Ransomware Time Line in 2020

6.2. Ransomware Attacks in 2020

From Table (2) we can that: Conti was the most ransomware in the attacking in year 2020, in addition, to RansomExx and Avaddon.

6.3. Ransomware Algorithms Used in 2020

According to figure (2), we found that: firstly, some of the ransomware uses a combination of two or three algorithms, like Nefilim and RansomExx. Secondly, most the ransomware has common uses in AES and RSA algorithms. Thirdly, Ragnar Locker, DarkSide and Egregore ransomware used a combination of RSA and Chacha20 or Salsa20 algorithms.

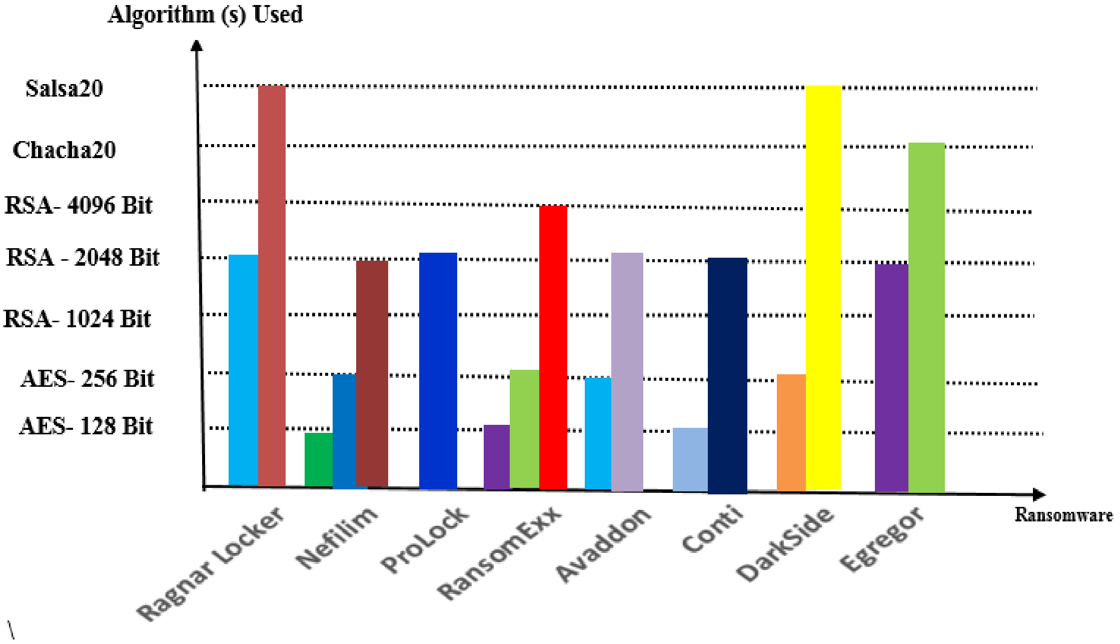

Figure (2) Algorithms used in Ransomware 2020.

6.4. Ransomware Ransoms Demanded in 2020

According to figure (3), we found that Egregore is the highest amount of ransom, which is $35 million, and in second order is Conti $25 Million. The amount of ransoms is not determined by two ransomware, which is Nefilim and RansomExx, while ProLock is the least amount of ransoms, which is only $40000.

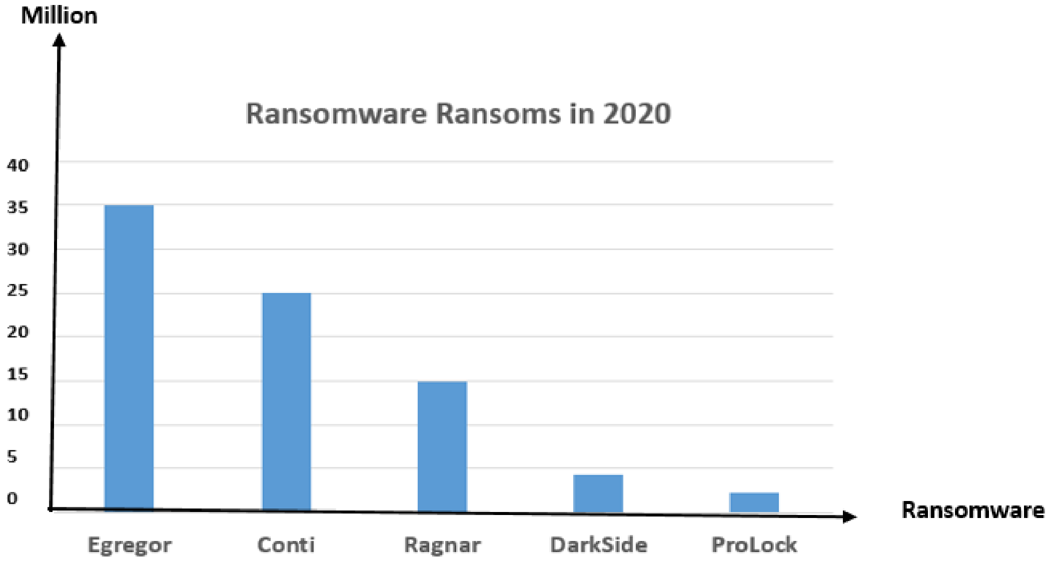

Figure (3) Ransomware Ransoms in 2020.

References

[1] A. Liska and T. Gallo, "Ransomware, Defending Against Digital Extortion", 2017, Published by O'Reilly Media, Inc., USA, [Online]. Available: https://www.academia.edu/33901157/Ransomware

[2] C. Simoiu, et al, ""I was told to buy a software or lose my computer. I ignored it": A study of ransomware", August 11–13, 2019, Santa Clara, CA, USA, [Online]. Available: https://5harad.com/papers/ransomware.pdf

[3] A. Imaji, "Ransomware Attacks: Critical Analysis, Threats, and Prevention methods Thesis", March 2019, [Online]. Available: https://www.researchgate.net/publication/332551447_Ransomware_Attacks_Critical_Analysis_Threats_and_Prevention_methods

[4] G. Cluley, "Ragnar Locker ransomware - what you need to know", March 10, 2022, [Online]. Available: https://www.tripwire.com/state-of-security/ragnar-locker-ransomware-what-you-need-to-know

[5] (PentaSecurity)," Ragnar Locker Ransomware Attacks From Virtual Machines", March 10, 2022, [Online]. Available:https://www.pentasecurity.com/blog/security-weekly-ragnar-locker-ransomware/

[6] T. Yoshikawa, and K. Sugawara, "Analyzing "Ragnar Locker" ransomware that threats a company by its name ", November 2020, [Online]. Available: https://www.mbsd.jp/Whitepaper/Analyzing_Ragnar_Locker_ransomware.pdf

[7] C. Brook, "Ragnar Locker Ransomware Connected to Hacks at 52 Organizations", March 10, 2020, [Online]. Available: https://digitalguardian.com/ja/blog/ragnarlocker-ransomware-connected-hacks-52-organizations

[8] Acronis cyber protect cloud, "Analysis of Ragnar Locker Ransomware ", June 4, 2021, [Online]. Available: https://www.acronis.com/en-us/blog/posts/ragnar-locker/

[9] G. Cluley, " ", November 9, 2020, [Online]. Available: https://www.bitdefender.com/blog/hotforsecurity/campari-staggers-to-its-feet-following-15-million-ragnar-locker-ransomware-attack/

[10] "Leveraging CRQ to understand growing ransomware attack costs", Covrr, December 13, 2021, [Online]. Available: https://www.kovrr.com/blog-post/leveraging-crq-to-understand-growing-ransomware-attack-costs

[11] "Indicators of Compromise Associated with Ragnar Locker Ransomware", FBI FLASH, November 19, 2020, [Online]. Available: https://www.documentcloud.org/documents/20413525-fbi-flash-indicators-of-compromise-ragnar-locker-ransomware-11192020-bc

[12] J. Agcaoili and B. Gelera, "An Analysis of the Nefilim Ransomware", February 23, 2021, [Online]. Available: https://www.trendmicro.com/en_us/research/21/b/nefilim-ransomware.html

[13] Kaspersky ICS SERT, "Threats Landscape for Industrial Automation Systems", September 24, 2020, [Online]. Available: https://icscert.kaspersky.com/media/KASPERSKY_H1_2020_ICS_REPORT_EN.pdf

[14] D. Riley, "Data stolen in ransomware attack on French telco Orange", July 19, 2020, [Online]. Available: https://siliconangle.com/2020/07/19/data-stolen-ransomware-attack-french-telco-orange/

[15] CYBLE research and intelligence labs, "Nefilim Ransomware Operators Allegedly Targeted the SPIE Group, an independent European leader in multi-technical services", August 10, 2020, [Online]. Available: https://blog.cyble.com/2020/08/10/nefilim-ransomware-operators-allegedly-targeted-the-spie-group-an-independent-european-leader-in-multi-technical-services/

[16] E. Georgescu, " Nefilim Ransomware: Everything You Need to Know", June 11, 2021, [Online]. Available: https://heimdalsecurity.com/blog/nefilim-ransomware/

[17] C. Osborne, "A deep dive into Nefilim, a ransomware group with an eye for $1bn+ revenue companies", June 8, 2021, [Online]. Available: https://www.zdnet.com/article/a-deep-dive-into-nefilim-a-double-extortion-ransomware-group/

[18] SEQURETEX, "ProLock Ransomware", 2020, [Online]. Available: https://sequretek.com/wp-content/uploads/2018/10/Sequretek-Advisory-ProLock-Ransomware.pdf

[19] Enigmasoftware, "ProLock Ransomware", 2021, [Online]. Available: https://www.enigmasoftware.com/prolockransomware-removal/

[20] C. Cimpanu, "ProLock ransomware - everything you need to know", September 10, 2020, [Online]. Available: https://www.zdnet.com/article/prolock-ransomware-everything-you-need-to-know/

[21] P. Bhardwaj, "What is ProLock Ransomware?", August 29, 2022, [Online]. Available: https://www.tutorialspoint.com/what-is-prolock-ransomware

[22] C. Cimpanu, "ProLock ransomware - everything you need to know ", September 10, 2020, [Online]. Available: https://www.zdnet.com/article/prolock-ransomware-everything-you-need-to-know/

[23] S. Conrad, " Ransomware Profile: RansomExx", March 23, 2022, [Online]. Available: https://www.emsisoft.com/en/blog/41027/ransomware-profile-ransomexx/

[24] S. Conrad, "Ransomware Profile: RansomExx", March 23, 2022, [Online]. Available: https://www.emsisoft.com/en/blog/41027/ransomwar

[25] F. Sinitsyn and V. Kuskov, "RansomExx Trojan attacks Linux systems", November 6, 2020, [Online]. Available: https://securelist.com/ransomexx-trojan-attacks-linux-systems/99279/

[26] J. Yuste and S. Pastrana, " Avaddon ransomware: an in-depth analysis and decryption of infected systems", February 9, 2021, [Online]. Available: https://arxiv.org/abs/2102.04796

[27] L. Castel, "Avaddon Ransomware Analysis", June 11, 2012, [Online]. Available: https://atos.net/en/lp/securitydive/avaddon-ransomware-analysis

[28] "2020-003: Ongoing campaign using Avaddon Ransomware", The Australian Cyber security Centre (ACSC), May 2021, [Online]. Available: https://www.cyber.gov.au/sites/default/files/2021-05/2021-003%20Ongoing%20campaign%20using%20Avaddon%20Ransomware%20-%2020210511.pdf

[29] A. Sanchez, et al, "One Source to Rule Them All: Chasing AVADDON Ransomware", Jan 19, 2022, [Online]. Available: https://www.mandiant.com/resources/blog/chasing-avaddon-ransomware

[30] "Avaddon ransomware cleans the bin for you", Acronis, October 7, 2020, [Online]. Available: https://www.acronis.com/en-us/blog/posts/avaddon-ransomware/

[31] E. Georgescu, "Avaddon Ransomware: Everything you need to know"¸ June 15, 2022, [Online]. Available: https://heimdalsecurity.com/blog/avaddon-ransomware/

[32] HHS, (2021), "Conti Ransomware and the Health Sector", August 07, 2021, [Online]. Available: https://www.hhs.gov/sites/default/files/conti-ransomware-health-sector.pdf

[33] PRODFAT, "Conti Ransomware Group In-Depth Analysis", November 18, 2021, [Online]. Available: https://www.prodaft.com/m/reports/Conti_TLPWHITE_v1.6_WVcSEtc.pdf

[34] HHS, (2021), "Conti Ransomware and the Health Sector", August 07, 2021, [Online]. Available: https://www.hhs.gov/sites/default/files/conti-ransomware-health-sector.pdf

[35] Healthcare.com, "FBI warns Conti ransomware", May 24, 2021, [Online]. Available: https://www.fiercehealthcare.com/tech/fbi-warns-conti-ransomware-hit-ireland-system-targeted-16-u-s-medical-emergency-networks

[36] HHS, (2021), "Conti Ransomware and the Health Sector", August 07, 2021, [Online]. Available: https://www.hhs.gov/sites/default/files/conti-ransomware-health-sector.pdf

[37] Healthcare.com, "FBI warns Conti ransomware", May 24, 2021, [Online]. Available: https://www.fiercehealthcare.com/tech/fbi-warns-conti-ransomware-hit-ireland-system-targeted-16-u-s-medical-emergency-networks

[38] "Cyber Threat Intelligence Alert DarkSide Ransomware", India Future Foundation, November 2021, [Online]. Available: https://www.indiafuturefoundation.com/wp-content/uploads/2021/11/Darkside-Ransomware.pdf

[39] "The DarkSide Ransomware", Tesaly, November 15, 2020, [Online]. Available: https://www.telsy.com/the-darkside-ransomware

[40] "What We Know About the DarkSide Ransomware and the US Pipeline Attack", TrendMicro, May 12, 2021, [Online]. Available: https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html

[41] "DarkSide Ransomware gang hits Canadian rental car company", Secureading, February 14, 2021, [Online]. Available: https://securereading.com/darkside-ransomware-gang-hits-canadian-rental-car-company

[42] C. Osborne, "DarkSide explained: The ransomware group responsible for Colonial Pipeline attack", May 14, 2021, [Online]. Available: https://www.zdnet.com/article/darkside-the-ransomware-group-responsible-for-colonial-pipeline-cyberattack-explained

[43] R. Emanuel, "DarkSide Ransomware Behavior and Techniques", May 18, 2021, [Online]. Available: https://blogs.keysight.com/blogs/tech/nwvs.entry.html/2021/05/18/darkside_ransomware-QfsV.html

[44] R. Dudley and D. Golden, " The Colonial pipeline ransomware hackers had a secret weapon: self-promoting cybersecurity firms", May 24, 2021, [Online]. Available: https://www.technologyreview.com/2021/05/24/1025195/colonial-pipeline-ransomware-bitdefender

[45] " A Closer Look at the DarkSide Ransomware Attack", NETdepot, 2020, [Online]. Available: https://www.netdepot.com/blog/a-closer-look-at-the-darkside-ransomware-attack

[46] "Threat Analysis: DarkSide Ransomware", Acronis, September 29, 2020, [Online]. Available: https://www.acronis.com/en-us/cyber-protection-center/posts/darkside-ransomware

[47] N. Price, "Reward Offers for Information to Bring DarkSide Ransomware Variant Co-Conspirators to Justice", US Department of State, November 4, 2021, [Online]. Available: https://www.state.gov/reward-offers-for-information-to-bring-darkside-ransomware-variant-co-conspirators-to-justice

[48] " How dark is DarkSide Ransomware Group", Intell Fence, May 17, 2021, [Online]. Available: https://www.intellfence.com/how-dark-is-the-darkside-ransomware-group

[49] C. Brumfield, "Egregor ransomware group explained: And how to defend against it", May 17, 2021, [Online]. Available: https://www.csoonline.com/article/3602148/egregor-ransomware-group-explained-and-how-to-defend-against-it.html

[50] E. Kost, "What is Egregor Ransomware? One of the Worst Threats of 2020", June 05, 2022, [Online]. Available: https://www.upguard.com/blog/what-is-egregor-ransomware

[51] " An Analysis of Egregor Ransomware", Morphisec, 2021, [Online]. Available: https://www.morphisec.com/hubfs/eBooks_and_Whitepapers/EGREGOR%20REPORT%20WEB%20FINAL.pdf

[52] L. Constantin, "Egregor ransomware takes a hit after arrests in Ukraine", February 17, 2021, [Online]. Available: https://www.csoonline.com/article/570383/egregor-ransomware-takes-a-hit-after-arrests-in-ukraine.html

[53] S. Gatlan, "Crytek confirms Egregor ransomware attack, customer data theft"¸ August 10, 2021, [Online]. Available: https://www.bleepingcomputer.com/news/security/crytek-confirms-egregor-ransomware-attack-customer-data-theft

[54] S. Cooper, "What is Egregor Ransomware & How to Protect Against It?"¸ November 15, 2022, [Online]. Available: https://www.comparitech.com/net-admin/egregor-ransomware

[55] " Egregor Ransomware"¸ CERT, February 3, 2021, [Online]. Available: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-007.pdf

[56] C. Caridi, "This Chat is Being Recorded: Egregor Ransomware Negotiations Uncovered", July 21, 2021, [Online]. Available: https://securityintelligence.com/posts/egregor-ransomware-negotiations-uncovered