

Ransomware Appeared in 2019

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

Abstract
Ransomware has become a form of electronic warfare and cybercrime, which is increasing day by day due to the large revenue of money it has generated, which estimated at millions of dollars. The act of paying or refusing it also poses another challenge to the countries and organizations, as their laws and regulations say not to pay the extortionists, but in return, to the needs of these organizations for their data, it will respond to the blackmailers and pay the ransom, which encouraged the extortionists to produce much dangerous ransomware.A part of the results in this paper includes the timeline for the most ransomware that appeared in 2019, such that the paper listed nine ransomware this year, started by (Mega Cortex) which appeared in January 2019, and ended by (Double Extortion) which appeared in November from the same year. In addition, the study found that: most of the ransomware uses a combination of three algorithms, like REvil and NetWalker, which use (RSA-2048, ECDH, and Chacha20) algorithms, while most of the ransomware jointly uses the RSA & AES algorithms. In addition, the paper pointed out that: REvil and LockBit2.0 have the largest amounts of ransoms, which is ($50) million for each one, instead (DoppelPaymer) has the lowest ransom which is ($1.2) million. While CLOP, REvil, and LockBit2.0 are the most dangerous ransomware in 2019, because of their wide separation and attacks in many countries in Europe, Asia, and USA.
Keywords: Cyberattack, Ransomware, Ransom, Encryption, AES, RSA, RC4
DOI: 10.7176/CEIS/10-1-02
Publication date: September 30th 2023

1. Introduction
There is no doubt that ransomware programs have become a major and dangerous threat to institutions, organizations, and all countries. Rather, it became a ghost that threatens these organizations and encrypt, leak, or steal their data at any moment, despite the security controls they made. This study focused on providing basic information about the ransomware that appeared in 2019, giving importance to the types that posed a greater threat and spread more widely such as REvil. In addition, it will shed light on the types of algorithms used in each ransomware type. As well as the studding of the amount of ransoms required from each type. I hope that this study will help the researchers and those who are interested in ransomware programs, and it will contribute to the challenges that faced computer science specialists.

2. Background
The following two sections will include the definition of ransomware and its trends in 2019.

2.1. Ransomware
Ransomware is malicious software that completely disables network systems and servers by encrypting them. It is an illegal act to earn money in illegal ways and demand a ransom of millions of dollars in exchange for decrypting the encrypted systems [1].

2.2. The Ransomware Trends in 2019
Ransomware attacks took a different trend in the previous years due to several factors, like:
1- The incremental ransomware attacks. According to (McAfee, 2019), the ransomware attacks grew by (118%), the detection of new ransomware families, in addition to the use of innovative techniques, in the first quarter of 2019 [2].
2- Difficulties, if not impossibility in decrypting the files targeted by the cybercriminals.
3- It became one of the powerful financial sources for the global cyber mafia and international gangs.
4- Incremental ransoms rates and amounts.
5- It has become a part of the electronic and intelligence war between countries, as happened between Iran and Israel, Russia and the USA, or between Russia and Ukraine.
6- Some attackers aim to disrupt the electronic services in some organizations and companies, for example, the paralysis of electronic services in American health sectors and organizations.
7- Denial – of - Services (DoS) in many countries.
8- The presence of parties that buy stolen information.

9- Boldness in electronic extortion to the extent that, the attackers leak a sample of your data in their websites.
10- Insolence in requesting of resending one of the encrypted files to be decrypted.
11- Insolence in selling your data to another party and telling you by that sale.
12- Deciding parties are anonymous and the location
13- The great calamity is that there are no guarantees to sell your data after extorting you and paying the required ransom.
14- The operations of the ransomware attacks do not stop at the limits of paying the required ransom only, but exceeded it to the following:
a- Disrupting the organization's activities.
b- The continuation of employees in taking their financial wages.
c- The institution's income stopped after the disruption and paralysis of its systems
d- The tarnish of the organization's reputation

3. Types of Ransomware

There are many types of ransomware, but this study focused on the ransomware that appeared in 2019, and the attacked countries, organizations, or companies. In addition to the different encryption algorithms used and the extortion, ransoms demanded. The following sections will include most of the ransomware that appeared in 2019.

3.1. Mega Cortex Ransomware

3.1.1. Mega Cortex Ransomware Description

Mega Cortex appeared in January 2019 with strange features, including offering security-consulting services. It uses Emotet and Qakbot to distribute in the network [3].

3.1.2. Countries, Organizations, or Companies Attacked by Mega Cortex

It attacked Italy, the USA, Canada, the Netherlands, Ireland, and France [3].

3.1.3. Mega Cortex Encryption Algorithms Used and Ransoms Demand

It uses two encryption algorithms, AES-256 and RSA 4096. The encryption of the victim's files is often done by the AES algorithm, and then generate the keys for each file by RSA. Therefore, these keys will be hidden in remote servers by cyber criminals [4]. After careful searches, there was no information about the amount of ransoms for Mega Cortex Ransomware, but many sources referred to ransom notes sent by the Mega Cortex actors.

3.2. Locker Goga Ransomware

3.2.1. Locker Goga Ransomware Description

It appeared in January 2019, when it attacked the French engineering consultancy Altran Technologies and affected the operations in many European countries [5].

3.2.2. Countries, Organizations, or Companies Attacked by Locker Goga

Locker Goga targeted the aluminum company Norsk Hydro, which is headquartered in Norway on March 19, 2019, as that attack led to the company losing between $35 to $41 million of its income, according to what the company announced at a press conference [5]. In addition, it disrupted Hexion and Momentive, which are two of the largest American companies in the field of chemistry [6].

3.2.3. Locker Goga Encryption Algorithms Used and Ransoms Demand

It uses two encryption algorithms, AES-128 to encrypt each file, and then generate a key for each encrypted file by using RSA-1024. [7] There was no information offered about the amount of ransoms for Locker Goga Ransomware.

3.3. CLOP Ransomware

3.3.1. CLOP Ransomware Description

CLOP ransomware group uses the double extortion tactic, and it appeared in February 2019 in an attack known as TA505. Like most of the other ransomware, it followed Ransomware-as-a-Service (RaaS) strategy [8].

3.3.2. Countries, Organizations, or Companies Attacked by CLOP

CLOP ransomware separated in many countries like Switzerland, Great Britain, Belgium, the United States, The Netherlands, Croatia, Porto Rico, Germany, Turkey, Russia, Denmark, Mexico, Canada, and the Dominican Republic [9]. In addition, CLOP operators attacked the UK water Supplier that provides water supplier, which services 16 million consumers daily in London [10]. In addition, it attacked the US, Australia, Brazil, Canada, Germany, Hong Kong, India, Mexico, Philippines, Singapore, Spain, Sweden, UK [8].

3.3.3. Clop Encryption Algorithms Used

It uses a combination of more than two encryption algorithms, which are AES – 256 and RSA-1024 and Chacha20 [11].

3.3.4. Clop Ransom Demand

Many sources indicated that CLOP ransomware requested ransoms from different companies like Software AG,

which is the second largest company in Germany, and demanded from it $23 million as a ransom [12]. In addition, Maastricht University in the Netherlands has paid about $220,000 as a ransom to the CLOP operators [13].

3.4. REvil Ransomware

3.4.1. REvil Ransomware Description

It appeared in April 2019, as a form of Sodinokibi ransomware and emerged as a new group named (GandCrab), where a member of this group confirmed that in an interview they used an old database obtained by the group [14]. It exploited the vulnerability (CVE-2019-2725) in the Oracle web logic server to make its first attack on Oracle on April 17, 2019. Also exploited a vulnerability in Microsoft Windows, which is (CVE-2018-8453) that allowed them to access victim's RAMs and obtained undetected administrative instructions to control victims' devices [15].

3.4.2. Countries, Organizations, or Companies Attacked by REvil

REvil attackers targeted about 200 American companies and disrupted their systems [16]. In addition, ransomware attacked several US states, including Maryland, Boston, and Georgia. As well as the disruption of electronic services and the required ransoms [17].

3.4.3. REvil Encryption Algorithms Used

t uses five encryption algorithms in one combined system, which are: Elliptic curve Diffie-Hellman (ECDH), Salsa20, AES, and Curve25519 to generate private-public key pairs using Curve25519 [18].

3.4.4. REvil Ransom Demand

(L. Constantin, 2021) referred that the ransom amounted to $40 million [19]. Moreover, according to (S. Battaglio, 2020), REVil operators hacked the files that threaten President Trump and they demanded $42 million as a ransom. In addition, REVil operators attacked Travelex Exchange Company in London and demanded $6 million as a ransom, and then Travelex paid $2.3 million of the ransom after the threat kept its services offline for several weeks [20]. While (L. Abrams, 2021) referred that JBS, which is the largest beef producer in the world paid $11 million to REvil as a ransom, after the ransomware group claimed $22.5 million [21].

3.5. Maze Ransomware

3.5.1. Maze Ransomware Description

Maze ransomware appeared in May 2019, and it uses a binary file from 32-bit. It encrypts the victim's files and sends the ransom notes [22]. Operators used an email as a way to distribute the Maze ransomware, and later they used more sophisticated methods and procedures to control the victim's devices and thus increase the extortion amounts [23].

3.5.2. Countries, Organizations, or Companies Attacked by Maze

Maze ransomware operators attacked the American company Cognizant, one of the information technology service providers, which resulted in the company losing between $50-$70 million of its income [24]. While (C. Dinu, 2021) referred that: Maze operators attacked the Allied Universal company and published 700 MB from the stolen data, also attacked the Hammersmith Medicines Research, in addition to their attack on Xerox company and stole more than 100 GB from the company [25].

3.5.3. Maze Encryption Algorithms Used

Maze uses two types of algorithms chacha20 and RSA, and in each operation, Maze generates a public RSA key to encrypt the files [26]. While (F. Sinitsyn, et al, 2020), referred that: Maze uses two algorithms, Chacha20 and RSA2048, such that the ChaCha20 keys and none values are encrypted by a session public RSA-2048 key, which is generated when the malware is launched; then the session private RSA-2048 key is encrypted by the master public RSA-2048 key [27].

3.5.4. Maze Ransom Demand

(G. Iddon, 2020) indicated that Sophos Managed Threat Response (MTR) team ensured that they were summoned by an organization to help it decrypt its files that were encrypted by Maze ransomware actors after they demanded a ransom of $15 million [28].

3.6. DoppelPaymer Ransomware

3.6.1. DoppelPaymer Ransomware Description

DoppelPaymer targeted its first victims in June 2019. It is an evolution of previous versions, where some improvements have been made to it [29].

3.6.2. Countries, Organizations, or Companies Attacked by DoppelPaymer

DoppelPaymer attacked many countries and organizations like the State Oil Corporation of Mexico, the Ministry of Agriculture of Chile, Apex of Farmingdale Laboratory of the USA, and the eminent emergency service of Germany [30]. In addition, it attacked about (911) call centers and about (380) servers in the healthcare field [31].

3.6.3. DoppelPaymer Encryption Algorithms Used

DoppelPaymer uses RSA-2048 and AES-256 encryption algorithms, and appends .locked extension to each file

[32].

3.6.4. DoppelPaymer Ransom Demand

(I. Arghire, 2020) referred that DoppelPaymer operators attacked the American medical center which required several weeks to restore their systems from offsite backups, and they demanded $600,000 as a ransom [33]. While (trend micro, 2021) referred that, the ransom of DoppelPaymer ranged between $25000 and $1.2 million [34].

3.7. NetWalker Ransomware

3.7.1. NetWalker Ransomware Description

It appeared in August 2019, and it follows the ransomware-as-a-Service (RaaS) tactic, which means that it is an integrated company with professional members, and infrastructure and its first goal is to raise money via extortion [35]. In addition, (HHS, 2020) referred that it was discovered in September 2019 with a compilation timestamp dating back to August 28, 2019. In addition, it is known as Malito, Koko, KazKavKovKiz and is operated as Ransomware-as-a-Service (RaaS) by a cybercrime group known as (Circus Spider). It exploited (CVE-2019-11510 and CVE-2019-18935) Vulnerabilities [36].

3.7.2. Countries, Organizations, or Companies Attacked by NetWalker

NetWalker members attacked several institutions and countries, including the University of California San Francisco (UCSF), and the attackers demanded ($3.0) million as a ransom in exchange for decrypting the university's systems. In February 2020, NetWalker attacked the largest Australian company (Toll Group). While in September 2020, the Pakistani Electric Corporation (K-Electric) was attacked by this ransomware, then the attackers demanded a ransom of ($3.8) million, which will become ($7.7) million in the event of non-payment [37].

While the Spaniards were suffering from the Corona Pandemic, which reached at that time (2020) thousands of people, and while Spanish hospitals are doing their best to provide medical services to the victims of Covid-19, NetWalker operators have sent a faked PDF that hospitals, to extort the Spanish health institutions [38].

(F. Erazo, 2020) referred that NetWalker attacked Michigan State University (MSU) and stole students' records and threatened to publish them if the university did not pay the required ransom, but (MSU) refused to pay the ransom [39]. In addition, NetWalker attacked the healthcare organizations Like Champaign-Urbana Public Health District, which is a public-health agency in Illinois, Crozer-Keystone that is a health organization in Philadelphia, and Lorien Health Services. In addition, to the Trento Metro attack in July 2020 [40].

3.7.3. NetWalker Encryption Algorithms

NetWalker uses a set of algorithms, which are: SHA256, CRC32, and RC4 KSA, which causes the ransomware to be strong in encryption [41].

3.7.4. NetWalker Ransom Demand

(B. Krebson, 2021), referred that: the money earned from NetWalker ransoms has reached more than ($46) million in the year 2020 [42].

3.8. LockBit2.0 Ransomware

3.8.1. LockBit2.0 Description

It appeared in September 2019 by the name (ABCD Virus), and it was named so because the victim's encrypted files have a part of this name in its extension. LockBit 2.0 belongs to the (Mega Cortex & Locker Goga) malware, and according to experts, it is a type of virus that targets organizations. (Server Message Block) and (Windows PowerShell), is exploited to distribute the malware to the network victims [43]. In addition, LockBit2.0 follows the double extortion tactic, after some improvements have been made to it, like port scanning, automatic distribution, and printing from the network [44].

3.8.2. The attacked Countries, Organizations, or Companies by LockBit2.0

According to the (BlackBerry, 2021) LockBit2.0 targeted the United States, Canada, Europe, Asia, and Latin America [45]. Wile (J. P. Bernardo, et al, 2020) in their report on (the Trend Micro website) referred that: LockBit2.0 targeted Chile, Italy, Taiwan, and the UK. So Chile is the most infected country[46].

3.8.3. LockBit2.0 Encryption Algorithms Used

((Arconis, 2021) referred that this ransomware uses a variety of cryptographic algorithms, from simple XOR, Tiny Encryption Algorithm (TEA), and AES-NI, to encrypt victims' files [47].

3.8.4. LockBit2.0 Ransom Demand

(E. Barlow, 2021) referred that LockBit2.0 attackers stole 6TB of Accenture company, and they demanded $50 million as a ransom [48]. While (A. Ivanyuk, et al, 2022) referred that: it attacked Bangkok Airways, which includes more than 3,000 employees in eleven countries, and threatened to publish 200GB of the company data [49].

3.9. Double Extortion Ransomware

3.9.1. Double Extortion Description

Double extortion is a development of Maze ransomware, after it back in November 2019. Known as (Name and Shame), and like other ransomware, it steals files and then encrypts them and contacts victims to pay the ransom or publish their sensitive data [50]. In addition, (M. Al-Dwairi, et al, (2022) referred that Double extortion attackers threaten to publish the stolen data if their demands are not met [51].

3.9.2. The attacked Countries, Organizations, or Companies by Double Extortion

Double extortion targeted the energy company based in Canada, and other 1200 ransomware incidents across 63 countries, with over (60%) of these aimed at the US and the UK. In addition, to hundreds of organizations [52].

3.9.3. Double Extortion Encryption Algorithms

It uses a combination system of two algorithms, Chacha20, which is used to encrypt the victims' files, and then the attackers, will give each file an encrypted key by using RSA – 2048 [53].

3.9.4. Double Extortion Ransom Demand

One of the double extortion groups named itself TA2102, attacked an American security company, Allied Universal, and demanded a ransom of ($2.3) million, with threatened to release the stolen data if the requested ransom was not paid [54].

4. Ransomware Information

4.1. Some Characteristics of Nine Ransomware in 2019

Table (1) illustrates the characteristics of the most dangerous ransomware that appeared in the year 2019. Therefore, the first column underlines the timeline for this ransomware. The second column presents the names of the nine ransomware. The third column presents the action (s) that can be done by each ransomware. The fourth column displays the average ransom demanded by each ransomware. The fives column presents the encryption algorithm (s) used by each ransomware.

Table (1) Some Characteristics of Nine Ransomware in 2019

I	Month	Name	Ransomware Action	Ransom	Algorithm
1	January	Mega Cortex	Offered security consulting services and uses Emotet and Qakbot to distribute in the network	Not determined	AES-256 RSA-4096
2	January	Locker Goga	Attacked many European countries and demand a ransom	Not determined	AES-128 RSA-1024
3	February	CLOP	Encrypts the victims' files and adds the ". clop" extension to the file	$23 million	AES – 128 RSA-1024
4	April	REvil	Attacked about 200 American companies and disrupted their systems	$50 million	AES –256 RSA-1024 ECDH+Curve25519 Salsa20+ AES
5	May	Maze	Effective in the tactic of publishing victim data and collecting two fees: Standard ransom and do not-publish $15 million ChaCha20 and RSA 2048	$15 million	ChaCha20 RSA 2048
6	June	DoppelPaymer	Attacked the Medical sectors in many countries	$1.2 million	AES-256 RSA-2048
7	August	NetWalker	Attacked the hospitals in the US and Spain	$10 million	SHA256 CRC32 RC4 + RSA
8	September	LockBit 2.0	The attacker overwrote the (MBR) requiring a password to boot.	$50 million	TEA + AES-NI
9	November	Double Extortion	Encrypts the victims' files and asks them to pay a ransom	$2.3 million	ChaCha20 RSA - 2048

4.2. The Countries, Organizations, and Companies Targeted by the Nine Ransomware in 2019

From Table (2), the first column presents the name of the nine ransomware. The second column presents the

countries or organizations attacked by each ransomware.

Table (2) listed the countries, organizations, or companies targeted by the nine ransomware in 2019.

I	Name	Countries/ Organizations/ Companies
1	Mega Cortex	USA, Canada, the Netherlands, Ireland, and France
2	Locker Goga	aluminum company Norsk Hydro, which is headquartered in Norway
3	CLOP	USA, Germany, India, Mexico, Russia, and Turkey, Switzerland, UK, Belgium, US, Netherlands, Croatia, Porto Rico, Germany, Russia, Denmark, Mexico, Canada, Dominican Republic.
4	REvil	200 American companies, several US states, including Maryland, Boston and Georgia, and the largest of these attacks were on Texas
5	Maze	Attacked the Allied Universal company and published 700 MB from the stolen data, also they attacked the Hammersmith Medicines Research, in addition to their attack on Xerox company
6	DoppelPaymer	380 servers in US medical sector
7	NetWalker	University of California San Francisco (UCSF), Australian company Toll Group, Pakistan Electric Corporation (K-Electric)
8	LockBit 2.0	Targeted the United States, Canada, Europe, Asia, and Latin America. In addition to Chile, Italy, Taiwan, and UK
9	Double Extortion	Targeted the energy company based in Canada, and other 1200 ransomware incidents across 63 countries. In addition, hundreds of organizations

5. Results

5.1. Ransomware Timeline 2019

From Table (1) we noticed that Mega Cortex and Locker Goga are the first ransomware that appeared in 2019, while Double Extortion is the last ransomware that appeared in 2019, which appeared in November. Figure (6) shows the ransomware timeline in 2019:

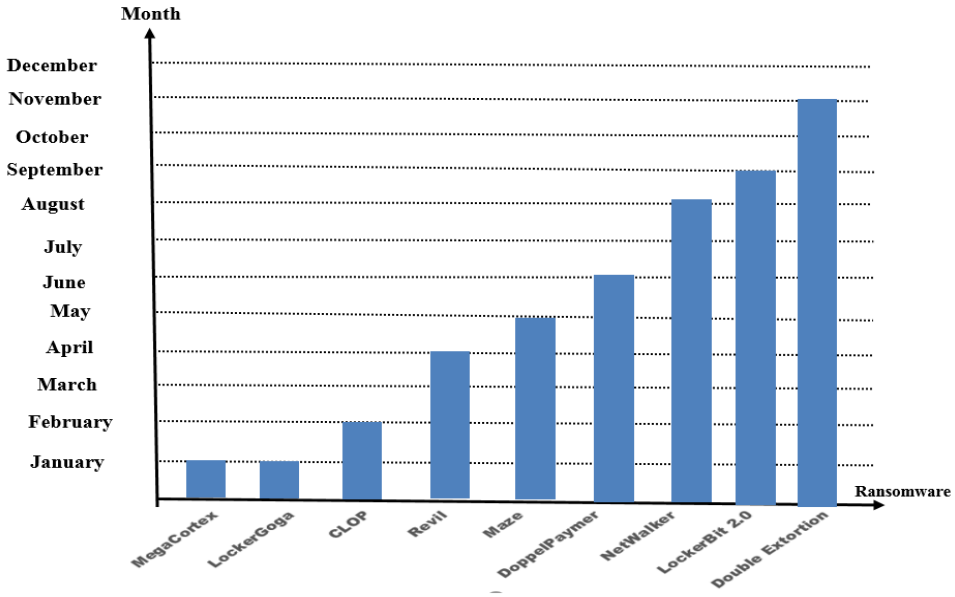

Figure (1) Ransomware Timeline 2019

5.2. Ransomware Algorithms Used in 2019

According to table (1), we found that: firstly, most of the ransomware uses a combination of two or three algorithms. Secondly, most the ransomware has common uses in AES and RSA algorithms. Thirdly, CLOP, REvil, and NetWalker ransomware used a combination of three algorithms, which are (AES-256, RSA-2048, and Chacha20). Surely using of combination gives strength to the encryption system, so the victims may find difficulties in decrypting their data, and may force them to pay the ransom.

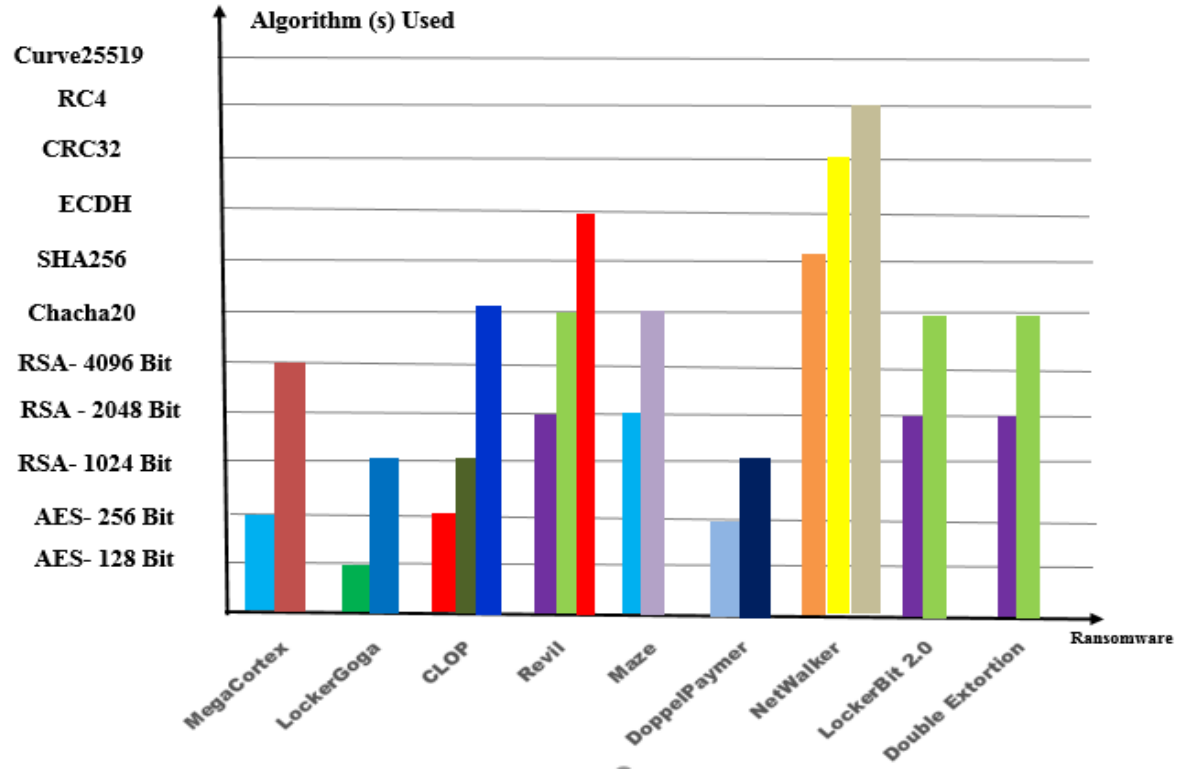

Figure (2) shows the algorithms used in Ransomware 2019.

5.3. Ransomware Ransoms Demanded in 2019

According to the values listed in table (1), we found that REVil and LockerBit2.0 are the highest amount of ransoms, which is ($50) million, while DoppelPaymer is lowest ransom, which is $1.2 Million. In addition, there are no values for both Mega Cortex and Locker Goga.

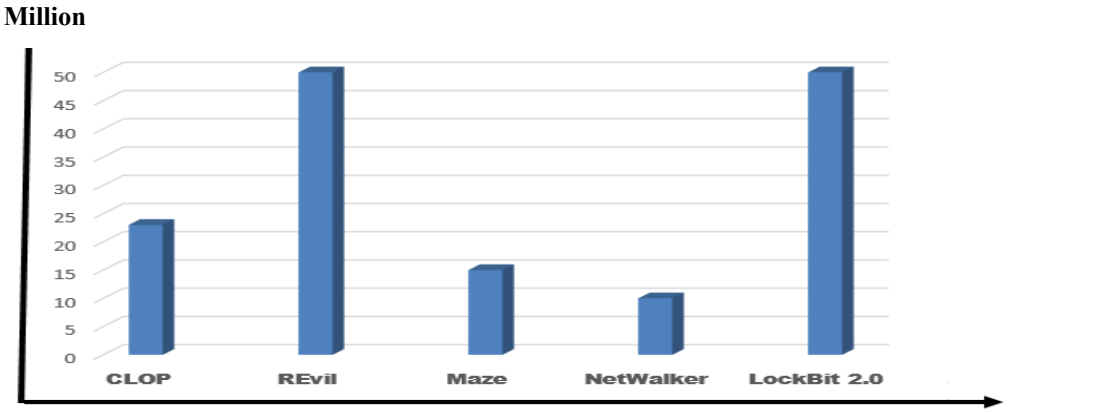

Figure (3) Some Averages of Ransoms Requested in 2019

5.4. Ransomware General Attacks in 2019

From Table (2) we found that: CLOP, REvil, and LockBit 2.0 are the most dangerous ransomware, they attacked many countries in Europe and Asia, in addition to many states in the USA.

References

[1] M. Aliperti, "What You Need to Know About Ransomware", November 15, 2020, [Online]. Available: https://www.doit.nh.gov/sites/g/files/ehbemt506/files/inline-documents/sonh/nl2020-11-ransomware.pdf
[2] "Cyber Attack Trends, 2019 Mid-year Report", 2019, McAfee Labs, [Online]. Available: https://www.ispin.ch/fileadmin/user_upload/partner/pdf/CP-mid-year-report-2019.pdf
[3] I. Arghire, "Cybercriminals Unleash Mega Cortex Ransomware in Global Attack Campaign", May 2019, [Online]. Available: https://www.securityweek.com/cybercriminals-unleash-megacortex-ransomware-global-

attack-campaign
[4] T. Meskauskas, “Megac0rtx ransomware removal instructions”, October 2021, [Online]. Available: https://www.pcrisk.com/removal-guides/15466-megac0rtx-ransomwareb
[5] T. Nayak, “The Locker Goga Ransomware Attack: A worst-case scenario for industrial operations”, June 2019, [Online]. Available: https://axaxl.com/fast-fast-forward/articles/the-lockergoga-ransomware-attack_a-worst-case-scenario-for-industrial-operations
[6] E. Kovacs, “Major U.S. Chemical Firms Hit by Cyberattack”, March 2019, [Online]. Available: https://www.securityweek.com/major-us-chemical-firms-hit-cyberattack
[7] G. More, “Ransomware as a Tool – Locker Goga”, July 2019, [Online]. Available: https://blogs.quickheal.com/ransomware-tool-lockergoga/
[8] H.C. Yuceel, “Clop Ransomware Gang”, August 2022, [Online]. Available: https://www.picussecurity.com/resource/clop-ransomware-gang
[9] A. Mundo, “CLOP Ransomware”, August 2019, [Online]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/clop-ransomware/
[10] E. Montalbano, “U.K. Water Supplier Hit with Clop Ransomware Attack”, August 2022, [Online]. Available: https://threatpost.com/water-supplier-hit-clop-ransomware/180422
[11] J. Walter, "The Good, the Bad and the Ugly in Cybersecurity – Week 25", June 18, 2021, [Online]. Available: https://www.sentinelone.com/blog/the-good-the-bad-and-the-ugly-in-cybersecurity-week-25-2/
[12] S. Ikeda, “Clop Ransomware Attack Hits German Software Giant Software AG; Confidential Documents Stolen, $23 Million Ransom Demanded”, October 2020, [Online]. Available: https://www.cpomagazine.com/cyber-security/clop-ransomware-attack-hits-german-software-giant-software-ag-confidential-documents-stolen-23-million-ransom-demanded/
[13] A. Bannister, “Ransomware attack: Maastricht University pays out $220,000 to cybercrooks”, May 2020, [Online]. Available: https://portswigger.net/daily-swig/ransomware-attack-maastricht-university-pays-out-220-000-to-cybercrooks
[14] L. Constantin, “REvil ransomware explained: A widespread extortion operation”, November 2021, [Online]. Available: https://www.csoonline.com/article/3597298/revil-ransomware-explained-a-widespread-extortion-operation.html
[15] T. DiMaggio, A history of REvil, January 27 2019, [Online]. Available: https://analyst1.com/file-assets/History-of-REvil.pdf
[16] J. Kane, A 'Colossal' Ransomware Attack Hits Hundreds Of U.S. Companies, A Security Firm Says, July 3, 2021, [Online]. Available: https://www.npr.org/2021/07/03/1012849198/ransomware-cyber-attack-revil-attack-huntress-labs
[17] " Virsec Systems, Ransomware (Sodinokibi/REvil) Attacks Rising Against Many Cities, Striking Local Governments & School Campuses, August 30, 2019, [Online]. Available: https://www.virsec.com/blog/ransomware-attacks-rising-against-many-cities-striking-local-governments-school-campuses
[18] " REvil/Sodinokibi Ransomware vs. The Health Sector", HHS, August, 2021, [Online]. Available: https://www.hhs.gov/sites/default/files/revil-update-tlpwhite.pdf
[19] L. Constantin, “REvil ransomware explained: A widespread extortion operation”, November 2021, [Online]. Available: https://www.csoonline.com/article/3597298/revil-ransomware-explained-a-widespread-extortion-operation.html
[20] S. Battaglio, Celebrity law firm won’t pay ransom to hackers claiming to have ‘dirty laundry’ on Trump, May 18, 2020, [Online]. Available: https://www.latimes.com/entertainment-arts/business/story/2020-05-18/hackers-demand-42-million-to-keep-from-leaking-law-firms-stolen-data-on-president-trump
[21] L. Abrams, JBS paid $11 million to REvil ransomware, $22.5M first demanded, June 10, 2021, [Online]. Available: https://www.bleepingcomputer.com/news/security/jbs-paid-11-million-to-revil-ransomware-225m-first-demanded/
[22] R. Shemesh, “What is Maze Ransomware and How Does it Work?”, May 2021, [Online]. Available: https://www.datto.com/nl/blog/what-is-maze-ransomware-and-how-does-it-work
[23] C. Dinu, Maze Ransomware: Origins, Operating Mode, Attacks, November 4, 2021[Online]. Available: https://heimdalsecurity.com/blog/maze-ransomware-101/
[24] K. Yasar, “What You Need to Know About the Cognizant Maze Ransomware Attack”, February 2021, [Online]. Available: https://www.makeuseof.com/know-about-cognizant-maze-ransomware/
[25] C. Dinu, “Maze Ransomware: Origins, Operating Mode, Attacks”, November 2021, [Online]. Available: https://heimdalsecurity.com/blog/maze-ransomware-101/
[26] A. Mundo, “Ransomware Maze”, March 2020, [Online]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/
[27] F. Sinitsyn, et al, “Life of Maze ransomware”, October 2020, [Online]. Available: https://securelist.com/maze-

ransomware/99137/
[28] G. Iddon, “MTR Casebook: Blocking a $15 million Maze ransomware attack”, September 2020, [Online]. Available: https://news.sophos.com/en-us/2020/09/22/mtr-casebook-blocking-a-15-million-maze-ransomware-attack/
[29] B. Stone-Gross, et al, “BitPaymer Source Code Fork: Meet DoppelPaymer Ransomware and Dridex 2.0”, July 2019, [Online]. Available: https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/
[30] A. Yurchenko,” DoppelPaymer Ransomware Detection”, January 2021, [Online]. Available: https://socprime.com/blog/doppelpaymer-ransomware-detection/
[31] F.J. Thomas, “Stolen County Data Viewed More Than 30,000 Times Online”, 2022, [Online]. Available: https://www.wci360.com/stolen-county-data-viewed-more-than-30000-times-online/
[32] L. Kiguolis, “DoppelPaymer ransomware (Virus Removal Instructions)”, April 2020, [Online]. Available: https://www.2-spyware.com/remove-doppelpaymer-ransomware.html
[33] I. Arghire, “FBI Warns of DoppelPaymer Ransomware Targeting Critical Infrastructure”, December 2020, [Online]. Available: https://www.securityweek.com/fbi-warns-doppelpaymer-ransomware-targeting-critical-infrastructure
[34] TrendMicro, "An Overview of DoppelPaymer Ransomware", January 05, 2021, Available Online: https://www.trendmicro.com/en_dk/research/21/a/an-overview-of-the-doppelpaymer-ransomware.html
[35] Cybereason Nocturnus, "Cybereason vs. NetWalker Ransomware", February 16, 2021, [Online]. Available: https://www.cybereason.com/blog/research/cybereason-vs.-netwalker-ransomware
[36] "NetWalker Ransomware", HHS, February 9, 2022, [Online]. Available: https://www.hhs.gov/sites/default/files/netwalker.pdf
[37] I. Thomas, “Ransomware Gangs: NetWalker”, January 2022, [Online]. Available: https://ironscales.com/blog/ransomware-gangs-netwalker
[38] J. Walter, “NetWalker Ransomware: No Respite, No English Required”, June 2020, [Online]. Available: https://www.sentinelone.com/labs/netwalker-ransomware-no-respite-no-english-required/
[39] F. Erazo, “Michigan State University Hit by Ransomware, Refuses to Pay Criminals”, June 2020, [Online]. Available: https://cointelegraph.com/news/michigan-state-university-hit-by-ransomware-refuses-to-pay-criminals
[40] Emsisoft Lab, "NetWalker Profile", February 15, 2021, [Online]. Available: https://blog.emsisoft.com/en/37677/ransomware-profile-netwalker/
[41] P. Travares, “NetWalker ransomware full analysis” September 2021, [Online]. Available: https://seguranca-informatica.pt/netwalker-ransomware-full-analysis/#.YxQFmX1BwnQ
[42] B. Krebson, "NetWalker Profile", February 15, 2021, [Online]. Available: https://krebsonsecurity.com/2021/01/arrest-seizures-tied-to-netwalker-ransomware/
[43] "LockBit ransomware — What You Need to Know", Kaspersky, 2020, [Online]. Available: https://www.kaspersky.com/resource-center/threats/lockbit-ransomware
[44] " Cybereason vs. LockBit2.0 Ransomware", Cybereason Nocturnus, August 24, 2021, [Online]. Available: https://www.cybereason.com/blog/research/cybereason-vs.-lockbit2.0-ransomware
[45] "How LockBit 2.0 Ransomware Works and Indicators of Compromise", BlackBerry Research and Intelligence team, December 8, 2021, [Online]. Available: https://blogs.blackberry.com/en/2021/08/threat-spotlight-lockbit-2-0-ransomware-takes-on-top-consulting-firm
[46] J. P. Bernardo, et al, “LockBit Resurfaces with Version 2.0 Ransomware Detections in Chile, Italy, Taiwan, UK”, August 2020, [Online]. Available: https://www.trendmicro.com/en_us/research/21/h/lockbit-resurfaces-with-version-2-0-ransomware-detections-in-chi.html
[47] "Threat analysis: LockBit ransomware", Acronis, July 5, 2021, [Online]. Available: https://www.acronis.com/en-us/blog/posts/lockbit-ransomware/
[48] E. Barlow, “Cyber Consulting Company, Accenture, Hit by LockBit Ransomware Attack”, August 2021, [Online]. Available: https://www.securityhq.com/blog/cyber-consulting-company-accenture-hit-by-lockbit-ransomware-attack/
[49] A. Ivanyuk, et al, “Acronis Cyber Threats Report 2022”, 2022, [Online]. Available: https://dl.acronis.com/u/rc/White-Paper-Acronis-Cyber-Protect-Cloud-Cyberthreats-Report-Mid-year-2022-EN-US-220811.pdf
[50] C. Page, “The rise of double extortion ransomware”, May 2022, [Online]. Available: https://www.itpro.co.uk/security/ransomware/367624/the-rise-of-double-extortion-ransomware
[51] M. Al-Dwairi, “Ransomware-Resilient Self-Healing XML Documents, Department of Computer Engineering, Jordan University of Science and Technology, Jordan”, April 2022, [Online]. Available: https://www.researchgate.net/publication/359811458_Ransomware-Resilient_Self-Healing_XML_Documents
[52] B. Leddy, “Double Extortion Ransomware”, May 2021, [Online]. Available: https://darktrace.com/blog/double-extortion-

ransomware#:~:text=Darktrace%20has%20detected%20a%20huge,quickly%20and%20stealthily%20once%20inside

[53] "Mount Locker Ransomware-as-a-Service Offers Double Extortion Capabilities to Affiliates", BlackBerry Research and Intelligence team, November 12, 2020, [Online]. Available: https://blogs.blackberry.com/en/2020/12/mountlocker-ransomware-as-a-service-offers-double-extortion-capabilities-to-affiliates

[54] " What is double extortion Ransomware?", August 22, 2022, [Online]. Available: https://www.packetlabs.net/posts/double-extortion-ransomware/