Obsolete Ransomware: A Comprehensive Study of the Continued Threat to Users

Arsh Arora, Ragib Hasan, Gary Warner
University of Alabama at Birmingham
Birmingham, Alabama, USA

Abstract

There are many variants of different malware (malicious software) like trojans, adware, keylogger, worms, and others, but ransomware is the most catastrophic among them. Ransomware is the type that encrypts the user file system and seeks compensation in return to make it usable again. Ransomware has been evolving at a massive pace and reached an all-time high, with 552 variants recorded in the year 2017 and 352 variants in 2018. In comparison to the prior years, the number was significantly higher than the combination of all the previous years. The primary reason for this massive shift is the ease of production of new ransomware variants as well as ransomware being used as a service. The paper highlights a worrying state for the current safeguard measures of the anti-virus industry, a significant majority, more than 50% of ransomware samples produced in both the years are actively encrypting the users' machine. Despite the advancement and regular monitoring of the anti-virus industry, the ransomware problem remains a significant issue. The concern is not only for the industry but also for the end-user as the new variants are being produced regularly, and old variants are not being eliminated. The following paper tries to raise awareness among the community about the increasing ransomware problem and the importance of taking proper preventive measures to safeguard against the rising attacks.

1. Introduction

Different types of malware and method of infections are being developed continuously to impact the maximum number of users. The rise in the users that have been provided access to the internet and email technology has not helped the cause. With this increase in users, criminals have found a readily available list of targets that can be exploited with these new techniques of malware infections. Although the malware infections have been on the continuous rise, a no Table change was observed in the past couple of years. The criminals started to get attracted to the 'Ransomware' variant from among all the different types of malware. Ransomware is a type of malware that encrypts the user machine and seek currency in return to make the machine usable again. Since the year 2016, ransomware was the hot topic among the security industry as it drastically began impacting the end users with rising attacks. On the other hand, there were not enough preventive measures to safeguard the end users against these ransomware attacks. As can be seen in the Figure 1, there is a steep increase from the year 2015 onwards in the ransomware variants. Prior to 2015, other types of malware were dominant but 2016 changed the threat landscape completely as it was dominated by ransomware and banking trojans, with ransomware leading the charts since then. According to the Malware Year in Review 2016 from various security companies , malware infections increased tremendously more than predicted [1], [2], [3]. The year 2016 was the year that revolutionized malware infections leading to an escalation in the ransomware infections [4]. The threat actors were captivated by the ransomware and focus all their attention towards the production of new ransomware families. When compared to previous years, ransomware infections say a substantial change as mentioned in the Yearend report.

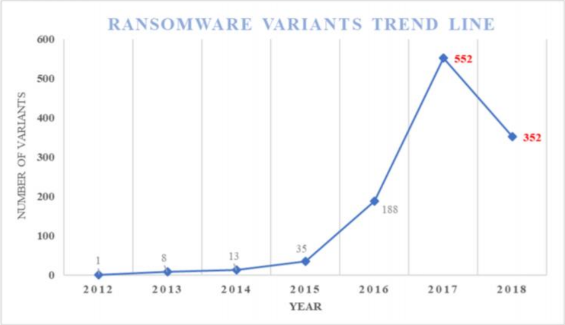


Figure 1. Ransomware Variants Trend

The graph shows an upward trend for the year 2016 to 2017 with a slight dip in 2018. Despite the decrease, the ransomware was able to maintain the consistency of producing a new variant daily on an average. The paradigm shift in the malware production and distribution was a high motivation for the researcher to start learning about ransomware.

2. Literature Review

The primary focus of this paper is the ransomware variants for the year 2017. There has been little research focused on these variants as most of the variants were fresh and never seen before. In one of the papers Kharraz et al., the authors described the growth of ransomware and all its variants from 2006 to 2014 [12]. Few other papers primarily focused on the 'CryptoWall' ransomware as it was the most dominant for the year 2015 [13]. In another paper, different botnets were discussed, along with the understanding of the internal infrastructure and the spam campaigns associated with the different botnets [14]. The 'Locky' ransomware campaign brought a dynamic change in the ransomware industry as it yielded the maximum revenue as well as initiated the ransomware business being distributed as a service [15]. The paper described the various stages of the campaign and how the ransomware evolved from its inception. In this paper, researchers are trying to carry on the tradition and providing a case study of all the ransomware samples recorded in the year 2017.

3. Revenue Generated for the year 2016

As in most cases, money earned, or revenue plays a critical role in determining the success or failure of a business. Ransomware business provided fruitful results that it attracted many individuals who initiated and started joining the ransomware business. The hypothesis became evident when there was a sudden upsurge in ransomware production over the past couple of years. Also, the number of attacks started increasing, and ransomware took the top spot in the malicious payloads that were being delivered by email to infect the end-users or organization. It became extremely convenient for criminals to conduct their business as there was minimal fear of being caught or taken into custody. Another positive benefit for the attackers was that more than 85% of victims paid the ransom amount as they did not want to experience any difficulties in their daily routine activities.

The rise in the ransomware was initiated by a single ransomware campaign that was distributing Locky Ransomware. Necurs botnet distributed locky ransomware, and the botnet constitutes approximately 55-60% of the entire spam in the world [5]. After the takedown of the Kelihos Botnet, Necurs botnet took over and started to dominate the spamming community [6], [7], [8]. It was estimated that the Locky ransomware campaign yielded 7.8million US dollars in revenue for the criminals. Other variants that were dominating, in terms on revenue, seen in the Figure 2 were Cerber, CryptoLocker, CryptoWall, SamSam and many others [9].

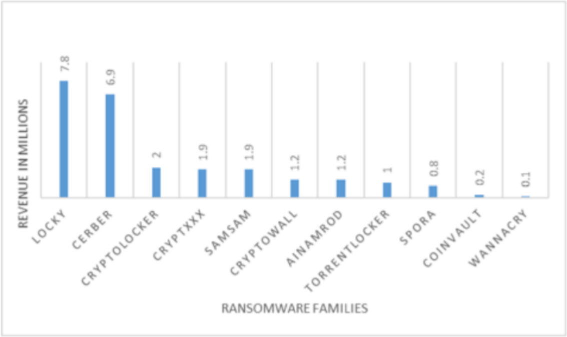


Figure 2. Revenue Generated by Ransomware Campaigns

4. Variants in 2017

In the paper, researcher will provide the recap of the ransomware landscape for the year 2017, which displays 384 unique ransomware variants that were recorded, 430 unique ransomware extension. The most alarming aspect of the landscape is that 243 ransomware binaries are still active and encrypting even at the end of Q4 in 2018.

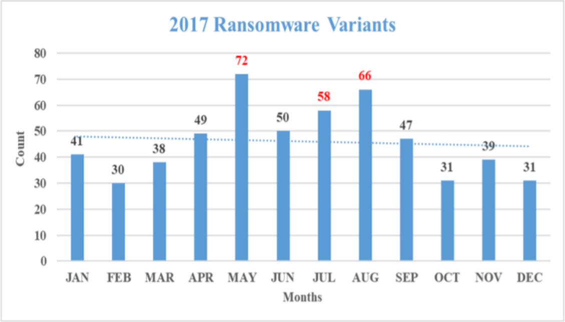


Figure 3. 2017 Ransomware Variants - 552

The following Figure 3 display the ransomware production increase for the 2017 [10]. In the year 2017, a large number of ransomware variants were seen in the wild. According to the bleeping computer website, there were 552 variants reported. Bleeping computer website writes a weekly report on the new ransomware found by their researchers as well as the ones reported to the website authors [11].

5. Variants in 2018

A similar pattern was observed in 2018 with the consistent growth of producing one ransomware per day. Another interesting thing to note in the Figures 3 and 4 is the trend for individual months. The trend for both the years is similar as a decrease in the 2nd and 3rd month, followed by increase and reaching high potential in 5th month, then again observing a decrease for a month then to again rise up for the coming months, and followed by up and down trend for the end of the year.

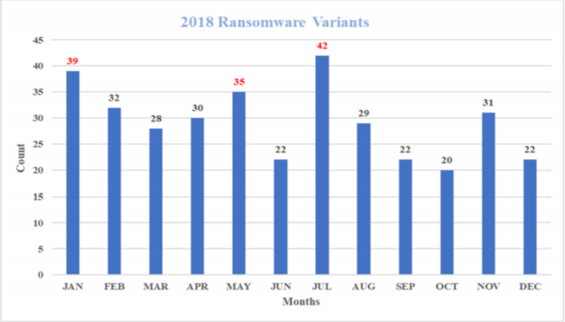


Figure 4. 2018 Ransomware Variants - 352

In the paper, researcher will be provide the recap of the ransomware landscape for the year 2017 and 2018, which displays the unique ransomware variants that were recorded, along with, unique ransomware extensions. The most alarming aspect of the landscape is that 243 ransomware binaries from the year 2017 are still active and encrypting even at the end of Q4 of 2018. For ransomware binaries of 2018, ?? variants are actively encrypting in Q4 of 2019. The next section discusses the different types of ransomware attacks, followed by understanding the functioning of ransomware, then followed by testing the available ransomware samples from the year 2017 and 2018, discussion of results and future work with conclusion.

6. Ransomware Attacks

To understand the ever-growing problem of ransomware, one has to be familiar with the attack vector of how ransomware infiltrates and performs the necessary encryption functions. In addition, be familiar with the different types of ransomware that are produced to infect users. There are two types of attacks that are prevalent:

6.1. Locker Ransomware

Locker ransomware is the ransomware that encrypts the file system, locks the screen, and displays the ransom note. The attacker tries to exploit a vulnerability in hardware or software and encrypt's the Master File Table (MFT) to make it unusable for the organization. These attacks are performed on a large-scale and encrypt the entire organization's file system. Another interesting fact is that the amount of ransom demand is much higher when compared to individual crypto ransomware. Locker ransomware is difficult to analyze as the entry point is a tiny vulnerability, but the impact is organization-wide, thus, makes the timely detection extremely difficult before the actual attack. This type of ransomware are quite sophisticated and are a handful, yet more impactful.

6.1.1 WannaCry. A worldwide outbreak occurred on the 12th of May 2017, when WannaCry ransomware crypto worm infected encrypted more than 200,000 Microsoft Windows computer across 150 countries [16]. WannaCry exploited a vulnerability of the Windows that was identified in the implementation of the Server Message Block (SMB) protocol. Although Microsoft released the patch, NSA created a code 'Eternal Blue' to exploit the SMB protocol vulnerability. The 'Eternal Blue' code was stolen by a hacking group called Shadow Brokers and leaked, which led to the eventual attack. A security researcher named 'Marcus Hutchins' accidentally discovered a kill switch domain that, when replied with a definite answer, would stop WannaCry from infecting the users. Soon after the heroic event, Hutchins was arrested for the development of the Kronos Banking Trojan malware in 2014 [17].

6.1.2. SamSam Ransomware. SamSam is a ransomware that primarily targets healthcare industry. The attack mechanism is to exploit a wide range of already known vulnerabilities or brute-forcing weak passwords [18]. In the initial phase, SamSam was known to exploit a vulnerability in the JexBoss (JBoss) host servers to compromise the server, then install backdoors for remote access and eventually dropped the malicious ransomware payload to infect the entire file system of the organization [19]. In the later phase, SamSam upgraded to focus on vulnerabilities in the Java-based web applications and servers, remote desktop protocols (RDP), file transfer protocol(FTP) servers to gain access to the victims' machines. The most impactful outbreak of the SamSam ransomware was when it caused severe outrage in five out of 13 local government offices of the city of Atlanta in the USA [20].

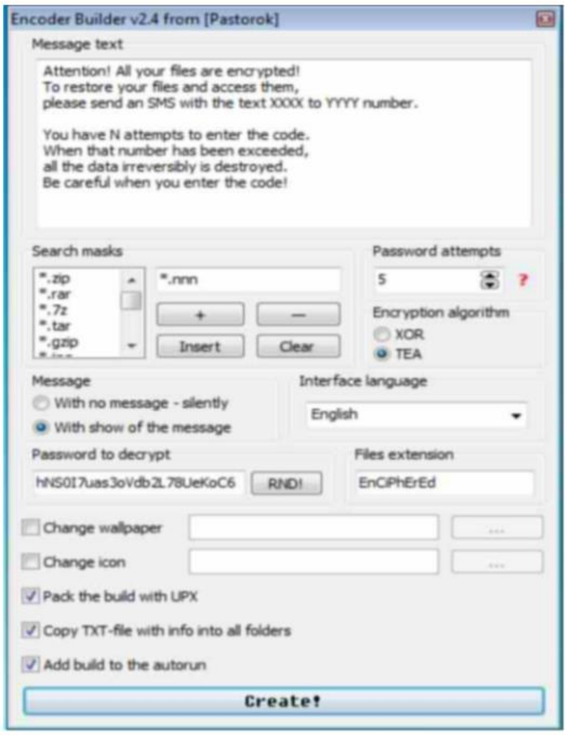
6.2. Crypto Ransomware

Crypto ransomware is the ransomware that encrypts the user's files and seeks a ransom payment in return to make the files usable again. These are the most commonly used attacks, directing towards a unique and wide variety of users. The targets range include organizations, large or small business, government officials, students, individual home users, and others. In comparison to the locker ransomware, crypto ransomware is less dangerous but impact a large population. The crypto ransomware has the highest number of variants, and it is incredibly convenient to create new variants. As shown in Figure 3, there were 552 variants produced by the ransomware in the year 2017. Crypto ransomware is more commonly used than the locker ransomware due to the ease of reproduction. Due to a large number of variants being produced, researchers were highly motivated to do an in-depth analysis on the crypto ransomware to learn more about their production, distribution, and to develop a prevention solution against these attacks.

6.2.1. Production of Ransomware Variants. For the past couple of years, crypto ransomware has been on an all-time high, with many variants being produced regularly with an average of more than one new ransomware per day. The rise is scary as the development of these attacks is much higher than the preventive measures developed against these ransomware attacks. The attackers are always leading the pack, but the defenders always end up playing the catch-up game. The resulting gap between the attackers and defenders is always widening without any proper measures taken to reduce this gap. These were a few of the reasons that attracted the researchers to focus on the core problem of these new ransomware variants as to why such a large number is produced and the impact created by these new ransomware variants. For this thesis, the researcher only focused on the variants produced in the year 2017 as it had the most significant number of variants produced when compared to previous years.

Over the past few years, production ransomware binaries have become extremely convenient and accessible to the experienced as well as newbie attackers. Numerous software is developed that can generate a customized ransomware binary in a short duration without any hassle. In turn, these binaries are sold to the newbie attackers with the promise of sharing profit after the successful recovery of the ransom payment after encrypting the end-users files. The attackers tend to partner with the creators of already developed software rather than creating their ransomware binary from scratch. It seems to be more futile for the attackers as there is less investment of time and resources, but a higher return on investment.

From the facts mentioned above, it becomes evident that ransomware is the most catastrophic variant out of the entire malware community. The speed at which it is increasing makes it much more attractive for budding attackers to contribute to the production and distribution of new ransomware variants. One of the primary reasons for the increase in the ransomware variants is the 'Ease of production of new ransomware variants.' As can be seen in Figure 5, a Graphical User Interface (GUI) is displayed on how to create a ransomware [21]. The steps mentioned are convenient and can be followed by any individual with the necessary computer skills.



Encoder Builder v2.4 from [Pastorok]

Message text

Attention! All your files are encrypted!
To restore your files and access them,
please send an SMS with the text XXXX to YYYY number.

You have N attempts to enter the code.
When that number has been exceeded,
all the data irreversibly is destroyed.
Be careful when you enter the code!

Search masks: *.zip, *.rar, *.7z, *.tar, *.gzip; *.nnn

Password attempts: 5

Encryption algorithm: ○ XOR ● TEA

Message: ○ With no message - silently ● With show of the message

Interface language: English

Password to decrypt: hNS0I7uas3oVdb2L78UeKoC6

Files extension: EnCiPhErEd

□ Change wallpaper

□ Change icon

☑ Pack the build with UPX

☑ Copy TXT-file with info into all folders

☑ Add build to the autorun

Figure 5. Ransomware Encoder Builder

The message text areas display the ransom note that will be seen by victims after infection, search masks are the file extensions that are to be searched for encrypting the specific files, '*.nnn' is the extension that will be appended at the end of the new file name, one can also select their choice of wallpaper and icon. The final step is to hit the magic button 'Create' to generate the binary that will be used to infect the victims.

In Figure 5, it is displayed that building a ransomware binary is convenient and can easily be created without requirements of technical skills. The convenience in ransomware production attracted several newbies or buddying cybercriminals to try and send spam/phishing messages with embedded ransomware links or attachment. An additional factor is that the risk involved is significantly less because of the geo-location barrier. All of the mentioned factors lead to ransomware spreading being advertised as a service.

6.2.2. Ransomware as a Service. Ransomware is used as a service in which a binary is produced by the help of similar builders as displayed in Figure 5 and then distributed to the attackers, who, in turn, share the profit from infection among themselves and the operator of the ransomware builder. Some of the Ransomware as a Service kit providers are:

• Philadelphia - It is the most sophisticated and have options to personalize, and one get an unlimited license for $389.

• FrozrLocker - FileFrozr kits can encrypt 250 extensions for the price of 0.14 in bitcoins. A license is required to use the builder.

• Satan - The operators create a ransomware sample, that is available for download. The service providers infect and collects the ransom on the attacker's behalf and pays out 70% of the proceeds to the attacker.

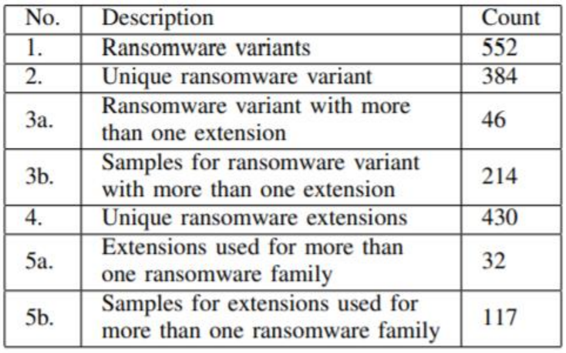
• RaasBerry - This service is for long term investors in which they have many packages ranging from daily, weekly or monthly at different prices.

New binaries with slight variations of name or extension are being developed with the same source code, which is one of the primary reasons for massive growth in the crypto ransomware production and distribution [22].

7. Statistics - 2017

The year 2016 was referred to as the 'year of ransomware,' but the year 2017 led the ransomware industry to a new level. Out of the 552 variants recorded, there were 384 unique ransomware variants. Out of the 384 variants, 46 of them had variants with more than one extension appended at the end of the encrypted files. The combined number of samples for the 46 variants was 214.

Table 1. Ransomware Statistics - 2017



No.	Description	Count
1.	Ransomware variants	552
2.	Unique ransomware variant	384
3a.	Ransomware variant with more than one extension	46
3b.	Samples for ransomware variant with more than one extension	214
4.	Unique ransomware extensions	430
5a.	Extensions used for more than one ransomware family	32
5b.	Samples for extensions used for more than one ransomware family	117

Additionally, there were 430 unique ransomware extensions recorded. Out of the 430 extensions, 32 of them were used by more than one ransomware family, totaling 117 different samples. Due to an extensive range of ransomware variants, it became enticing to Figure out the ransomware samples that were still active and infecting the end users.

The count of different ransomware produced in 2017 is shown in Table 1. A large number of samples with the same family name with different extensions or different families with the same extension is quite surprising.

The numbers raise a suspicion that there is some connection at the back end of the ransomware builders either they are working in conjunction or all of these ransomware's are being developed by the same individual or group of individuals. Also, maybe the builders are using the ransomware builder tool as a service and providing it to budding attackers.

7.1. Different Extensions Same Family

Many ransomware families were known to be of the same family but had more than one extension. In the year 2017, 46 ransomware families used more than one extension to encrypt end-users' files during different times of the year. The recurring ransomware variants were not part of a single campaign but various campaigns over the year. A direct indication that these were the long-lasting campaigns without proper preventive measures by the anti-virus industry. In total, 214 ransomware variants were recorded to be sent by the 46 different ransomware families. Among these different families, the dominant ones were 'GlobeImposte,' 'Jigsaw,' 'SamSam,' 'BTCWare,' 'Locky,' 'CryptoMix,' 'Oxar,' 'Xorist,' and many others as shown in Figure 6. In the year 2017, GlobeImposter is the most dominant ransomware family, with 41 extensions used during the year.

7.2. Same Extension Different Family

Similar to having different extensions for the same family name, there were instances in which the different ransomware families used the same extensions. Thirty-two different extensions were used by more than one ransomware family, with a total of 117 samples. Some of the prominent extensions used were 'locked,' 'encrypted,' 'enc,' 'crypt,' 'fucked,' 'fun,' and others are shown in Figure 7, with locked being the most commonly used by 29 different ransomware families. Combination of Different Families and Extensions There are many variations among the ransomware families, as can be seen in Figure 6 and 7. Additionally, there was quite a bit of overlap and linkages when reviewed the top contenders in the same chart, as shown in Figure 8.

The Figure 8 demonstrates differentransomware families with the shape of a 'Circle' and different extensions with the shape of a 'Square.' 'GlobeImposter' and 'BTCWare' are the dominant ransomware families with multiple extensions. On the other side, 'locked' and 'enc' leading thepack for the extensions used, followed by 'wallet' and 'crypt.'

An exciting thing to note is the overlap of the four different extensions for particular ransomware.

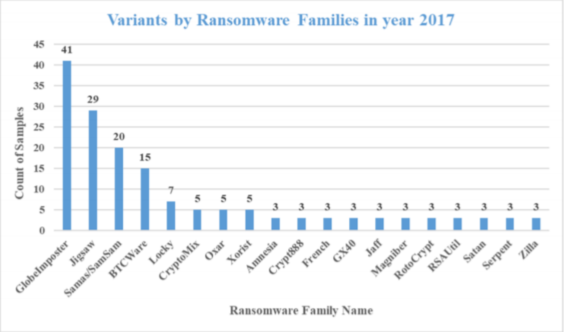


Figure 6. Ransomware Variant with More Than One Extension

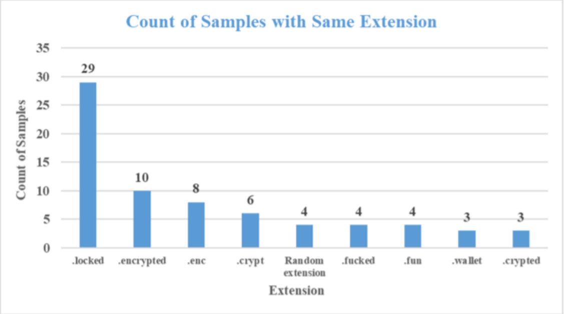


Figure 7. Extensions Used for More Than One Ransomware Family

For instance, 'GlobeImposter' is seen to use the 'wallet,' 'locked,' and 'crypt' extensions, but 'crypt' is also used by 'Cypher' and 'DynA-Crypt' ransomware family. Based on that, does it mean that all the three ransomware families are the same, or are they being operated by the same group of individuals or organization.

Similarly, 'wallet' extension is used by both 'BTCWare' and 'GlobeImposter,' so does that make both of them the same or is it a mere coincidence. Along the same lines, 'locked' extensions have 29 variants, including 'GlobeImposter,' so does that mean all the ransomware developed with 'locked' extension are created by the same individual or same ransomware builder tool.

8. Statistics - 2018

A similar trend was seen in 2018 when compared to 2017; there was 352 number of ransomware variants produced in the year as shown in Table 2.

Table 2. Ransomware Statistics – 2018

No.	Description	Count
1.	Ransomware variants	352
2.	Unique ransomware variant	223
3a.	Ransomware variant with more than one extension	36
3b.	Samples for ransomware variant with more than one extension	164
4.	Unique ransomware extensions	273
5a.	Extensions used for more than one ransomware family	25
5b.	Samples for extensions used for more than one ransomware family	60

Due to the unavailability of a decent number of samples whose hashes were not available in 2017, researchers decided to ignore those for the year 2018 except for the ones that had duplicates either with different ransomware name or extension, therefore, the decrease in the total number of ransomware variants when compared to 2017, in addition to the low production for the year. Another fact is that even though there was low production, but the ransomware attacks were more specific to industries and organizations. Upon researching, it was calculated that among the 352 ransomware variants, there were 223 unique ransomware variants. As predicted based on the year 2017, out of 223 variants, 36 ransomware variants had more than one extension. The total count of the duplicate ransomware variants was 164. On the contrary, 273 unique extensions were recorded, with 25 of them being used by more than one ransomware family. The total samples for those extensions were calculated to be 60. The Figures and methods of production and distribution remained similar for both the years.

8.1. Different Extensions Same Family

Inspired by the 2017 variants shown in Figure 6, the researcher displayed a similar graph of the ransomware variants that had more than one extension. In the year 2018, as shown in Figure 9, 'Dharma' and 'Jigsaw' ransomware families claimed the first and second position respectively, followed by 'RotorCrypt,' 'GandCrab,' 'Matrix,' 'Scarab,' and so on. Last year, 'GlobeImposter' was the most dominant family but was not able to create the same impact for 2018, as 'Dharma' ransomware was the topmost family with 29 variants. An interesting thing to observe is that 'Jigsaw' family has been consistent in the second spot for both the years with 29 variants in 2017 and 27 in 2018. To conclude, 36 different ransomware families were observed to have more than one extension in the year 2018, constituting a total of 164 samples.

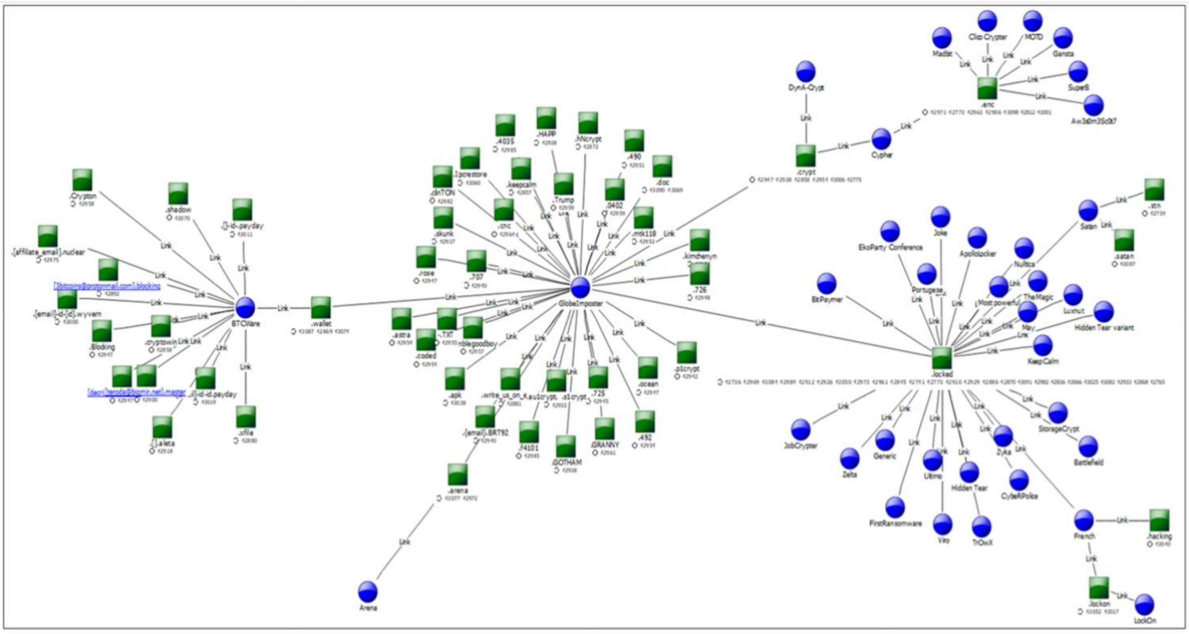


Figure 8. Top Results Combined

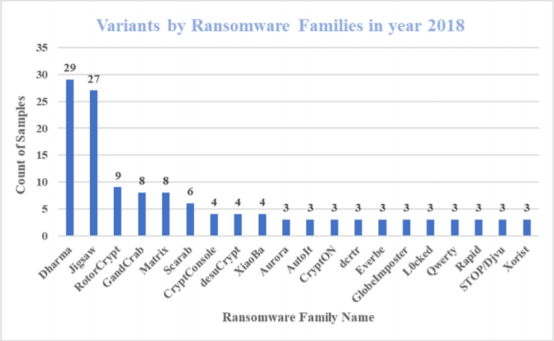


Figure 9. Ransomware Variant with More Than One Extension – 2018

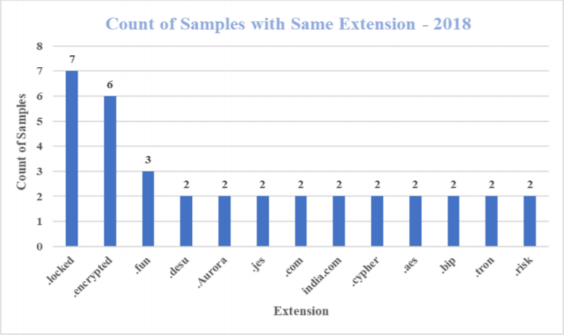


Figure 10. Ransomware Variant with More Than One Extension - 2018

8.2 Same Extension Different Family

Different extensions are likely being used as a unique identifier, but based on the results, it cannot be denied that different ransomware names can be used for the same extension.

Twenty-five different extensions were used by more than one ransomware family constituting a total of 60 ransomware variants for the year 2018, shown in Figure 10. Similar to 2017, '.locked' with seven different ransomware families is the most dominant extension followed by '.encrypted,' 'fun,' 'desu,' and so on.

8.3. Combination of Different Families and Extensions

The Figures 9 and 10 make it evident that there is a wide variety of results among the different ransomware families and extensions. Moreover, Figure 11 displays the overlap of different ransomware names with various extensions and cross connections among them. In the Figure, different ransomware is displayed as 'Circle' and extension are 'Square.' From Figure 11, it can be inferred that for the 'Dharma' cluster, '.tron' and '.bip' extensions are also used by Tron and GusCrypter ransomware family respectively. The depiction raises a doubt whether these families are related to each other, or this is a mere coincidence.

Similarly, the 'Jigsaw' cluster has '.jes' extension also being used by 'BlackRansomwareFireeye' ransomware family. Moreover, 'Jigsaw' family is also seen to be using '.locked' extension which is shared among many other ransomware families. In connection to the '.locked' extension which is used by 'HiddenTear' and 'L0cked' ransomware family along with '.rape' and '.lckd' extensions. So, will it

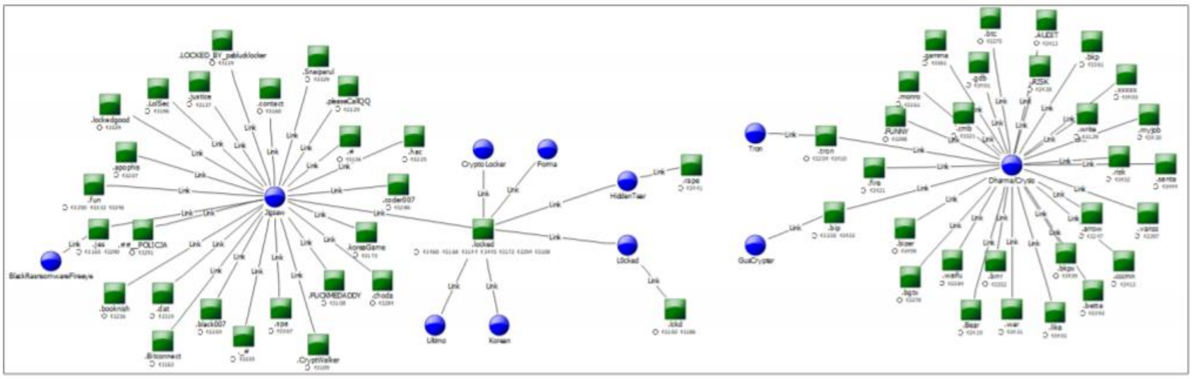


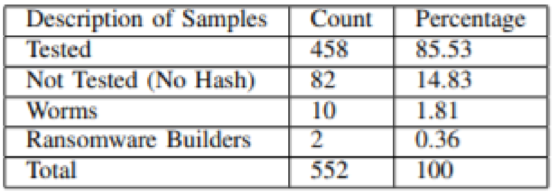
Figure 11. Top Results Combined - 2018

be safe to assume that all of these ransomware family are linked to each other with similar functionalities or created by the same individual.

9. Testing

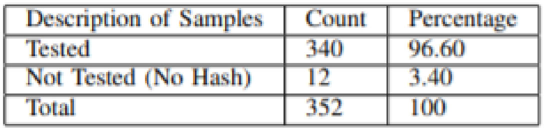
Upon selection, total number of ransomware samples to be analyzed for the year 2017 were 552 as shown in the Table 4, and the testing was conducted in Q3 and Q4 of 2018. Out of the selected variants, unfortunately there was no record of the hashes for 82 of them. Of the remaining, two samples were ransomware builders, and ten samples were Worms, namely SamSam, WannaCry, which are also referred as Locker Ransomware, mentioned in section 6. The risk of analyzing the locker ransomware was that it was known to encrypt the entire organization, so it was quite dangerous to analyze them within the university's network. Finally, 458 ransomware samples were selected for dynamic analysis.

Table 3. Samples Tested - 2017



Description of Samples	Count	Percentage
Tested	458	85.53
Not Tested (No Hash)	82	14.83
Worms	10	1.81
Ransomware Builders	2	0.36
Total	552	100

Table 4. Samples Tested - 2018



Description of Samples	Count	Percentage
Tested	340	96.60
Not Tested (No Hash)	12	3.40
Total	352	100

For the year 2018, 352 ransomware variants were selected for analysis. On purpose, researchers ignored the variants that were worms, ransomware builders, and had no hashes, except for the ones that were duplicates of the other ransomware families.

Finally, 340 ransomware variants were selected for further analysis. After finalizing the ransomware samples to be tested, the next step was to lay out the framework on how to approach these samples to find common attributes to formulate a solution against these ransomware attacks. The steps followed are mentioned below.

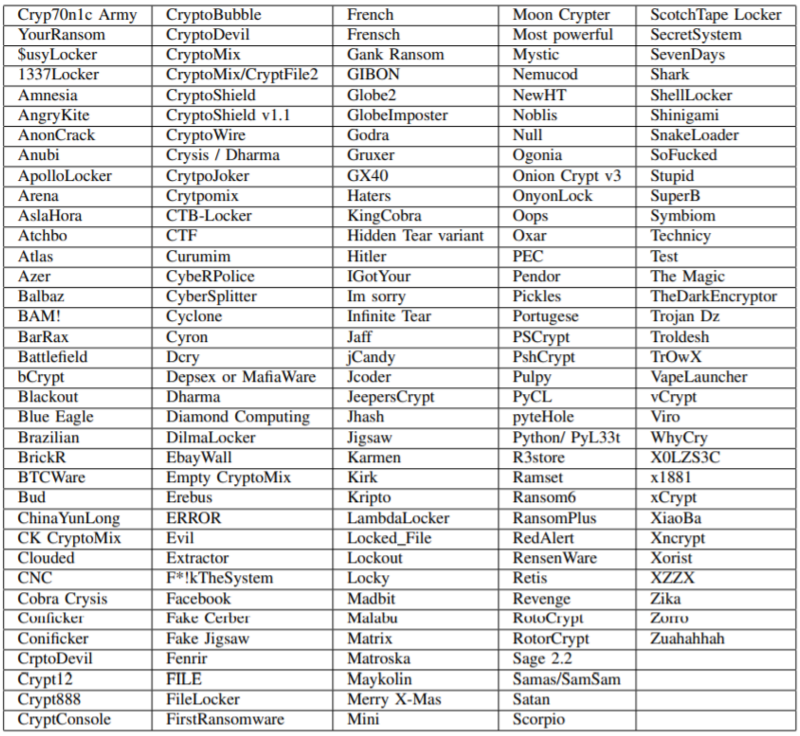
9.1. Download and Static Analysis Check

The ransom ware samples were dowloaded from the Virus Total website [23]. Once the samples are downloaded, it is run through static analysis tools such as PEStudio, PEView for further analysis to find out unique features in the Imports, Directory, Header, or Strings section. The results help determine signatures that can be developed based on the static analysis and get more information from the ransomware binary. The analysis was performed at an overview level, which could be used for some future research, but not in-depth as the ransomware behaved differently after the execution as compared to when performing static analysis.

9.2. Encryption Test

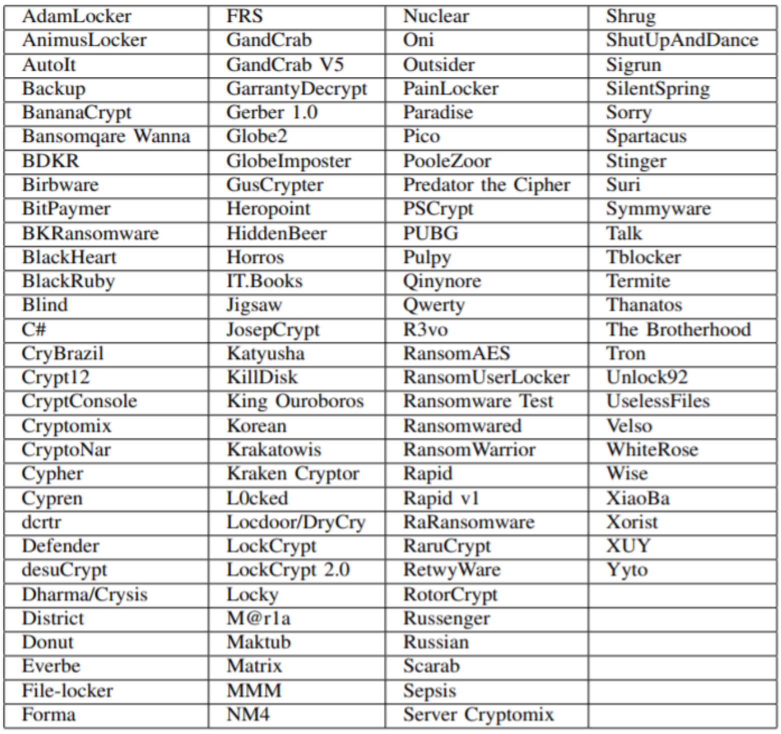
Once the 458 ransomware binaries were downloaded, the next answer needed was that how many ransomware binaries are active even in the year 2018. These samples were being tested on a Microsoft Windows 7 machine in a virtualized environment. Out of all the variants, 53% of the samples were actively encrypting, shown in Figure 12, which is a considerably high percentage and gives a sense that there were not enough preventive measures taken by the industry to stop the execution of these programs. A growing concern that 243 binaries are functioning properly with the complete list in Table 5.

Table 5. Active Ransomware Variants for the year 2017



Cryp70n1c Army	CryptoBubble	French	Moon Crypter	ScotchTape Locker
YourRansom	CryptoDevil	Frensch	Most powerful	SecretSystem
$usyLocker	CryptoMix	Gank Ransom	Mystic	SevenDays
1337Locker	CryptoMix/CryptFile2	GIBON	Nemucod	Shark
Amnesia	CryptoShield	Globe2	NewHT	ShellLocker
AngryKite	CryptoShield v1.1	GlobeImposter	Noblis	Shinigami
AnonCrack	CryptoWire	Godra	Null	SnakeLoader
Anubi	Crysis / Dharma	Gruxer	Ogonia	SoFucked
ApolloLocker	CrytpoJoker	GX40	Onion Crypt v3	Stupid
Arena	Crytpomix	Haters	OnyonLock	SuperB
AslaHora	CTB-Locker	KingCobra	Oops	Symbiom
Atchbo	CTF	Hidden Tear variant	Oxar	Technicy
Atlas	Curumim	Hitler	PEC	Test
Azer	CybeRPolice	IGotYour	Pendor	The Magic
Balbaz	CyberSplitter	Im sorry	Pickles	TheDarkEncryptor
BAM!	Cyclone	Infinite Tear	Portugese	Trojan Dz
BarRax	Cyron	Jaff	PSCrypt	Troldesh
Battlefield	Dcry	jCandy	PshCrypt	TrOwX
bCrypt	Depsex or MafiaWare	Jcoder	Pulpy	VapeLauncher
Blackout	Dharma	JeepersCrypt	PyCL	vCrypt
Blue Eagle	Diamond Computing	Jhash	pyteHole	Viro
Brazilian	DilmaLocker	Jigsaw	Python/ PyL33t	WhyCry
BrickR	EbayWall	Karmen	R3store	X0LZS3C
BTCWare	Empty CryptoMix	Kirk	Ramset	x1881
Bud	Erebus	Kripto	Ransom6	xCrypt
ChinaYunLong	ERROR	LambdaLocker	RansomPlus	XiaoBa
CK CryptoMix	Evil	Locked_File	RedAlert	Xncrypt
Clouded	Extractor	Lockout	RensenWare	Xorist
CNC	F*!kTheSystem	Locky	Retis	XZZX
Cobra Crysis	Facebook	Madbit	Revenge	Zika
Conficker	Fake Cerber	Malabu	RotoCrypt	Zorro
Conificker	Fake Jigsaw	Matrix	RotorCrypt	Zuahahhah
CrptoDevil	Fenrir	Matroska	Sage 2.2	
Crypt12	FILE	Maykolin	Samas/SamSam	
Crypt888	FileLocker	Merry X-Mas	Satan	
CryptConsole	FirstRansomware	Mini	Scorpio	

Table 6. Active Ransomware Variants for the year 2018



AdamLocker	FRS	Nuclear	Shrug
AnimusLocker	GandCrab	Oni	ShutUpAndDance
AutoIt	GandCrab V5	Outsider	Sigrun
Backup	GarrantyDecrypt	PainLocker	SilentSpring
BananaCrypt	Gerber 1.0	Paradise	Sorry
Bansomqare Wanna	Globe2	Pico	Spartacus
BDKR	GlobeImposter	PooleZoor	Stinger
Birbware	GusCrypter	Predator the Cipher	Suri
BitPaymer	Heropoint	PSCrypt	Symmyware
BKRansomware	HiddenBeer	PUBG	Talk
BlackHeart	Horros	Pulpy	Tblocker
BlackRuby	IT.Books	Qinynore	Termite
Blind	Jigsaw	Qwerty	Thanatos
C#	JosepCrypt	R3vo	The Brotherhood
CryBrazil	Katyusha	RansomAES	Tron
Crypt12	KillDisk	RansomUserLocker	Unlock92
CryptConsole	King Ouroboros	Ransomware Test	UselessFiles
Cryptomix	Korean	Ransomwared	Velso
CryptoNar	Krakatowis	RansomWarrior	WhiteRose
Cypher	Kraken Cryptor	Rapid	Wise
Cypren	L0cked	Rapid v1	XiaoBa
dcrtr	Locdoor/DryCry	RaRansomware	Xorist
Defender	LockCrypt	RaruCrypt	XUY
desuCrypt	LockCrypt 2.0	RetwyWare	Yyto
Dharma/Crysis	Locky	RotorCrypt	
District	M@r1a	Russenger	
Donut	Maktub	Russian	
Everbe	Matrix	Scarab	
File-locker	MMM	Sepsis	
Forma	NM4	Server Cryptomix	

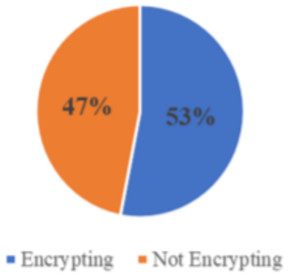


Figure 12. Ransomware Samples 2017

Similarly, for the year 2018, the results obtained for almost identical as 52% of the ransomware samples constituting 176 variants were actively encrypting and capable of infecting the end-users of the 340 tested samples. The Figure 13 displays the relation of the encrypting and non-encrypting for the tested samples for the year 2018. A comprehensive list of all the active variants is shown in Table 6.

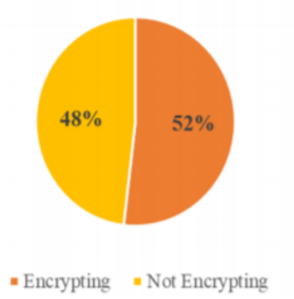


Figure 13. Ransomware Samples 2018

A point to note is that 47% and 48% of the binaries for both the years were inactive and did not perform the desired function of encrypting the files. Following could be the few reasons for the binaries being inactive:

- Command and Control Center could be down
- Old version of the binary
- Aware of being tested in a virtualized environment

A reason to worry is that the active ransomware binaries are from the previous years, making it concerning as the general notion among the industry is that old binaries are not prominent, but in the following paper, we display that old is undoubtedly active and will probably never die. Therefore, the end-users should always be aware of the obsolete as well as new developing ransomware attacks.

10. Preventive Measures and Future Work

Our results show that the current nomenclature of the anti-virus industry preventive measures is not up to the mark. Despite the tested samples being obsolete, the variants were still able to perform the desired function. The active variants are a big sign of worry for the industry as well as the end-users, as ransomware production is growing at a steeper pace, making it necessary for the industry to contribute in information sharing about upcoming ransomware families pro-actively. Also, educational programs should be launched to enlighten the users about the various ransomware attacks. For future work, the researcher will focus on understanding the internal infrastructure of the active variants and trying and find similarities that can help in better clustering, as well as a prediction for the future ransomware attacks.

The contribution of the paper is to bring awareness among the security industry to develop safeguards not only against the new attacks but also for the old ransomware active variants. Also, make the end-user alert about these attacks and to maintain proper active backups (on-site and off-site) to prevent them from these ransomware attacks. To conclude, old binaries never go out of fashion; they can be re-used to haunt the end-user for a long time.

11. References

[1] Phishme, (2016), Malware year in review https://phishme.com/whitepaper/2016-year-in-review (Access Date: 12 January 2020).

[2] McAfee, (2016), Mcafee labs threats report, http://www.mcafee.com/us/resources/repor ts /rp-quarterly-threatsmay-2016.pdf (Access Date: 2 December 2019).

[3] Malwarebytes, Understanding the depth of the global ransomware problem, Aug. 2016. https://www.malwarebytes.com/surveys/ransomware/?aliId=13242065 (Access Date: 14 December 2019).

[4] Crowe, J. (2016), Ransomware by the numbers: Must-know ransomware statistics, https://blog.barkly.com/ransomware-statistics-2016 (Access Date: 16 November 2019).

[5] Bisson, D., (2016), Necurs botnet goes quiet, leads to drop in locky and dridex activity, https://www.tripwire.com/state-of-security/latest-security-news/necursbotnet-goes-quiet-leads-to-drop-in-locky-and-dridex-activity (Access Date: 8 November 2019).

[6] D. of Justice, (2017), “Justice department announces actions to dismantle Kelihos botnet, https://www.justice.gov/opa/pr/justice-departmentan n ounces-actions-dismantle-kelihos-botnet-0 (Access Date: 9 May 2018).

[7] Arora, A., Gannon, M., Warner, G., (2017), Kelihos botnet: A never-ending saga, Annual ADFSL Conference on Digital Forensics, Security and Law. 4.

[8] Gannon, M., Warner, G., Arora, A., (2017), An accidental discovery of IOT botnets and a method for investigating them with a custom lua dissector, Annual ADFSL Conference on Digital Forensics, Security and Law.

[9] Symantec, (2017), Internet security threat report, https://www.symantec.com/content/dam/symantec/docs/securitycenter/white-papers/istr-ransomware-2017-en.pdf (Access Date: 23 June 2018).

[10] Crowe, J., (2017), Musy-know ransomware statistics, https://blog.barkly.com/ransomware-statistics-2017 (Access Date: 23 February 2019).

[11] Bleepingcomputer, (2017), https://www.bleepingcomputer.com (Access Date: 23 August 2019).

[12] Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., and Kirda, E., (2015), Cutting the gordian knot: A look under the hood of ransomware attacks, in International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Springer, pp. 3–24.

[13] Cabaj, K. and Mazurczyk, W. (2016), Using software-defined networking for ransomware mitigation: the case of crypto wall, IEEE Network, vol. 30, no. 6, pp. 14–20.

[14] Silva, S. S, Silva, R. M, Pinto, R. C. and Salles, R. M., (2013), Botnets: A survey, Computer Networks, vol. 57, no. 2, pp. 378–403.

[15] Floser Bacurio, R. D. P., Joven, R., (2016), Locky strike: Smoking the locky ransomware code. Virus Bulletin Conference, https://d3gpjj9d20n0p3.cloudfront.net/fortiguard/research/VB2016-Locky-Paper.pdf (Access Date: 11 June 2018).

[16] Sherr, I., (2017), Wannacry ransomware: Everything you need to know, https://www.cnet.com/news/wannacrywannacrypt-uiwix-ransomware-everything-you-need-to-know (Access Date: 19 January 2019).

[17] Guardian, T., (2017), Briton who stopped wannacry attack arrested over separate malware claims, https://www.theguardian.com/technology/2017/aug/03/researcherwho-stopped-wannacry-ransom waare-detained-in-us (Access Date: 12 December 2019).

[18] Boyd, C. (2018), Samsam ransomware: what you need to know, https://blog.malwarebytes.com/cybercrime/2018/05/samsamransomware-need-know (Access Date: 22 September 2019).

[19] Rashid, F. Y., (2016), Patch jboss now to prevent Samsam ransomware attacks, https://www.infonworld.com/article/3058254/patch-jboss-now-toprevent-samsam-ransomware-attacks.html (Access Date: 2 May 2019).

[20] WIRED, (2018), Atlanta spent 2.6 mtorecover froma52,000 ransomware scare, https://www.wired.com/story/atlanta-spent-26m-recover-fromransomwarre-scare (Access Date: 23 June 2019).

[21] NetStealer, (2017), Encoder builder v2.4-ransomware, http://netstealer.com/489/encoder-builder-v2-4-ransomware (Access Date: 29 June 2019).

[22] Labs, S., (2017), 5 ransomwares as a service (raas) kits, https://nakedsecurity.sophos.com/2017/12/13/5-ransomwareas-a-service-raas-kits-sophoslabs-investigates (Access Date: 2 December 2019).

[23] Virustotal (2018), Virus total, https://www.virustotal.com (Access Date: 4 April 2019).