Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 15 (2020) pp. 107-125
© MIR Labs, www.mirlabs.net/jias/index.html

Windows-based Ransomware: A Survey

Ayesha Naseer
Department of Computer Science
Capital University of Science & Technology
Islamabad 44000, Pakistan
ayesha_naseer1993@hotmail.com

Riffat Mir
Department of Computer Science
Capital University of Science & Technology
Islamabad 44000, Pakistan
riffatmir52@gmail.com

Azmat Mir
Department of Computer Science
Capital University of Science & Technology
Islamabad 44000, Pakistan
azmatmeer5@gmail.com

Muhammad Aleem
Department of Computer Science
National University of Computer and Emerging Sciences, Islamabad
44000, Pakistan
[Corresponding author:
m.aleem@nu.edu.pk]

***Abstract*—Nowadays, ransomware attacks are rapidly being increased across the globe. Ransomware causes loss of the huge amount of user's data and financial loss. Ransomware is malware that encrypts the user's data and makes it inaccessible for the user until and unless the user pays some ransom amount. The existing operating systems fail to provide adequate protection to evade this harmful ransomware. This paper presents a comprehensive analysis of various Windows-based ransomware. Dating back from 1989, when first ransomware was discovered to date, this paper recapitulates attacks, symptoms, types, infection methods, encryption type, and form of ransomware of over 40 Windows-based harmful ransomware. The main purpose of this survey is to provide awareness to window's users how this ransomware can affect their systems and data and how they can prevent their systems.**

Keywords— ***Ransomware, Distribution Method, Encryption, Symptoms, Ransom, Bitcoin.***

I. Introduction

Malware holds great potential to adversely affect the performance of a computer system. Malware is a software specifically designed to harm a computer, user, server, or computer network. Although, all ransomware [76] behaves similarly, however, each of them adopts different destruction methods. Ransomware is a dangerous malware that hijacks a user's system and steals all of his sensitive data. The ransomware then demands a ransom to give access back to the victim [64].

Most of the operating systems like Windows, MAC, and Android [75] fail to secure the data of a user, thus, becoming an easy target for ransomware.

Ransomware is dangerous because it uses unbreakable encryption methods [64]. This paper presents a comprehensive analysis of 40 Windows-based ransomware. More than 80% of the world's population uses Windows-based operating systems. We focus on ransomware that causes damage to a wider community in the form of encrypting the data and demanding a huge amount of ransom. Moreover, certain cascade attacks can be launched too using the victims' social contact information [73] This study will aware of people of different ransomware attacks that can be faced while using windows operating systems.

The notion of discovering ransomware was coined in 1989 [61]. This study enlists attributes of over 40 different types of windows-based ransomware. The attributes include their discovery date, encryption types, distribution method, types of ransomware, etc. i.e. when particular ransomware was discovered? Which countries were targeted by this ransomware? What is the type of ransomware? i.e., Crypto or Locker, what are distribution methods of this ransomware? What are the symptoms, their encryption types, and what type of payment method these ransomware use for receiving the ransom? This survey is helpful for those people who want to get information about ransomware and their behavior so we provide the basic information about the description of different ransomware. This would also be beneficial for the people to adopt some precautionary measures as it provides information that how particular ransomware can affect your system.

The rest of the section is organized as follows: Section II presents the background of some most terrific ransomware. Section II describes the methodology to gather the information of this ransomware. Section IV describes the characteristics and behavior of this ransomware. Section V describes the discussion and conclusion of this study.

II. Background

The first Ransomware PC Cyborg was discovered in 1989 and it targeted the United States of America using a program known as AIDS information introductory Diskette [61]. It targeted the United States and infected over 20,000 disks. In 2005, GPcoder was introduced [61]. The GPcoder targeted Russia and the ransom amount was $100 - $200 [61]. The distribution method used by GPcoder was "drive-by download”.

After 2005, different ransomware DDoS harmed user’s systems to a great extent by exploiting their information and demanding a huge amount for ransom. In 2006, CryZip was discovered that stored the victim’s documents inside a commercial zip library [61]. In 2012, Reveton was discovered and it claims to be from a legitimate law enforcement authority. The main targets of Reveton were stealing user’s passwords of their email address and FTP.

In 2013, the amount of ransomware increased rapidly. CryptorBit spread quickly through spam email and targeted the United States and the ransom demand was $500 [65]. In 2015, a ransomware named Hidden tear was discovered. It employed a strong encryption algorithm i.e. symmetric *Advanced Encryption Standard* (AES), wherein the same key is used to encrypt and decrypt the data. This ransomware affected OS win32/win64bit, Windows XP, Vista/7,8/8.1, and Windows 10.

Most of the ransomware has some characteristics in common such as they perform data encryption like PCCyborg and PGPcoder [2] [3]. Some of them steal the user’s data and corrupts their system. They lock the systems and demand a ransom amount to unlock them. Some masquerades to be from legitimate authorities such as Reveton. It fraudulently claims to be from a legitimate law enforcement authority and prevents users from accessing their infected machine [12]. Some of these ransomware reside in your system even if you pay the ransom amount.

The ransomware gets into the user’s system by fooling them. One example of such ransomware is Ophionlocker [20]. It asks the user to click on a certain area of a website and then takes over the system once the user clicks on it and then it demands a ransom.

III. Methodology

We have analyzed 40 different Windows-based ransomware, their behaviors, architecture, and recapitulated a comparative study in Table 1 and Table 2.

We have collected the information about this ransomware from different research papers and websites. Different ransomware has different encryption techniques and distribution methods.

We have formed their comprehensive analysis and performed some comparisons on them. Most of them share the same behavior and have some characteristics in common.

IV. Ransomware characteristics

Table 1 illustrates details about all the 40 ransomware i.e. about their discovery year, their short description, and notable features they have in common and the countries targeted by them.

There are two types of ransomware: (a) Crypto-ransomware and, (b) Locker-ransomware. The Crypto-ransomware encrypts user’s files and makes them inaccessible to the users [15]. The Locker-ransomware locks the user’s device interface and demands for ransom to unlock the device [15].

Most of the ransomware has almost identical features as shown in Table 1.

Data Encryption means that ransomware encrypts user’s files by using algorithms like Advanced Encryption Standard (AES) so that the users have no longer access to their data. AES is a strong encryption technique that is malicious for the files. Encryption provides confidentiality to data [1] and users have to pay ransom usually in the form of Bitcoins to gain access back.

Data Locking means that ransomware locks the files that are present in the user's computer drive [2] and restrict the victim's access to the files.

Data Deletion means that some ransomware like PGPcoder and CryZip delete user's files [3,4] from their device no matter whether a user pays the ransom or not.

Data Stealing means that some ransomware like Kriptovor steals the user's data from the user's device [5] to threaten them.

Data Decryption means that some ransomware like Synolocker converts the encrypted data back into the form that is understandable by the user [6] i.e., they decrypt the encrypted data.

Ransomware often targets particular countries. In this survey, the most targeted countries from this ransomware are Russia and the United States. Some ransomware generates false notices which means that they masquerade to be from legitimate law enforcement authorities (e.g., Reveton ransomware) or some other authorities.

Some ransomware like Cryptorbit communicates using the C&C server [13] to create a network of infected devices so that they can Distribute Denial-of-Service (DDos) attacks [66]. While some ransomware scrambles the user's records like PCLOCK and Cryptowall in which files are renamed with the intention that users may not be able to recognize them.

PC Cyborg is the first-ever ransomware and was discovered in 1989 [7]. It is a crypto type ransomware and released employing a floppy disk [7]. It targeted the United States and was distributed in 20,000 infected disks labeling them as "AIDS Information Introductory Diskettes" [8].

PGPCoder was discovered in 2005 and encrypted files on the victim's machine [9]. It is a crypto type ransomware and the country targeted by it was Russia. It adopted data encryption and deletion.

CryZip is a crypto type ransomware that was discovered is 2006. It uses a commercial zip library to store files inside a password-protected zip library [10]. It searches for a certain type of file, compresses them, and then password protects the archive [11].

Reveton is a crypto type ransomware discovered in 2012. It fraudulently claims to be from a legitimate law enforcement authority and prevents users from accessing their infected machine [12]. It mainly targeted European countries. It locked the system and steal the user's passwords for FTP, VPN, email, and web browsers.

Cryptorbit is crypto type ransomware introduced in 2013. It works the same as crypto locker ransomware but it is not a variant of it and corrupts the first 212 or 1024 bytes of data [13]. It performs data encryption and then demands a ransom by communicating with the C&C server [14].

DirtyDecrypt is a crypto type ransomware and its discovery year is 2013. It blocks access to victims' computers from about 15 countries [16]. It encrypts the data and creates replicas of its files. It also corrupts the data. It has targeted Europe and United States.

CryptoLocker is a crypto type ransomware and discovered in 2013[69]. It does not encrypt images, videos, and audio files [17]. It encrypts and locks the data and scans the network drives [17].

Kovter is a locker type ransomware and its discovery year is 2013. This works similar to police ransomware scams and shows a fake message for tricking the victim [18]. It steals the data and encrypts the files and makes these files unreadable.

Urausy is a locker type ransomware and its discovery year is 2013. It acts as the Police Virus or FBI virus. It creates false notices seemingly from a police force [19] and locks the computer. It mainly targeted Greece, Norway, and Ireland.

Ophionlocker is a locker type ransomware introduced in 2014. It fools users by forcing them to click on an area of a website. One a user clicks on the area, Ophionlocker gets into his/her machine [20]. It performs data encryption and to search the files to encrypt, it performs a case-sensitive match of the extension [20].

SynoLocker is a crypto type ransomware and its discovery year is 2014. It targets the network storage devices attached to Synology [21]. It performs data encryption and allows data decryption. It disables the user's access to the system. It mainly targeted Taiwan.

Virlock is a crypto type ransomware and its discovery year is 2014. It terminates task manager and other applications such as explorer. It not only encrypts the data but also infects binary files and spreads to the cloud faster [22][74]. It mainly targeted the United States, China, and Australia.

CoinVault is a crypto type ransomware and its discovery year is 2014. It is file-encrypting ransomware and targets all the versions of Windows [23]. It performs data encryption and allows data decryption.

Table 1. List of Windows Based Ransomware with their discovery date, short description, notable features, types, and targeted countries

Sr.	Name	Discovery Date	Short Description	Notable Features			Type	Targeted Countries
1	PC Cyborg	1989	This ransomware was released by means of a floppy disk	Data encryption	Data Locking	Hides all directories	Crypto	United States
2	PGPcoder	2005	Encrypts files on the victim's machine	Data encryption	Data deletion	Files decryption	Crypto	Russia
3	CryZip	2006	Stores user's data inside a password-protected zip library	Data encryption	Data deletion	Creates password-protected ZIP files	Crypto	-
4	Reveton	2012	Claims to be from a legitimate law enforcement authority	Data encryption	Locks the PC	Steals passwords for FTP, VPN, email, web browsers	Crypto	European Countries
5	Cryptorbit	2013	This works similar to crypto locker virus	Data encryption	Corrupts data	Communicates with C&C server	Crypto	-
6	DirtyDecrypt	2013	It blocks access to victims' computers from about 15 countries	Data encryption	Creates replicas of its files	Corrupts data	Crypto	Europe and United States
7	CryptoLocker	2013	Doesn't encrypt image, video, audio files	Data encryption	Data locking	Scans network drives	Crypto	-
8	Kovter	2013	Works same as police ransomware scam	Data encryption	Data-stealing	Files become unreadable	Locker	-
9	Urausy	2013	Commonly known as the Police Virus or FBI virus	Creates false notices	Locks the PC	Communication done by using HTTP	Locker	Greece, Norway and Ireland
10	OphionLocker	2014	Fools users by forcing them to click on an area of a website that gets into their machine	Data encryption	Does not deletes the files	Performs case-sensitive match	Locker	-

11	SynoLocker	2014	Targets the network storage devices attached to Synology	Data encryption	Disable access to system	Data decryption	Crypto	Taiwan
12	Virlock	2014	Terminates task manager and other applications such as explorer	Data encryption	Infects binary files	Spreads to the cloud faster	Crypto	United States, China, Australia
13	CoinVault	2014	File encrypting ransomware and targets all the versions of Windows	Data encryption	Data deletion	Data decryption	Crypto	-
14	CryptoWall	2014	Makes the files inaccessible and hard to recover for the user	Data encryption	Scrambles file names	Data deletion	Crypto	United Stated and Canada
15	Decryptor Max	-	Once, attack victim’s device it’ll create randomly named executable file	Data encryption	Creates ransom executable files	Data deletion	Crypto	-
16	Kriptovor	2015	Purpose to target those companies which is located in Russia	Data encryption	Data stealing	Terminates if stealing is not successful	Crypto	Russia
17	Hidden Tear	2015	First open-source ransomware and cannot be detectable by antivirus software	Data encryption	Used by cybercriminals	Open-source	Crypto	Turkey
18	Vault Crypt	2015	Encrypt file by adding the extension. Vault	Data encryption	Steals web credentials	Data deletion	Crypto	Russia
19	PCLOCK	2015	Ransomware produces any fake alert to delete the anti-virus that was installed in the user’s system, and save itself	Data encryption	Scrambles records	Targets more than 2583 extensions	Crypto	-
20	Alpha Crypt	2015	The purpose is to scan all available drives	Data encryption	Data Locking	Data deletion	Crypto	-
21	Threat Finder	2015	Installed into the system by fake downloads	Data encryption	Scrambles documents	Data decryption	Crypto	Texas
22	Troldesh	2015	Uses extension XTBL at	Data encryption	Data locking	Data decryption	Crypto	Russia

			the end of encrypted files					
23	Hydra Crypt	2016	Encrypts the file by using extension hydra_crypt_ID_[8 random characters]	Data encryption	Data deletion	Encrypts using C&C server	Crypto	Switzerland
24	Radamant	-	Encrypts the victim's file and add the extension. RDM at the end of file	Data encryption	Data deletion	Encrypts using C&C server	Crypto	-
25	NanoLocker	2016	Corrupts valuable files and encrypts victim's file	Corrupts files	Data Locking	Encrypts using C&C server	Crypto	-
26	TeslaCrypt	2016	It tries to infect typical gaming files	Encrypts game files	Does not encrypts files larger than 268MB	Infects user profiles	Crypto	-
27	8lock8	2015	It encrypts the victim files and adds the extension .8lock8.	Data encryption	Targets only specific files	Encrypts using C&C server	Crypto	Russia
28	Jigsaw	2016	It encrypts 226 different file types	Data encryption	Data deletion	Performs data deletion on a timer	Crypto	Germany, Turkey, Spain, Korea
29	OMG	-	Pops up a decryption program to regain files.	Data encryption	Data Locking	Data decryption	Crypto	-
30	Poshcoder	2014	Uses the Windows PowerShell to encrypt the files	Data encryption	Data deletion	Data decryption	Crypto	United States
31	KeyHolder	-	Encrypts all the files with the XOR cipher and uses CFB mode	Data encryption	Uses XOR cipher	Makes data decryption risky	Crypto	-
32	Cerber	2016	Cannot be stopped by unplugging your PC	Data encryption	Causes the victim's computer to speak	Data decryption	Crypto	Russia

33	JobCrypter	2016	Used to target computer users in France	Data encryption	Data Locking	Scrambles documents	Crypto	France
34	Sage	2016	Doubles the ransom amount after 7 days	Data encryption	Data deletion	Data decryption	Crypto	-
35	Apocalypse	2016	Encrypts the victim’s file and changes extensions of encrypted files	Data encryption	Locks the PC	Falsifies the timestamp of the files	Crypto	-
36	Paycrypt	2016	Enters into victim’s machine as PDF files	Data encryption	Blocks access to websites	Data Locking	Crypto	-
37	7ev3n	2016	Modifies a variety of setting and disables system’s recovery	Data encryption	Modifies PC settings	Blocks security websites	Crypto	-
38	CryptoHas You	2016	Its encryption process makes the ransomware more vigilant	Data encryption	Data Locking	Blocks the browser	Crypto	-
39	Xorist	2016	Encrypts user’s files by adding a custom file extension	Data encryption	Data Locking	Data decryption	Crypto	-
40	777	-	It scans the device and targets specific files and folders	Data encryption	Data Locking	Data decryption	Crypto	-

Crypto wall is a crypto type ransomware discovered in 2014. It spreads through spam emails [70]. The purpose of Cryptowall is to disable the security system on targeted systems [24]. It performs data encryption and deletion. It targeted the United States and Canada.

Decryptor Max is a crypto type ransomware. When the ransomware attacks, the system's wallpaper turns into red. This ransomware attacks all the versions of windows and gives the duration of 7days to the victim for payment [25].

Kriptovor is a crypto type ransomware that was discovered in 2015 [26]. It is the derivation of two words. Kripto means, "steal" and vor means "thief". It spreads through emails. This ransomware attacked businesses in Russia and other international companies. The purpose of Kriptovor is to scan the victim's computer and to target documents, pictures, and explore that file which contains login or password information [27].

The hidden tear is a crypto type ransomware discovered in 2015. The hidden tear claims that it is undetectable by antivirus software and performs data encryption [29]. It mostly targets Turkey.

Vault crypt is a crypto type ransomware and its discovery year is 2015 [28]. The purpose of this ransomware is to encrypt files from your system and enter to your system by adding ". vault" at the end of every file [28].

PC lock is a crypto type ransomware and its discovery year is 2015 [24]. The ransomware gets download into the system through spam emails. It locks the data with a strong encryption algorithm. This ransomware is very difficult to detect without a good antivirus [40].

Alpha Crypt is a crypto type ransomware and its discovery year is 2015 [31][71]. This ransomware targets all the versions of the Windows operating system. Its main purpose is to scan all available drives; network media drop box mapping by creating an executable file named %AppData% [32].

Thread finder is a crypto type ransomware and discovered in 2015. It gets into the system through fake downloads. It performs data encryption, decryption, and scrambles the documents. It mostly targets Texas.

Troldesh is a crypto type ransomware and its discovery year is 2015. Troldesh is known as Encoder .858 mostly targeted Russia [34]. This ransomware spreads through email attachment links. It uses extension XTBL at the end of encrypted files [33].

Hydra Crypt is a crypto type ransomware and its discovery year is 2016. The purpose is to encrypt the file by using extension hydra_crypt_ID_ [i.e., 8 random characters] [35]. It performs data encryption. It mostly targeted Switzerland.

Radamant ransomware is a crypto type ransomware that attacks a victim's file. The purpose of this ransomware is to encrypt the victim's file by adding. RDM extension at the end of the file.

Nano locker is a crypto type ransomware and discovered in 2016. It corrupts the files and encrypts the victim's file by adding. nano extension [62]. It also performs data locking.

Teslacrypt is a crypto type ransomware and its discovery year is 2016. It is equipped with self-deleting features and removes malicious executable files from victim's machines [68]. After encryption, it demands from the victim to pay a ransom amount for decryption. This ransomware does not attack those files whose size is more than 256MBS [38].

8lock8 is a crypto type ransomware and discovered in August 2015. After encrypting the victim's files, it displays a ransom note to retrieve the infected files. [41] [42]. It performs data encryption and mostly targets Russia.

Jigsaw is a crypto type ransomware and its discovery year is 2016. It encrypts computer files and deletes the files if the user does not pay the ransom to decrypt them. It mainly targets Germany, France, Turkey, Spain, and Korea [43].

OMG is a crypto type ransomware. After the infection, the. OMG pops up a decryption program that shows that the user can regain access to its lost files but it does not happen and the attacker gets access to all the victim's files and emails [44].

Poshcoder is a crypto type ransomware discovered in 2014. It uses the English language to display a ransom note. After execution, it adds registry entries to encrypt files and then change the name of the files as {filename}. POSHCODER. It uses a Windows power shell to encrypt the victim's files. It mainly targets users of the United States [45].

The keyholder is a crypto type ransomware. It uses CFB mode and encrypts files with XOR cipher. After encryption, it sends a ransom note in which the information about the access of malware TOR site is available. This site contains information about the ransom payment and the bitcoin address to send the ransom amount in which the ransom should be paid [46].

Cerber is a crypto type ransomware and its discovery year is 2016 [70]. It deletes the shadow volume copies of the targeted machine [47] [48]. It performs data encryption. and mostly targeted the Russian region.

JobCrypter is a crypto type ransomware discovered in2016. It mainly targets users of France and French banks. This ransomware locks the victim's files and also tracks users' activities and collect their major data. It can perform encryption only when it gets connected to the internet [49].

Sage is a crypto type ransomware introduced in 2016. It displays a ransom note in multiple languages. If the victim does not pay the ransom within 7 days, the ransom amount becomes double. [50] [51].

Apocalypse is a crypto type ransomware discovered in 2016. It is file-encrypting ransomware and attacks those systems that have a weak password vector. It encrypts the victim's data and then adds .encrypted extension to it. This ransomware creates a window that displays a ransom message [52].

Paycrypt is a crypto type ransomware and its discovery year is 2016. It encrypts the victim's data and demands for a ransom payment. It enters into the victim's machine as PDF files, Microsoft Office document, and image files rather than showing its actual format that is executable. (EXE) file [53].

7ev3n is a crypto type ransomware discovered in 2016. This is one of the renowned ransomware because it demands a huge ransom amount. It changes various system settings and disables the system's recovery options and keyboard keys. It also blocks access to security websites [54].

CryptoHas You is a crypto type ransomware and its discovery year is 2016. It encrypts the user's data and pretends to be a helpful assistant asking for 300$ in the first 3 days and 150$ each day after the deadline [55].

Xorist is a crypto type ransomware and its discovery year is 2016. It locks the victim's machine, displays a ransom note to the user, and asks the victim to send an ID through SMS. Once the victim follows the attacker's instructions, the attacker sends a code via SMS and starts the decryption process. It causes permanent data loss. [56].

Table 2 describes the following attributes/parameters of the ransomware, which are encryption type, distribution method symptoms, modes of payment, and ransom amount.

Encryption Type is a method used by different ransomware to convert the user's data into a code. Ransomware uses different encryption techniques/algorithms to convert the data. Some of these algorithms are explained below:

- Symmetric Cryptography is an encryption algorithm, which uses the same key for both encryption and decryption of data [24];
- Cryptography Encryption keeps the user's data confidential and does not disclose it until the user pays the ransom;
- RSA 2048 is a strong encryption algorithm that is malicious for the files.
- AES stands for Advanced Encryption Standard (AES) which is an asymmetric encryption algorithm. It uses the same key for both the encryption and decryption of data [25].

Open Source Crypto++ Elliptical Cryptography is an open-source and free class library of C++. Cryptography algorithms use this library for encryption.

The distribution method is a method used by different ransomware for getting into the user's computer. These methods are shown below:

A drive-by download is a method through which a user unintentionally downloads computer software without understanding its consequences.

Online advertising campaigns is a method through which a user clicks on an ad and unintentionally downloads ransomware in his computer.

Some ransomware gets downloaded from the torrent network when you use them for downloading any software.

Cybercriminals use exploit kits to distribute malware into the user's machines. They use them to exploit the vulnerabilities of the user's machine.

Symptoms describe what happens to the user's computer when ransomware infects it. What type of indications this do ransomware leave for the users about their infected computer?

A mode of Payment is a way through which the user pays the ransom amount that is usually in the form of Bitcoin but different other modes are also used [68].

Bitcoin is a form of electronic cash or digital currency through which a user sends an amount to other users [68].

Ransom Amount is the amount, which the users pay to get access back to their systems. This amount varies for different ransomware. It means that it uses the same key for both encrypting and decrypting of data [24]. This ransomware gets into the user's machine through disk known as AIDS information introductory diskette [2][72]. It demands a ransom amount of $189 and the user pays it through post [2].

PGPcoder uses the same symmetric cryptography encryption technique as PC Cyborg [3]. This ransomware gets into the user's machine through a drive-by download method. It demands a ransom amount of $100 to $200 and the user pays it to an E-gold or Liberty Reserve account [3].

CryZip stores the user's data inside a password protected zip file [4]. Once this ransomware gets into the user's machine, it creates _CRYPT_.ZIP extension of all the files. It demands a ransom amount of $300 which the user pays in the form of bitcoins.

Reveton gets into the user's machine when the user downloads some music files. It then infects the machine and removes the original files by removing their entries from MFT (Master File Table) [68]. This ransomware demands a ransom amount of $300USD that the user pays in the form of bitcoins [12].

Cryptorbit uses the cryptography encryption technique for encrypting the data. Cryptography encryption keeps the user's data confidential and does not disclose it until the user pays the ransom. This ransomware gets into the machine through spam email and after that, it creates howdecrypt.gif file extension of all the files. It demands a ransom amount of $400 that is in the form of bitcoins [13].

DirtyDecrypt gets into the machine through unsecured websites or by downloading unknown software. It demands a ransom amount of $300 to $1000. It uses Ukash, Paysafecard, or MoneyPak as a mode of payment [16].

PC Cyborg uses symmetric cryptography for CryptoLocker uses RSA 2048 and AES encryption for encrypting the data. RSA 2048 is strong encryption that is malicious for the files [69]. AES stands for Advanced Encryption Standard and it is a symmetric encryption algorithm, which means that it uses the same key to encrypt and decrypt the data [25]. This ransomware gets into the machine through infected email attachments. It demands a ransom amount of $300 that is in the form of bitcoin.

Kovter gets into the machine through spam email and locks the device. It then demands a ransom amount of $300 in the form of bitcoin.

Urausy gets into the machine through fake updates and email attachments. Once it gets into the machine, it restricts access of a user and displays a message demanding a ransom amount to be paid through MoneyPak, Ukash or Paysafecard.

OphionLocker uses open-source crypto++ elliptical cryptography encryption technique. Crypto++ is an open-source and free class library of C++. Cryptography algorithms use this library for encryption. This ransomware gets into the machine through online advertising campaigns and then locks the machine. It demands a ransom amount of 1 bitcoin.

Synolocker uses RSA 2048 and AES encryption techniques to encrypt the data. A system gets infected when the user runs/installs a malicious executable. This ransomware infects those users who use port 5000 and 5001 on the internet. It demands a ransom amount of 6BTC or $350USD and the payment is usually in the form of bitcoins.

Virlock uses RSA 2048 encryption techniques to encrypt the data. This ransomware gets into the machine through cloud storage. It infects the user's images, documents, and binary files and demands a ransom amount of $250 to be paid in the form of bitcoins.

Table 2. List of Windows Based Ransomware with their encryption type, distribution method, symptoms, modes of payment and the ransom amount

Sr.	Name	Encryption Type	Distribution Method	Symptoms	Modes of Payment	Ransom Amount
1	PC Cyborg	Symmetric Cryptography	Through DISK also known as AIDS information introductory Diskette	-	Through post	$189
2	PGPcoder	Symmetric Encryption	Drive-by download	-	E-gold or Liberty Reserve	$100-$200
3	CryZip	Creates password-protected ZIP files	-	Files are found with _CRYPT_.ZIP extension	Bitcoin	$300
4	Reveton	-	Downloading Music Or Files	-	MoneyPak	$300USD
5	Cryptorbit	Cryptography Encryption	Spam email	Generates howdecrypt.gif file in the device	Bitcoin	$400
6	DirtyDecrypt	-	Visiting unsafe websites, downloading unknown software	-	Ukash, PaySafeCard or MoneyPak	$300 to $1000
7	CryptoLocker	RSA 2048, AES	Propagated via infected email attachments	-	Bitcoin	$300
8	Kovter	-	Spam email	Locks the device	Bitcoin	$300
9	Urausy	-	Fake updates, Email attachments	You can't access your PC, and instead, see an image demanding ransom	MoneyPak, Ukash or Paysafecard	-
10	OphionLocker	Open source Crypto+++ Elliptical Cryptography	Online advertising campaigns	Ransom malware infects the machines and locks down access to the machine	Bitcoin	1BTC
11	SynoLocker	RSA 2048, AES	Spreads via exploits	Infects port 5000 and 5001on the internet	Bitcoin	6BTC or $350USD
12	Virlock	RSA-2048	Via cloud storage & collaboration apps	Infects images, documents and binary files	Bitcoin	$250
13	CoinVault	AES-256	Spam email	-	Bitcoin	0.7BTC
14	CryptoWall	AES , RSA 2048	Spam campaigns, malvertising, Exploit Kits	Files become inaccessible	Bitcoin	$200 to $10,000
15	Decryptor Max	AES-265 and RSA	Spam Email compromised website	The infected device will display a red	Bitcoin	-

				wallpaper		
16	Kriptovor	Open source Delphi library called LockBox 3	Spam email	Files become inaccessible	Bitcoin	-
17	Hidden Tear	-	-	Files are found with. locked extension	Bitcoin	$500 and $1500
18	Vault Crypt	Gnupg encryption tool, RSA-2048	Spam email	Files become inaccessible	Bitcoin	-
19	PCLOCK	RC4 Algorithm	Torrent network	-	Bitcoin	0.55BTC or $570
20	Alpha Crypt	RSA-2048	Spam email, angler exploit kit	Sensitive files become inaccessible	Bitcoin	$500USD
21	Threat Finder	RSA 2048	Spam email, angler exploit kit, fake downloads	Random Pop-Ups	Bitcoin	1.25BTC
22	Troldesh	AES256	Via emails and using exploit kit	Files become inaccessible	Bitcoin	0.5 – 1.5BTC
23	Hydra Crypt	AES-265 and RSA	Spam email, fake downloads	Dump of encrypted files on the desktop of the affected computer	Bitcoin	0.5 – 1.5BTC
24	Radamant	AES 256	Spam Email compromised website	Unwanted Pop-Ups	Bitcoin	$230.88USD
25	NanoLocker	AES	Spam Emails, Email Attachments	Important files are locked and renamed with. Nano extension	Bitcoin	0.10BTC or 43USD
26	TeslaCrypt	-	Adobe Flash exploit, Email	Files become inaccessible	Bitcoin	$500
27	8lock8	AES 256	Spam Email attachment, fake URLs	Some files become inaccessible, the extension of the encrypted files will be changed	Bitcoin	-
28	Jigsaw	-	Spam email	Files are found with. FUN, .BTC, .KKK extension	Bitcoin	$150
29	OMG	RSA1024	Via spam emails, malvertising techniques	All the files are found with an. OMG extension	Bitcoin	-
30	Poshcoder	AES & RSA 4096 Key exchange	Via emails	Some of the files become inaccessible	Bitcoin	1BTC

31	KeyHolder	An immensely strong RSA-2048 encryption algorithm	Spam Emails, Email Attachments, File Sharing Networks	Files become inaccessible	Bitcoin	1.5BTC
32	Cerber	AES 256	Trojan Horse, Email attachment	Changes the desktop background	Bitcoin	$499
33	JobCrypter	RSA 2048	Via spam email attachments containing ZIP files	The victim's documents, images and videos not larger than 20 megabytes are encrypted	PaySafeCard	300Euros
34	Sage	-	Pandex spamming botnet, the Trik botnet, and the RIG exploit kit	-	Bitcoin	$2000
35	Apocalypse	RSA encryption	Spam email	Some files become inaccessible	Bitcoin	-
36	Paycrypt	-	Via malicious Files, exploit kits and compromised URL's	The victim may witness the wallpaper changed	Bitcoin	-
37	7ev3n	-	Spam mail, Fake downloads	Some files become inaccessible	Bitcoin	13BTC
38	CryptoHas You	AES (256), RSA(2046)	E-mail, Third-party freeware, Pirated programs	Some files cannot be opened	Bitcoin	$300USD
39	Xorist	XOR or TEA encryption	Via malicious URLs or file attachments	Files being encoded with a ransom message	Bitcoin	0.3 to 2BTC
40	777	-	Spam Email with an infected attachment	System' performance is reduced	Bitcoin	$500 or $1500

` CoinVault uses AES 256 encryption technique to encrypt the user's data placed on the machine. AES 256 is a strong encryption technique that is malicious for the files. This ransomware gets into the machine through spam emails and demands a ransom amount of 0.7 bitcoins.

Cryptowall ransomware spreads through emails, malicious PFD files, and many other exploit kits. When a system gets attacked by Cryptowall, the user can no longer access the files. Attackers demand ransom to be paid in the form of Bitcoins.

Decryptor Max ransomware spreads through spam emails or when a user clicks on any compromised web site. This ransomware uses AES-265 and RSA encryption algorithms.

Kriptovor ransomware spreads through spam emails and makes files inaccessible to the user. The user gains access back only when the ransom amount is paid [38].

Hidden tear uses the AES algorithm for encryption [29]. The basis of this encryption is on this ransomware's source code [39].

Vault crypt uses RSA-2048 for encryption. The ransomware spreads through emails. When it gets into the system, it demands payment from the victim to get back all the files and data.

PCLOCK encrypts a file using the most powerful algorithm RSA and demands from a victim an amount of 0.5BTC for decryption. This ransomware encrypts all files and displays a deadline message on wallpaper [30].

Alpha crypt uses the AES algorithm for encryption [32]. The starting amount of Alpha crypt ransomware is $500 and the user pays the amount in the form of Bitcoin [57].

Threadfinder ransomware uses RSA 2048 algorithm for encryption and spreads through fake downloads and angler exploit kit. It also gets into the system through random popups.

Troldesh ransomware uses AES 256 algorithm and spreads through emails. It makes the files inaccessible to a user until some ransom amount is paid in the form of Bitcoin.

Hydra crypt ransomware performs encryption using the RSA-2048 key (AES CBC 256-bit encryption algorithm). After encryption, it displays a message on the user's screen that offers to decrypt the file within 72 hours by paying a ransom amount in the form of Bitcoin. If a user does not pay the ransom, it destroys the victim's private key and files remain encrypted forever [36].

Radamant uses the AES-256 algorithm for encryption. After encryption, it displays a message for decryption and payment details on the website. The ransomware payment is .5 Bitcoin, which is equal to $230.88 USD [37].

Nano locker ransomware is a cryptovirus, which spreads through spam emails and email attachments [58].

The Teslacrypt is a Trojan horse that spreads through adobe flash exploits and spam emails. After this, the attacked user will have no longer access to their files. A user can only access the files by paying the ransom in the form of Bitcoin.

8lock8 uses the AES-256 algorithm to encrypt the victim's data and add the extension .8lock8 at the end of the files. This ransomware spreads through spam email attachment, peer-to-peer (P2P) networks and fake URLs [41] [42].

Jigsaw spreads through malicious attachments in spam emails. This ransomware uses AES cipher to encrypt the victim's data and then demands a ransom for decryption [42]. Jigsaw locks and encrypts them with. booknish, pay, jes. This ransomware not only exponentially increases the ransom amount as time passes by, but also deletes victim's files permanently, and increases the number of files that cannot be recovered [68].

OMG ransomware spreads through spam email and some malvertising techniques. It adds an extension .OMG at the end of files.

Poshcoder uses AES and RSA 4096 keys to encrypt the files. Once it encrypts the files on the victim's machine, it displays a message that contains certain instructions in the form of a ransom note [45].

Keyholder uses a strong RSA-2048 encryption algorithm. It encrypts files and becomes inaccessible. It spreads through spam emails, file sharing networks, and file attachments. A ransom note shows the instructions for paying the ransom amount of 500$.

Cerber uses the RSA-2048 key to encrypt the victim's data. It spreads through magnitude exploit kit; spam campaigns and RIG exploit kit. Cerber incorporate some delays of few minutes to even a few days between their encryption trial in order to avoid detection [68]. It changes the desktop background and demands to pay a ransom amount of $499 in the form of Bitcoin.

JobCrypter uses RSA 2048 algorithm to encrypt the victim's data. It spreads via spam email attachments containing ZIP files. It encrypts the victim's documents, images, and videos that are no longer than 20 megabytes. It demands ransom in 300 Euros and the user uses Paysafecard to pay the ransom amount and displays the ransom note in the French language [67].

Sage uses RSA 4096 public key to encrypt the victim's file by adding .sage file extension at the end of the files. It spreads via pandex spamming botnet, the trik botnet, and the RIG exploit kit. It demands a ransom amount of $2000 to be paid in the form of Bitcoin [50] [51].

Apocalypse uses the RSA encryption technique to encrypt a victim's data. It spreads through spam email and software updates. It shows ransom message in text files about the encrypted files, provides some email addresses to contact the attackers. It also tells how to pay the ransom amount. It locks the system and displays a ransom note [52].

PayCrypt infects the victim's machine via malicious files, exploit kits, malicious URLs, PDF files, and image files rather than showing its actual format that is executable (EXE) file. The user may observe the wallpaper changes that show the instructions of how to recover the files by paying the ransom in monetary mode [53].

7ev3n spreads through spam mail and fake downloads. After encryption, some files become inaccessible. It demands a ransom in the form of Bitcoin that is 13BTC, which is the highest ransom payment.

CryptoHasYou uses 256-RSA to encrypt the victim's data. Encryption disorganizes the contents of a file to make it unclear. It spreads through malicious URLs, third-party freeware, and supporting payload executables. This ransomware locks some files. It demands a ransom of $300USD in the form of bitcoins [55].

Xorist uses XOR or TEA encryption technique. It spreads through malicious URLs or file attachments. It shows a ransom message of data encryption. After encrypting the files, this ransomware creates a 'How to Decrypt Files.txt' text file on the victim's desktop. This file contains the phone number to contact the criminals. It demands a ransom payment of 0.3 to 2BTC [56].

V. Discussions and Conclusion

This study presents a comprehensive analysis of over 40 Windows-based ransomware. All of the ransomware have different attributes and follow their behavior of infecting the system. All of them have varying intensity affecting the user's files. Some of them demand ransom to give access back to the victim while others permanently destroy the user's files. We have done an analysis of 40 windows based ransomware based on their types and other particular parameters. The prime purpose of this study is to provide Windows users an insight that how they can be aware of this ransomware and what kind of harm this ransomware can provide to them. From this study, we have found that TeslaCrypt and Locky are the most harmful ransomware. Here are some of the precautions on how to protect your files from Locky ransomware. Use internet security that helps you avoid fake emails and spam. Use an up to date antivirus. Make sure to disable Microsoft Office macros by default. Back important files up, either online or on external drives. Do not open suspicious emails or attachments from unreliable sources. To confirm your operating system is updated and patched.

VI. References

[1] "Welivesecurity",Available:"https://www.welivesecurity.com/2016/09/13/how-encryption-molded-crypto-ransomware/", [Accessed online: Jan 2020].

[2] "KnowBe4",Available:"https://www.knowbe4.com/aids-trojan", [Accessed online: Jan 2020].

[3] "Wikipedia",Available:"https://en.wikipedia.org/wiki/PGPCoder", [Accessed online: Jan 2020].

[4] "Secureworks",Available:"https://www.secureworks.com/research/cryzip", [Accessed online: Jan 2020].

[5] "VinRansomware",Available:"http://www.vinransomware.com/index.php?option=com_content&view=article&id=33", [Accessed online: Jan 2020].

[6] "VinRansomware",Available:"http://www.vinransomware.com/index.php?option=com_content&view=article&id=91", [Accessed online: Jan 2020].

[7] "KnowBe4",Available:"https://www.knowbe4.com/aids-trojan", [Accessed online: Jan 2020].

[8] "VinRansomware",Available:"http://www.vinransomware.com/pc-cyborg-ransomware", [Accessed online: Jan 2020].

[9] “Wikipedia”,Available:“https://en.wikipedia.org/wiki/PGPCoder”, [Accessed online: Jan 2020].

[10] “Secureworks”,Available:”https://www.secureworks.com/research/cryzip”, [Accessed online: Jan 2020].

[11] “McAfee”,Available:”https://home.mcafee.com/virusinfo/virusprofile.aspx?key=138886#none”, [Accessed online: Jan 2020].

[12] “F-Secure”,Available:”https://www.f-secure.com/v-descs/trojan_w32_reveton.shtml”, [Accessed online: Jan 2020].

[13] “KnowBe4”,Available:“https://www.knowbe4.com/cryptorbit-ransomware, [Accessed online: Jan 2020].

[14] “VinRansomware”,Available:”http://www.vinransomware.com/index.php?option=com_content&view=article&id=79”, [Accessed online: Jan 2020].

[15] “VinRansomware”,Available:”http://www.vinransomware.com/types-of-ransomware”, [Accessed online: Jan 2020].

[16] “VIRUSES”,Available:”https://www.2viruses.com/remove-dirtydecrypt-ransomware”, [Accessed online: Jan 2020].

[17] “VinRansomware”,Available:”http://www.vinransomware.com/index.php?option=com_content&view=article&id=77”, [Accessed online: Jan 2020].

[18] “VinRansomware”,Available:”http://www.vinransomware.com/kovter-ransomware”, [Accessed online: Jan 2020].

[19] “VinRansomware”,Available:”http://www.vinransomware.com/urausy-police-ransomware”,[Accessed online: Jan 2020].

[20] “VinRansomware”,Available:”http://www.vinransomware.com/ophionlocker-ransomware”,[Accessed online: Jan 2020].

[21] ”VinRansomware”,Available:”http://www.vinransomware.com/index.php?option=com_content&view=article&id=91”,[Accessed online: Jan 2020].

[22] “KnowBe4”,Available:“https://www.knowbe4.com/virlock-ransomware”, [Accessed online: Jan 2020].

[23] “BleepingComputer”,Available:“https://www.bleepingcomputer.com/virus-removal/coinvault-ransomware-information”, [Accessed online: Jan 2020].

[24] “IBM”,Available:“https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.14/gtps7/s7symm.html”, [Accessed online: Jan 2020].

[25] M.Pitchaiah, Philemon Daniel, Praveen, “Implementation of Advanced Encryption Standard Algorithm”, In International Journal of Scientific & Engineering Research, March 2012.

[26] ”Vinransomware”,Available:”http://www.vinransomware.com/decryptor-max-ransomware“,[Accessed online: 27-Dec-2018].

[27] “ISTR special Report: Ransomware and business 2016”,Available:”https://conferences.law.stanford.edu/cyberday/wp-content/uploads/sites/10/2016/10/5c_ISTR2016_Ransomware_and_Businesses.pdf”, [Accessed online: Jan 2020].

[28] ”EnigmaSoft”,Available:”https://www.enigmasoftware.com/kriptovorransomware-removal/”, [Accessed online: Jan 2020]

[29] ”Giraffe connected solution”, Available:”http://www.giraffesolutions.co.uk/vault-crypt-a-new-type-of-ransomware/” [Accessed online: Jan 2020]

[30] Daniel Kim, “Analysis of Hidden Tear. An Open Source Ransomware-like Crypter Kit”, December 15, 2015

[31] ”Sensors Tech Forum”, Available: ”https://sensorstechforum.com/remove-pclock-cryptolocker-ransomware-decrypt-encrypted-files/”,[Accessed online: Jan 2020]

[32] ”Bleepingcomputer”,Available:”https://www.bleepingcomputer.com/virus-removal/teslacrypt-alphacrypt-ransomware-information”,[Accessed online: Jan 2020].

[33] ”NJCCIC NJ CYBERSECURITY AND COMMUNICATION INTEGRATION CELL”,available”https://static1.squarespace.com/static/555b2d4ee4b011aa38092227/t/58b452d1cd0f68b719c6ef70/1488212697132/NJCCIC+%E2%80%93+Ransomware+%E2%80%93+An+Enduring+Risk+to+Organizations+and+Individuals”,[Accessed online: Jan 2020]

[34] ”EnigmaSoft”,Available:”https://www.enigmasoftware.com/troldeshransomware-removal/”,[Accessed online: Jan 2020]

[35] ”Check point Software Technologies LTD”,Available:”https://blog.checkpoint.com/2015/06/01/troldesh-new-ransomware-from-russia/”,[Accessed online: Jan 2020]

[36] ”PcRisk”,Available:”https://www.pcrisk.com/removal-guides/9776-hydracrypt-ransomware”,[Accessed online: Jan 2020]

[37] ”Malwaretips”,Available:”https://malwaretips.com/blogs/remove-hydracrypt-virus/”,[Accessed online: Jan 2020]

[38] ”Bleepingcomputer”,Available:”https://www.bleepingcomputer.com/news/security/new-radamant-ransomware-kit-adds-rdm-extension-to-encrypted-files/”,[Accessed online: Jan 2020]

[39] ”Symantec”,Available:”https://www.symantec.com/security-center/writeup/2015-030201-5710-99”,[Accessed online: Jan 2020]

[40] ”TRENDMICRO”,Available:”https://www.trendmicro.com/vinfo/nz/security/news/cybercrime-and-digital-threats/the-ongoing-development-of-hidden-tear-variants”,[Accessed online: Jan 2020]

[41] ”HowToRemoveGuide”,Available:”https://howtoremove.guide/pclock-encryption-ransomware-removal/”,[Accessed online: Jan 2020]

[42] ”EnigmaSoft”,Available:” https://www.enigmasoftware.com/8lock8ransomware-removal/”,Accessed online: Jan 2020]

[43] ”Vinransomware”,Available:” http://www.vinransomware.com/8lock8-ransomware“.[Accessed online: Jan 2020].

[44] ”SPYWARE”,Available:”http://www.vinransomware.com/decryptor-max-ransomware“.[Accessed online: Jan 2020].

[45] ”Vinransomware”,Available:”http://www.vinransomware.com/omg-ransomware”,[Accessed online: Jan 2020].

[46] ”TRENDMICRO”,Available:”https://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-now-uses-windows-powershell/”,[Accessed online: Jan 2020].

[47] ”Sensors”,Available:”https://sensorstechforum.com/keyholder-ransomware-back-remove-restore-encrypted-files/”,[Accessed online: Jan 2020].

[48] ”REVE”,Available:”https://www.reveantivirus.com/en/computer-security-threats/cerber-ransomware”,[Accessed online: Jan 2020].

[49] Dick O’Brien, “Internet security threat”, 2017.

[50] ”Fandom”,Available:”http://malware.wikia.com/wiki/Sage”,[Accessed online: Jan 2020].

[51] ”Emsisoft”,Available:”https://blog.emsisoft.com/en/22935/apocalypse-ransomware-which-targets-companies-through-insecure-rdp/”,[Accessed online: Jan 2020].

[52] ”Solvusoft”,Available:”https://www.solvusoft.com/en/malware/ransomware/paycrypt/”,[Accessed online: Jan 2020].

[53] ”MalwarebytesLabs”,Available:”https://blog.malwarebytes.com/threat-analysis/2016/05/7ev3n-ransomware/”Accessed online: Jan 2020].

[54] ”Sensors”,Available:”https://sensorstechforum.com/remove-cryptohasyou-ransomware-and-restore-enc-encrypted-files/”Accessed online: Jan 2020].

[55] ”PCrisk”,Available:”https://www.pcrisk.com/removal-guides/9905-xorist-ransomware”Accessed online: Jan 2020].

[56] ”Viruses”,Available:”https://www.2-viruses.com/remove-alpha-crypt-ransomware”,[Accessed online, Jan 2020].

[57] ”SensorsTechForum”,Available:”https://sensorstechforum.com/nano-files-virus-ransomware-remove/”,[Accessed online, Jan 2020].

[58] M.Pitchaiah, Philemon Daniel, Praveen, “Implementation of Advanced Encryption Standard Algorithm”, International Journal of Scientific & Engineering Research, March 2012.

[59] Nikolai Hampton, Zubair A. Baig, “Ransomware: Emergence of the Cyber-extortion menace”, Australian Information Security Management Conference, 2015.

[60] Richardson, R. and North, M.M., 2017. Ransomware: Evolution, mitigation and prevention. International Management Review, 13(1), p.10., 2017

[61] Aaron Zimba, “Malware-free Intrusion: A Novel approach to ransomware infection vectors”, International Journal of Computer Science and Information Security, Volume (15), 2017.

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

[63] “TechBeacon”,Available:“https://techbeacon.com/ransomware-rise-evolution-cyberattack” ,[Accessed online, Jan 2020]

[64] ”Datarecovery”,Available:https://datarecovery.com/rd/cryptorbit-howdecrypt-ransomware-decryption-services/”,[Accessed online, Jan 2020]

[65] “TechTarget”,Available:”https://whatis.techtarget.com/definition/command-and-control-server-CC-server”, [Accessed online: Jan 2020].

[66] “Paloalto”,Available:”https://www.paloaltonetworks.com/cyberpedia/what-is-a-credential-based-attack”, [Accessed online: Jan 2020].

[67] “Wikipedia”,Available:“https://en.wikipedia.org/wiki/Bitcoin [Accessed online: Jan 2020].

[68] Dargahi, T., Dehghantanha, A., Bahrami, P.N. et al., “A Cyber-Kill-Chain based taxonomy of crypto-ransomware features”, J Comput Virol Hack Tech 15, 277–305 (2019).

[69] Asibi O. Imaji, “Ransomware Attacks: Critical Analysis, Threats, and Prevention Methods”, hal-02558819f, 2019.

[70] Zimba, A., Wang, Z. and Chishimba, M.. “Addressing Crypto-Ransomware Attacks: Before You Decide whether To-Pay or Not-To”. In Journal of Computer Information Systems, pp.1-11, 2019

[71] Herrera Silva, J.A.; Barona López, L.I.; Valdivieso Caraguay, Á.L.; Hernández-Álvarez, M. “A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters”. Remote Sens. 2019, 11, 1168.

[72] Nikolai Hampton, Zubair Baig, Sherali Zeadally, “Ransomware behavioural Analysis on Windows Platforms”, Journal of Information Security and Applications, 2018.

[73] A. Samad, M. A. Islam, M. A. Iqbal, M. Aleem and J. U. Arshed, "Evaluation of features for social contact prediction," 2017 13th International Conference on Emerging Technologies (ICET), Islamabad, 2017, pp. 1-6, doi: 10.1109/ICET.2017.8281744.

[74] Muhammad Azhar Iqbal, Muhammad Aleem, Muhammad Ibrahim, Muhammad Arshad Islam and Saleem Anwar, "Amazon Cloud Computing Platform EC2 and VANET Simulations", International Journal of Ad Hoc and Ubiquitous Computing, Vol. 30, No. 3, pp.127-136, 2019

[75] Madiha Ameer, Sumera Murtaza and Muhammad Aleem, "A Study of Android-based Ransomware: Discovery, Methods, and Impacts", Journal of Information Assurance & Security, Vol. 13. No. 3,pp. 109-117, 2018

[76] Sana Aurangzeb, Muhammad Aleem, Muhammad Azhar Iqbal, Muhammad Arshad Islam, "Ransomware: A Survey and Trends", Journal of Information Assurance & Security, Vol. 6, No.2.,pp.48-58, 2017