Ransomware: A Survey and Trends

Article · June 2017

CITATIONS
74

READS
19,149

4 authors:

Sana Aurangzeb
National University of Computer and Emerging Sciences
12 PUBLICATIONS **242** CITATIONS
SEE PROFILE

Muhammad Aleem
National University of Computer and Emerging Sciences Islamabad
139 PUBLICATIONS **2,089** CITATIONS
SEE PROFILE

Muhammad Azhar Iqbal
University of Management and Technology (Pakistan)
99 PUBLICATIONS **1,195** CITATIONS
SEE PROFILE

Muhammad Arshad Islam
FAST-NUCES Islamabad
87 PUBLICATIONS **895** CITATIONS
SEE PROFILE

Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 12 (2017) pp. XXX-XXX

Ransomware: A Survey and Trends

Sana Aurangzeb, Muhammad Aleem, Muhammad Azhar Iqbal and Muhammad Arshad Islam
Capital University of Science and Technology, Islamabad, Pakistan
sana.aurangzeb@gmail.com, aleem@cust.edu.pk, azhar@cust.edu.pk, arshad.islam@cust.edu.pk

***Abstract*: Ransomware are a recent scareware, a threat that is increasing gradually for last couple of years. Usually it encrypts users's files or steal/delete important information and holds the decryption key until a ransom is paid by the victim, which is mostly in bitcoins due to their untraceable properties. In this work, we have conducted a survey to comprehend more than 40 papers that consists of Windows based ransomware families from last 4 years by creating a benchmark for evaluating ransomware attacking methodologies, payment methods. Thus, providing a way of instigating for other researchers to come out with some new solutions to control their growth and to avoid their attacks. This work would be the ultimate opportunity to expand and organize research efforts in future work by applying some early preventions and strategies to defeat these malicious software's.**

***Keywords*:** *ransomware, malware, encryption, bitcoin;*

I. Introduction

Recently, ransomware have become a great threat to the computer and smart device users. Ransomware can be referred as scarewares that are designed basically to frighten users and force them either to quickly purchase the software used to protect user's private data, or to prevent irreversible damages. A ransomware encrypts the data of infected systems, and asks the user to pay a ransom usually, in Bitcoins [26] to regain full access to the attacked system. Many victims pay ransom in order to save their important data for which they do not have any backup. A recent example is CryptoWall version-3 [8], [34], which caused an estimated $325 million damage in the US alone during the period from November 2015 to June 2016. CryptoWall version 4 reached up to $7.1 million damage globally [8]. These types of ransomware usually pass through three phases 1) finding a target to victimize; 2) preventing access to local information; and then 3) displaying some scary or ransom message and try to extort some money.

According to [34], there are two basic types of ransomware available today, (a) locker-ransomware and, (b) crypto-ransomware. The first one is designed to lock the victim's computer and ultimately prevent the user from using it. The second one, which seems most common nowadays, encrypts personal files to make them inaccessible to its victim.

Windows malware are common in demanding ransom, however as far as mobile malwares are concerned they can employ a tool for blackmailing and demanding ransom. For example, the desktop Trojan Kenzero [14] not only steals the user's browser-history and also publishes it publicly on the Internet along with the person's name. It typically demands 1500 yen to take down the victim's browser history [11]. There has not yet been any mobile malware that seriously threatens or publicly embarrasses the user for profit except for one piece of mobile malware that demanded a ransom e.g., a Dutch worm [7] locks iPhone screens and later demands 5 euros to unlock the screens of the infected phone [7], [11]. Smartphones usually do not offer any technical advantages as compared to desktop computers where criminals keep on seeking for ransom from users. There might be a behaviour differences among users that makes one platform a more valuable ransom target than the other.

Victims usually are affected by threats which can be classified in three categorized:

A. Malware

Malware is a malicious piece of code that takes control of a device or a system for the purpose of either stealing data or damaging it and sometimes just annoying the user. This type of threat usually includes Trojans, worms, botnets, and viruses [11].

B. Personal Spyware

It tries to collect personal information such as geographical location or text message history over a particular period of time. With personal spyware, the attacker installs the software without the user's knowledge and has physical access to the device [11].

C. Ransomware

Malware that can be a used as a tool for blackmailing is referred as ransomware. Ransomware is malicious software that secretly infects victim's device, and suddenly demands a ransom payment in order to decrypt the encrypted data.

In this work, we present a study of the recent ransomware that have emerged during last 3 to 4 years. This study of 76 ransomware families aims to assist researchers and individual users to counter cybercriminal activities. In our knowledge, there does not exist any recent study related to these ransomware.

The remainder of the paper is organized as follows. In Section II, we present a brief overview related to evolution of ransomware. Section III presents our methodology we employed to collect and conduct ransomware data. In Section IV, we present detailed study of ransomware and their employed attack patterns. In Section V, we summarize 76 ransomware families, their features. Section VI describes the various payment methods employed byransomware. Section VII lists some characteristics related to attack methodology of ransomware. After analysis, we classify these ransomware families in Section VIII. Some preventions

and defence strategies are suggested in Section IX followed by conclusion in Section X.

II. Background

First ransomware attack was reported in 1989 using a program called AIDS Trojan [6]. In 2005, few initially reported cases were reported in Russia. After 2005, ransomware being evolved and spread using different social engineering techniques and employing more advanced encryption techniques to conceal user data. In 2013, a sudden increase in ransom amount was observed specially after emergence of CryptoLocker [40] ransomware. CryptoLocker spreads rapidly and infects computers and networks in both private and public sectors [27]. Few months later (after introduction of Cryptolocker), it caused $27 million worth of damages in the terms of ransom payments [12]. According to the Internet Crime Complaint Center, the release of a new ransomware program known as CryptoWall garnered cybercriminals over $18 million from April 2014 through June 2015 [44]. Statistics from US government agencies indicate that Cryptolocker infected 336856 machines in USA, 4593 in UK, 25841 in Canada, 15427 in Australia, 1832 in India, 100448 in other countries in 2014 mentioned in [22]. In summary, CryptoLocker, is infecting around 50000 computers per month [22].

The Dridex [4] a financial trojan has emerged as one of the most serious and dangerous online threat faced by consumers and businesses in 2015. Dridex steals credentials during online banking sessions and stole nearly 300 banks data and other financial institutions in over 40 countries. Dridex seems to be one of the major financial threats during the year 2016 [4]. Dridex is usually distributed through spam e-mails, malicious attachments, and is capable of injecting itself into the three most commonly used Windows web browsers [4]. The Windows based web browsers are infected during access of online back accounts (during a live banking session) [4].

The number of ransomware victimization in the first quarter of 2016 has increased by 3500% more that the fourth quarter of 2015 [6]. According to CNN News (2016) $209 million dollars were paid within few months of 2016. Currently, total number of ransomware has grown about 80% in 2016 [20].

III. Methodology

We have critically reviewed more than 40 authoritative papers from last three years that are published in a reputed journals and conferences. Based on these papers, we collected comprehensive data and analyzed it for several different ransomware families.

We analyzed 76 different ransomware families and summarized those in Table 1. In this study, we target only the desktop-based ransomware that are victimizing a huge community, causing a large financial loss, and difficult to beat. This survey helps in guiding users and other researchers to come up the way these ransomware attack, their type, target platform, ransom payment methods, and provides an opening many wide directions for future preventions and strategies to defeat them.

IV. Attack Patterns

In this section, we present a general ransomware attack pattern such as Windows ransomware and Android ransomware. In general, all ransomware go through similar stages. In the case of infected android devices, a ransomware first tries to gain an administrative privilege by simply asking for it or employing some social engineering tactics. Another way to acquire the administrative privilege is to ask the user to install software patches or click on some fake update pop-ups or antivirus updates. Generally, another step the ransomware employ is to ask for app-level permissions, which are required to perform necessary tasks. Mostly, an app asking for unnecessary permissions relative to its nature of work is always performing malicious activity. Almost all type of malwares have some sort of backdoor channel open for the attacker to get access to the infected system. Backdoored clients are referred as zombies. A Zombie machine or network often called botnet, are systems that hackers can control and make them for example join with other zombies to launch a *Distributed Denial of Service* (DDoS) attacks [31]. Employing these zombies, attackers exploit these for making money using several means and can hide his / her own identity. Moreover, a ransomware attacker can steal passwords and banking details easily.

If a ransomware attacker successfully gains administrative access and permissions of victim's device; the attacker may start gathering information and send the collected information to *Command and Control server* (C&Cs). C&Cs are used to gather stolen inform from different zombies spread across the network. Zombies usually connect C&Cs using encrypted Transport Layer Security mechanism to securely sending the stolen information [24]. For example, the crypto ransomware [24] obtains a private key from C&Cs in order to encrypt files of the victim's android device. After that the crypto shows threatening messages asking the victim to pay the ransom. The Locker [24] ransomware works differently compared to crypto, it eventually resets the device PIN and asks for the ransom payment.

On Windows platform, several attack mechanisms are common among the attacker ransomware [24]. A ransomware attacks the victim's machine via any malicious website, email attachment, or any malicious web-link, or several other ways mentioned in Section VI. Once the system gets infected, it contacts C&C server just like ordinary android application. It starts stealing victim's information and sends to the attacker. The attacker also acquires a randomly generated symmetric key from the C&C server. After that, it starts encrypting files and folders using asymmetric (RSA) encryption, where the key used for encryption cannot be used to decrypt the data. RSA algorithm uses two different keys, one (public key) for encryption of data and one (private key) for decryption [3], [21]. In parallel, the malware deletes all the restore points, backup folders, and shadow volume copies [24].

Considering locker ransomware [24], the same steps are carried out except it does not perform encryption on data. After acquiring administrative privileges, it locks the user access to the system and changes the desktop wallpaper or sometimes shows a window, which alerts ransomware attack and shows the steps to follow in order to regain system

access. Figure. 1 shows the details of ransomware attack based on 06 stages.

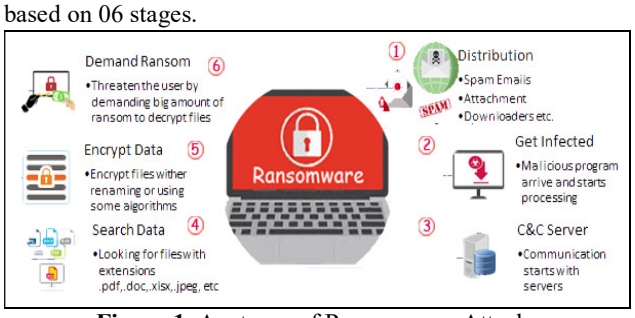

Figure 1. Anatomy of Ransomware Attack

V. Ransomware Characteristics

Almost all ransomware families show following characteristics i.e., *device locking*, *data encryption*, *data deletion*, *data stealing,* and *sending threatening messages* [2].

- *Device Locking:* It consists of denying victim to access devices, systems, data, or apps. With device locking, the attacker effectively disables hardware/software recourse access.
- *Data Encryption:* A ransomware employing data-encryption typically encrypts user's files. In some cases, the data is also stolen or removed. In order to access the encrypted data, the victim has to pay the ransom for decryption. Generally, the ransom is paid in bitcoins [30, 26]. Ransomware that employ data-encryption technique data are mentioned in Table 1.
- *Data Deletion:* Some ransomware (i.e., Reveton and Tobfy [16]) delete personal files and records no matter a user pays the ransom or not. Some ransomware enforce a user to pay ransom and in the case of late payment few files are deleted to threaten the victim.
- *Data Stealing:* Some ransomware (i.e., W32.Bolik.A!inf [37]) steals information and then later threaten the victim to publish it is another tactic performed by some cybercriminals.
- *Sending Threatening Messages:* A most all ransomware display some sort of threatening message and ask for some ransom payment. For ransom payments, ransomware mostly prefer bitcoins [26] or MoneyPak [13].

VI. Payment Method

The main aim of ransomware attacks is to get money from victims. That's why the payment method cannot be neglected. Cybercriminals constantly struggling to find more reliable and untraceable payment methods. They keep on improving their source of payment by discovering new ways that causes difficulty in tracing the identification of recipient of the payments, and can provide ease of exchanging payments into a preferred currency. Most common payment methods are:

1) Bitcoin

Bitcoin [26] is one of the most used payment method by cybercriminals. Bitcoin payment system was invented by an unidentified programmer or group of programmers, under the name of Satoshi Nakamoto [26]. Its untraceable nature is the main reason behind its popularity. According to the Massachusetts police, they paid a-bitcoin ransoms of worth more than $1,300 at the time, to decrypt one of their hard drives [32].

2) Premium Method

SMS ransomware are the main ways of payment for threatening. They ask to send SMS to a particular number in order to decrypt files. According to a paper [16] 'the premium rate numbers were hard-coded in the ransomware sample or were downloaded from the C&C servers in each infection. This class of ransomware attacks requires the least amount of technical background and when propagated in a large scale the revenue could be significant' [16].

3) Other Untraceable Methods

Some ransomware (for example Flocker [10]) instead of demanding payments via bitcoins, rather asks for iTunes gift cards worth of 200 USD. Some ransomware demand payments using Paypal [43], Ukash cards [32], MoneyPak [13], or by giving some email addresses and send instructions over there.

Our analysis concluded that most widely used payment method is bitcoin, MoneyPak, Paysafecard [32] a prepaid online payment systems. We found that other untraceable payment methods are also common among many ransomware families mentioned in Table 1.

Table 1 provides a list of the ransomware families (column 1). Some notable features of these ransomware are mentioned in column 2—11.

Table 1. List of Ransomware Families with their notable features, payment methods, type and platform.

Name	Notable Features					Payment Method			Type	Platform	Ref
	Summary	Data Deletion	Data Stealing	Data Encryption	Device Locking	Bitcoin	Premium	Untraceable			
DirtyDecrypt (2013)	Encrypts eight different file formats	-	-	✓	✓	-	×	✓	Trojan	Windows	[34]
CryptoLocker (2013)	Fetches a public key from the C&C for encryption	-	✓	✓	-	✓	×	✓	Trojan	Windows	[34]
CryptoWall (2013)	Requires TOR browser to make payments	-	✓	✓	✓	✓	-	-	Trojan	Windows	[34]
Android Defender (2013)	It is the first android locker-ransomware	✓	-	-	-	-	✓	-	Trojan	Android	[34]

Name	Notable Features					Payment Method			Type	Platform	Ref
	Summary	Data Deletion	Data Stealing	Data Encryption	Device Locking	Bitcoin	Premium	Untraceable			
Winlock (2013)	It is a Trojan horse that locks the desktop making the computer unusable	✓	-	×	✓	-	✓	-	Trojan	Windows	[16]
Loktrom Win32.zbot (2013)	Spreads through removable drives and may also download configuration files and updates from the Internet.	-	✓	-	✓	-	✓	-	Worm	Windows	[16]
Kovter (2013)	Steals information	-	✓	✓	-	-	-	✓	Trojan	Windows	[16]
Weelsof (2013)	Employs untraceable payments	-	-	-	-	-	-	✓	Worm	Windows	[16]
CryptoBit (2013)	Encrypt entire contents of the files.	-	-	✓	-	✓	-	-	Trojan	Windows	[41],[38]
RAA (2013)	RAA that is made 100% from JavaScript	✓	-	✓	-	✓	-	-	Trojan	Windows	
TorDroid (2014)	It is the first android crypto-ransomware	-	-	-	-	-	-	-	Trojan	Android	[34]
Critroni (2014)	Similar to CryptoWall	-	✓	✓	-	✓	-	-	Trojan	Windows	[34]
TorrentLocker (2014)	Stealthiness: indistinguishable from SSH connections, encrypt the files in parallel	✓	✓	✓	-	✓	-	-	Trojan	Windows	[34],[39]
CTB-Locker (2014)	Uses elliptic curve cryptography, TOR, and Bitcoin mechanisms			-	-	✓	-	-	Trojan	Windows	[34]
Reveton (2014)	Deletes files and steals information	✓	✓	-	-	-	-	✓	Trojan	Windows	[16]
Tobfy (2014)	Deletes files	✓	✓	×	-	-	-	✓	Trojan	Windows	[16]
Urausy (2014)	It is based on screen-locker. It does not allow access files without paying a ransom	-	-	-	✓	-	-	✓	Trojan	Windows	[16]
Filecoder (2014)	Encrypt files as well as delete the original unencrypted file's data	✓	-	✓	✓	-	-	✓	Trojan	Windows	[16]
CryptoDefense (2014)	Uses C2 Server, Cryptographically Secure Data Encryption	-	-	✓	-	-	-	-	Virus	Windows	[12]
Virlock (2014)	Virlock can now use as the cloud to spread	-	✓	✓	✓	✓	-	-	Virus	Windows	[18],[42]
GameOverZeus (2014)	Steals banking information and other types of user data	-	✓		-		-	-	Trojan	Windows	[41]
CryptoWall (2014)	Uses exclusively TOR for payment, encrypts file names	-	✓	✓	-	✓	-	-	Trojan	Windows	[34]
BackDoor.AlienSpy (2015)	Opens a back door on the compromised computer and may steal information and download files.	✓	✓	-	-	-	-	-	Trojan	Linux, Windows, Mac	[37][50]
Hidden Tear (2015)	It is an open-source ransomware released for educational purposes	-	-	✓	-	✓	-	-	Trojan	Windows	[34]
Chimera (2015)	Threatens to publish users' personal files	-	✓	✓	-	-	-	-	Trojan	Windows	[34]
Linux.Encoder (2015)	Encrypts Linux's home and other directories	-	-	✓	-	-	-	-	Trojan	Windows	[34]
Mabouia (2015)	Marques developed proof-of-concept to highlight the fact that Mac OS X computers may not be immune to ransomware.	-	-	-	-	-	-	-	Trojan	Windows	[25]
TeslaCrypt (2015)	Encrypts user file content, HiddenTOR, Diffie-Hellman Elliptic Curve Cryptography [DH-ECC] is used to generate public keys. DH-ECC is a new generation of fast and very secure public key algorithms.	✓	-	✓	-	✓	-	-	Trojan	Windows	[34],[12]
TorrentLocker (2015)	Encrypts files	✓	✓	✓		✓	-	-	Trojan	Windows	[18]
AlphaCrypt	File-encrypting ransomware program	✓		✓		✓	-	-	Trojan	Windows	[18]

Name	Notable Features					Payment Method			Type	Platform	Ref
	Summary	Data Deletion	Data Stealing	Data Encryption	Device Locking	Bitcoin	Premium	Untraceable			
(2015)											
Ransomware as-a-Service (2015)	Willingness to spread the ransomware	✓	✓	-	-	-	-	-	Trojan	Windows	[18]
Flocker (Android.Lockdroid.E) (2015)	It is capable of locking android smart TVs	-	-	-	-	-	-	✓	Trojan	Android	[25]
Phonywall (2015)	Fake ransomware, displays a ransom note identical to the real CryptoWall message	-	-	✓	-	-	-	✓	Trojan	Windows	[25]
W32.Disttrack.B (2016)	Disables the computer by overwriting the Master Boot Record	-	-	✓	-	-	-	-	Worm	Windows	[37]
DMA-Locker (2016)	Comes with a decrypting built-in feature	-	-	✓		✓	-	-	Trojan	Windows	[34]
Crysis (2016)	Targets individual and enterprise users		✓	✓		✓	-	-	Trojan	Windows	[23]
PadCrypt (2016)	It provides live chat support	-	-	✓		✓	-	-	Trojan	Windows	[34]
Locky (2016)	Installs using malicious macro in a Word document	-	-	✓		✓	-	-	Trojan	Windows	[34],[41]
CTB-Locker for WebSites (2016)	Targets Wordpress websites	✓	✓	×	×	-	-	✓		Websites	[34]
KeRanger (2016)	First ransomware for Apple's Mac computers	-	-	-	-	✓	-	-	Trojan	Mac	[34],[25]
Cerber (2016)	Offered as RaaS (& quote in Latin), ask for $500	-	-	✓	-	✓	-	-	Trojan	Windows	[34]
Samas (2016)	Pentesting on JBOSS servers	-	-	✓	-	✓	-	-	Trojan	Windows	[34],[41]
Petya (2016)	Overwrites MBT with its own loader and encrypts MFT	-	-	✓	-	✓	-	-	Trojan	Windows	[34]
Rokku (2016)	Use of QR code to facilitate payment	✓	-	✓	-	✓	-	-	Trojan	Windows	[34]
Jigsaw (2016)	Press victims into paying ransom	✓	-	✓	-	✓	-	-	Trojan	Windows	[34]
CryptXXX (2016)	Monitors mouse activities and evades sandboxed environment, contains a feature allowing it to gather Bitcoin wallet data and send it to the attackers.	-	-	-	-	✓	-	-	Trojan	Windows	[34],[25]
Mischa (2016)	Installs when Petya ransomware fails to gain administrative privileges	-	-	✓	-	✓	-	-	Trojan	Windows	[34]
W32.Bolik.A!inf (2016)	Steals login credentials		✓	-	-	✓	-	-	Virus	Windows	[37]
Satana (2016)	Combines the features of PETYA and MISCHA ransomware	-	-	✓	✓	✓	-	-	Trojan	Windows	[34]
Stampado (2016)	Promotes through aggressive advertising campaigns on the Dark web	✓	-	✓	✓	✓	-	✓	Trojan	Windows	[34]
Fantom (2016)	Uses a fake Windows update screen	-	-	✓	✓			✓	Virus	Windows	[34]
Cerber3 (2016)	Third iteration of the Cerber ransomware	-	-	✓		✓	-	-	Trojan	Windows	[34]
Website is locked ransomware (2016)	Targets websites (drupal)	✓	-	-	✓	-	-	✓	Trojan	Websites	[38]
DMA Locker (2016)	Encrypts files with similar names	-	-	✓	✓	✓	-	-	Trojan	Windows	[38]
Bucbi	Uses brute-force method and have	-	-	✓	-	✓	-	✓	Trojan	Windows	[25]

Name	Notable Features					Payment Method			Type	Platform	Ref
	Summary	Data Deletion	Data Stealing	Data Encryption	Device Locking	Bitcoin	Premium	Untraceable			
(Trojan.Ransomcrypt.AO) (2016)	strong grip over remote desktop protocol based servers.										
MM Locker (2016)	Behaves similar to the. locked ransomware	-	-	✓	-	✓	-	-	Trojan	Windows	[25]
8Lock8 (2016)	Encrypts your data and then appends the .8lock8 extension to encrypted files	-	-	✓	-	-	-	✓	Trojan	Windows	[38]
Shade/Troldesh (2016)	Creats using development kit that encrypts files using asymmetric encryption algorithm	-	-	✓	-	✓	-	✓	Viruses	Windows	[38]
Xorist (2016)	Allows a distributor to generate their own ransomware executable	-	-	✓	-	-	-	✓	Trojan	Windows	[38]
Zyklon Locker (2016)	It is variant of GNL locker	-	-	✓	-	-	-	✓	Trojan	Windows	[38]
MIRCOP (2016)	Highest ransom amount seen 48.48 bit coin (around $28,730.70)		✓	✓	-	✓	-	-	Trojan	Windows	[39]
Apocalypse (2016)	Apocalypse creates an autorun entry that prompts the ransomware to start when a user logs into the system	-	-	✓	✓		-	✓	Trojan	Windows	[46]
Chimera (2016)	Makes an additional threat in its ransom message, encrypts files,		✓	✓	-	✓	-	-	Trojan	Windows	[25]
Ransom32 (2016)	Uses NW.js framework and was packaged into an exe. File	-	-	✓	-	✓	-	-	Trojan	Windows, Linux, Mac	[25]
Necurs (2016)	Disables security services and elements	-	-	✓	-		-	-	Bootnet	Windows	[25]
Dridex botnet (2016)	Known for harvesting banking credentials		✓		-		-	-	Bootnet	Windows	[25]
ZCryptor (2016)	Infects all drives by copying itself before started encryption	-	-	✓	-	✓	-	-	Worm	Windows	[25]
Android.Lockdroid.E (2016)	Sends illegal videos on third-party app stores, the app snaps a picture of the victim using the device's camera and includes the image as part of the ransom note.	-	-	-	-	-	-	✓	Trojan	Android	[25]
Simplocker (Android.Simplocker) (2016)	Pretends to be legitimate apps and appear to be hosted on fake Google Play sites	-	-	✓	✓	-	-	✓	Trojan	Android	[25]
GhostCrypt (2016)	Uses AES encryption to encrypt data by calling itself CryptoLocker	-	-	✓	-	✓	-	-	Trojan	Windows	[38]
SNSLocker (2016)	This ransomware uses AES encryption and appends the .RSNS-locked extension to the encrypted files	-	-	✓	-	✓	-	-	Trojan	Windows	[38]
777 (2016)	The 777 ransomware encrypts data and then appends the 777 extensions to the encrypted files	-	-	✓	-	-	-	-	Trojan	Windows	[38]
BlackShades (2016)	The malware is known to encrypt 195 file types using 256-bit AES encryption	✓		✓	-	✓	-	-	Trojan	Windows	[1]
GOOPIC (2016)	This ransomware asks for US$500 payment and has a very professionally designed interface that gives more than 72 Hours for payment	-	-	✓	-	✓	-	-	Trojan	Windows	[30][47]
Kozy.Jozy (2016)	Runs the encryption in the background without the victim's knowledge and deletes the volume shadow copies to remove possible backups	✓	-	✓	-	✓	-	-	Trojan	Windows	[49]
.locked (2016)	Adds a .locked extension to each encrypted file	✓	-	✓	✓	✓	-	-	Trojan	Windows	[23]

VII. Attacking Mechanisms

Ransomware attackers try to hack the victims' system, for this purpose they adopt different strategies and infect the system in order to get access and demand for ransom. We studied 76 ransomware families and identify their attack mechanisms summarized in Table 2.

In Table 2, the first column indicates the name of ransomware and the rest of the columns represent several attacking parameters According to Cyber Threat *Alliance* [9], researchers discovered that the *crypt7* was the most active ransomware in CryptoWall 4 (CW4). Financially, the total CW4 profit was estimated at $18 million compared to CW3's profit of $325M. Both CW4 and CW3 ransomware families follow the same attack mechanism i.e., through email phishing and exploit kits [9].

- *Malicious Email or spam campaigns:* this attack mechanism comprises of malicious links or attachments. Email attachments are commonly masked as ZIP, PDF, DOC, or SCR file types.
- *Self-propagation:* means spreading from an infected computer to another. This technique represents a worm-like behaviour by spreading infected files to all contacts (available at that machine) using SMS messages e.g., ZCryptor is the first to display this self-propagation behavior on the Windows platform [38]. ZCryptor infects all removable drives too with a self- copy file. Before starting encryption process, it rapidly spreads itself to increase its chances of infecting other computers.
- *SMS messages and third-party app stores:* Android ransomware can be spread through third-party app stores and other means of communications e.g., messages etc. For example, Android.Lockdroid.E act as illegal video player and plays illegible pirated videos. Instead of playing such videos, it takes the snap of the victim using the device's camera and includes the image as part of video and asks for ransom [38].
- *Exploiting server vulnerabilities:* Ransomware attackers try to target control of vulnerable software that are installed and executing on servers in order to gain access to an organization's network.
- *Brute force passwords:* Another notorious tactic employed for spreading ransomware is through acquisition of login credentials using brute-force technique. Bucbi [38] ransomware uses this method to gain a foothold on remote desktop protocol servers [38]. After that, it starts encrypting files and infects other machines accessible from the server.
- *Exploit kits:* we usually see Ads on famous websites whose aim is to get more traffic and target a larger audience. The ransomware inject rogue advertisements into an advertising network sometimes known as *malvertising*. The *malvertising* redirects users to attacker's website exploiting vulnerability in the web browsers. The software systems used to compromise browsers are also known as exploit kits e.g., *Magnitude [15]*, *Angler [15]*, *Neutrino [15]*, and *Nuclear [15].* As mentioned in [34], almost 75% of exploits in Angler are based on Adobe Flash, whilst 20% are related to the Internet Explorer.
- *Downloader and Trojan Botnets:* are one of the ways to distribute malware, downloaders, etc. Downloaders infect a computer by downloading secondary malware onto the infected system. Trojan downloader come from software-hosting websites, whose main aim is to allow users to download legitimate files. However, sometimes they perform hidden functions by downloading malware without even notifying the user. The term *botnet* emerges with a combination of two words, *robot* and *network*. Botnets are computer network based auto software mentioned earlier as zombies. They control and instruct machines to do several tasks such as: *attack other computers*, *send spam* or *phishing emails*, *deliver ransomware*, *install spyware*, or many other similar malicious activities [5].
- *Social engineering tactics*: is based on deceiving a user to install a fake AntiVirus (by showing fake AntiVirus scans results). Psychologically, social engineering plays well in the context of deceiving, attackers to persuade people to perform certain actions or give away sensitive information or to extract data and gain unauthorized access. These tactics include lies, psychological tricks, bribes, extortion, impersonation and other type of threats.
- *Drive-by-Downloads:* are the legitimate websites that have malicious code injected in their web pages. Here, attackers compromise websites and embed malicious code such as malicious JavaScript code. This malicious code performs malvertisements, malicious redirects, and iFrames execution, cross-site scripting attacks, or other subtle attacks that potential victims cannot spot on their own [45], [48].

VIII. Classification

Malware can be classified into five groups according to their respective features as shown in Figure 2:

1) *Virus:* The code that replicates itself i.e., having features related to self-propagation is referred as virus. It has the feature of attaching itself to several other files;
2) *Trojan:* Trojan consists of malicious program that can harm any application or system easily;
3) *Worm:* A piece of code that can make copies of itself, can easily transfer from one removable drives to another. Thus, can damage files without notifying user;
4) *Rootkit:* A program that can easily apply changes to the operating system thus can remain there for a long period of time. Rootkit's main goal is to infect operating system, can install different Trojans and can even disable firewalls and antiviruses [29].
5) *Botnets:* As explained earlier in this survey, gives an attacker the ability to remotely control them. Botnets represent a serious security threat on the Internet for organized crime doing attacks to gain money, such as sending spam, *Denial-of-Service* (DoS) and many more.

We discuss mainly Trojans ransomware that are considered to be very serious among them and common in encrypting files and demanding ransom.

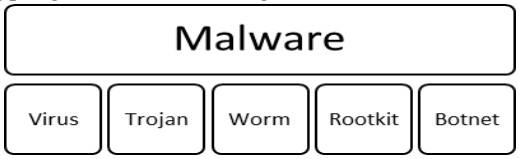

Figure 2. Classification of Malware

Table 2. Ransomware Attacking Methodology

Ransomware	Malicious Email / Spam Campaigns	Self-Propagation	Sms Messages	Third Party App Store	Exploiting Server Vulnerabilities	Brute-Forcing Passwords	Angler Exploit Kit	Neutrino Exploit Kit	Magnitude Exploit Kit	Downloader or Botnets	Social Engineering Tactics	Drive-By-Download	P2p Network	Other Ways
Zcryptor	-	✓	-	-	-	-	-	-	-	-	-	-	-	-
Android.Lockdroid.E	-	-	✓	✓	-	-	-	-	-	-	-	-	-	✓
Samsam	-	-	-		✓	-	-	-	-	-	-	-	-	-
Linux.Encoder	-	-	-	✓	✓	-	-	-	-	-	-	-	-	-
Ctb-Locker	-	-	-	-	✓	-	-	-	-	-	-	-	✓	-
Bucbi	-	-	-	-	-	✓	-	-	-	-	-	-	-	-
Dridex Botnet,	✓	✓	-	-	✓	✓	-	-	-	-	-	-	-	✓
Keranger	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Mabouia	-	-	-		-	-	-	-	-	-	-	-	-	-
Flocker	-	-	✓	✓	-	-	-	-	-	-	-	-	-	✓
Stuxnet	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Teslacrypt	✓	-	-	-	-	-	-	-	-	-	-	-	✓	-
Cerber	✓	-	-	-	-	-	-	✓	✓	-	-	-	-	-
Locky	✓	-	×	✓	-	-	-	✓	-	×	✓	×	✓	-
Cryptxxx	-	-	-	-	-	-	✓	✓	-	-	-	-	-	-
Reveton	-	-	-	-	-	-	-	-	-	✓	-	-	-	-
Php. Ransomcrypt.A	-	-	-	-	✓	-	-	-	-	-	-	-	-	-
Phonywall	✓	-	-	-	-	-	-	-	-	-	-	-	-	-
Chimera		-	-	-	-	-	-	-	-	-	-	-	-	-
Cryptowall	✓	-	-	-	-	-	✓	✓	-	-	-	-	✓	-
Samas	-	-	-	-	✓	-	-	-	-	-	-	-	-	-
Cryptolocker	✓	×	×	-	-	-	-	-	-	✓	✓	-	-	-
Dirtydecrypt	✓	-	-	-	-	-	-	-	-	✓	-	-	✓	-
Android Defender	-	-	-	✓	-	-	-	-	-	-	-	-	-	✓
Winlock	-	-	-	-	-	-	-	-	-	-	✓	-	-	-
Loktrom Win32.Zbot	-	✓	-	-	-	✓	-	-	-	-	✓	✓	-	-
Kovter	✓	-	-	-	✓		✓	✓	✓			✓		
Weelsof	-	✓	-	-	-	-	-	-	-	-	-	-	-	-
Tordroid	-	-	-	✓	-	-	-	-	-	-	✓	-	-	-
W32.Disttrack.B	-	✓	-	-	-	-	-	-	-	-	-	-	-	-
Cryptobit	-	-	-	-	✓	-	✓	✓	✓	-	-	✓	-	-
Critroni	-	-	-	-	✓	-	✓	✓	✓	-	-	✓	-	-
Torrentlocker	✓	✓	-	-	-	-	-	-	-	-	-	-	-	-
Tobfy	-	-	-	-	-	-	-	-	-	-	✓	-	-	-
Urausy	-	✓	-	-	✓	-	✓	-	-	-	-	✓	-	-
Filecoder	✓	-	-	-	-	-	-	-	-	✓	-	✓	-	✓
Cryptodefense	✓	✓	-	-	-	-	-	-	-	-	-	-	-	-
Virlock	-	✓	-	-	-	-	-	-	-	-	-	-	-	-
Alphacrypt	-	-	-	-	✓	-	✓	-	-	-	-	✓	✓	-
Ransomware As-A-Service	✓	-	-	-	-	✓	-	-	-	-	-	-	-	-
Dma-Locker	-	-	-	-	-	-	-	✓	-	-	-	-	-	-
Crysis	-	✓	-	-	-	-	-	-	-	-	-	-	-	-
Padcrypt	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Xorist	✓	-	-	-	-	-	-	-	-	-	-	-	-	-
Ctb-Locker For Websites	-	-	-	-	-	-	-	-	-	-	-	-	-	✓
Gameover Zeus	-	-	-	-	-	✓	-	-	✓	-	-	-	-	-
Petya	✓	-	-	-	-	-	-	-	-	-	-	-	-	-
Rokku	✓	-	-	-	-	-	-	-	-	-	-	-	-	-
Jigsaw	-	-	-	-	-	-	-	-	-	✓	-	-	-	-
W32.Bolik.A!Inf	-	-	-		-	✓	-	-	-	-	✓	-	-	-
Shade/Troldesh	✓	-	-	-	✓	-	-	-	-	✓	-	✓	-	-
Mischa	✓	-	-	-	-	-	-	-	-	-	-	-	-	-
Raa	✓	-	-	-	-	-	-	-	-	-	-	-	-	-
Satana	✓	-	-	-	-	-	-	-	-	-	-	-	-	-
Stampado	-	-	-	-	-	-	-	-	-	-	-	✓	-	-
Fantom	-	-	-	-	-	-	-	-	-	-	-	-	-	✓

Ransomware	Malicious Email / Spam Campaigns	Self-Propagation	Sms Messages	Third Party App Store	Exploiting Server Vulnerabilities	Brute-Forcing Passwords	Angler Exploit Kit	Neutrino Exploit Kit	Magnitude Exploit Kit	Downloader or Botnets	Social Engineering Tactics	Drive-By-Download	P2p Network	Other Ways
Cerber3	✓	-	-	-	-	-	-	-	-	-	-	-	-	
Website Is Locked Ransomware	-	-	-	-	-	-	-	-	-	-	-	-	-	✓
Mm Locker	✓	-	-	-	-	-	-	-	-	-	-	-	✓	✓
8lock8	✓	-	-	-	-	-	-	-	-	-	-	-	-	✓
Mircop	✓	-	-	-	-	-	-	-	-	-	✓			✓
Apocalypse	-	-	-			✓	-	-	-	-	-	-	-	✓
Zyklon Locker	✓	-	-	-	-	-	-	-	-	-	-	-	-	✓
Ransom32	✓	✓			-	-	-	-	-	-	✓			
Necurs	✓	-	-	-	-	-	-	-	-	✓	✓			
777	✓	-	-	-	-	-	-	-	-					
Simplocker	-	-	-	✓	-	-	-	-	-	-	-	-	-	✓
Ghostcrypt	✓	-	-	-	-	-	-	-	-	-	-	-	✓	-
Snslocker777	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Blackshades	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Goopic	-	-	-	-	-	-	✓	-	-	-	-	-	-	✓
Kozy.Jozy	-	-	-	-	-	-	-	-	-	-	-	-	-	
Backdoor.Alienspy	✓	-	-	-	✓	-	-	-	-	-	-	-	-	-
.Locked	✓	-	-	✓	-	-	-	-	-	-	-	-	✓	✓

IX. Preventions and Defeating Strategies

To reduce the risk of infected devices and victimization, prevention is the foremost option. Below, we discuss some of the prevention techniques:

- Microsoft Office attachment is unsafe if asking users to enable macros. So, avoid these prompts. Spam filtering and web gateway filtering are great ways to stop such ransomware [18].
- Email filtering services are essential to prevent from getting infected. One of the services provided by Symantec Email Security Cloud [38] can help to stop malicious emails before they target users.
- Block email messages with attachments *.exe, *.zip, *.rar, *.7z, *.js, *.wsf, *.docm, *.xlsm, *.pptm, *.rtf, *.msi, *.bat, *.com, *.cmd, *.hta, *.scr, *.pif, *.reg, *.vbs, *.cpl, and *.jar from suspicious sources [35].
- Don't give yourself more login power than needed as allowing yourself more administrator rights during normal usage, surfing the web, opening applications and other important documents, is very dangerous. In case you get attacked with malware while you have fewer rights, malware will also execute with fewer rights ultimately reduces the chance of getting infected [18].
- Make sure your firewall is properly configured [35].
- Browser protection is necessary, it is better to stay updated and have latest versions. For this purpose, make sure web-filtering technology is active and updated. As many ransomware strategies take advantage of vulnerabilities in the operating system or other apps to infect. Having updated and latest operating system and application versions will reduce the attack ratio.
- Backup and restore files locally on weekly basis by creating a storage volume and running archival differential-based file backups to that storage volume [18]. It helps removing ransomware by only going back in time with the backup to a point before the ransomware affected the files, and restores all the files that were affected once without paying any amount. Today, systems provide built-in options for backups.
- Backup should be stored on a separate drive that must not be connected to the network [18].
- Users are advised to immediately delete any suspicious activity on monitors [35].
- Scan all software downloaded from the Internet before executing and installing [35].
- Run USB's only if it is from trustable sources.
- Have up-to-date Anti-virus from latest patches.
- Scan computer system regularly.

Implementing these strategies can help defeating ransomware to a greater extent.

X. Conclusions

Ransomware threat is increasing rapidly for sometime years. After a critical analysis of 76 ransomware families, we come to a conclusion that ransomware are using varying methods to increase their spreading. Cybercriminals are keen in discovering new methods of social engineering tactics to target their victims. It is now becoming their prime source of earning by employing untraceable payment methods e.g., bitcoins. Cybercriminals are not only affecting individuals who are home users but also, they target large organizations and other businesses where the chances of acquiring ransom are high. In this study, we present ransomware' comparative analysis considering several properties and characteristics. After this study, we conclude that only way to avoid being affected from these malicious software are to implement precautionary measures including updated software, anti-viruses, proper screening of data acquired over network, maintaining backups, and avoiding untrusting links or emails, etc.

References

[1] B. Watkins. “The Impact of Cyber Attacks on the Private Sector”.*Briefing Paper, Association for International Affair*, pp.12, 2014

[2] N. Andronio.-“Heldroid: Fast and Efficient Linguistic-Based Ransomware Detection”, 2015

[3] M. Barbulescu, A. Stratulat, V. T. Popescu, E. Simion. “RSA Weak Public Keys available on the Internet”. In *International Conference for Information Technology and Communications*. Springer International Publishing, pp. 92-102, 2016

[4] O’Brien. “Dridex: Tidal waves of spam pushing dangerous financial Trojan”, *Symantec White paper*, 2016

[5] I. Ullah, N. Khan, H.A. Aboalsamh. “Survey on botnet: Its architecture, detection, prevention and mitigation”. In *Networking, Sensing and Control (ICNSC), 2013 10th IEEE International Conference IEEE,* pp. 660-665, 2013.

[6] K. S. Choi, T. M. Scott, D.P. LeClair. “Ransomware Against Police: Diagnosis of Risk Factors via Application of Cyber-Routine Activities Theory”, *International Journal of Forensic Science & Pathology*, IV (7), pp. 253-258, 2016

[7] G. Clucley. “Hacked iPhones held hostage for 5 Euros”, *Naked Security*, 2009

[8] Cyber Threat Alliance. “Lucrative ransomware attacks: Analysis of the cryptowall version 3 threat”, *Cryptowall version 3 Threat report,* 2016

[9] Cyber Threat Alliance. “Lucrative Ransomware Attacks: Analysis of the CryptoWall Version 4 Threat”, *Cryptowall version 4 Threat report,* 2016

[10] E. Duon. “FLocker Mobile Ransomware Crosses to Smart TV”, *Trend Micro Incorporated report*, 2016.

[11] A. P. Felt, M. Finifter, E. Chin, S. Hanna, D. Wagner. “A Survey of Mobile Malware in the Wild”. In *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices,* pp. 3-14, ACM, 2011.

[12] N. Hampton, Z. A. Baig. “Ransomware: Emergence of the cyber-extortion menace”. In *The Proceedings of 13th Australian Information Security Management Conference*, pp. 47-56, 2015.

[13] K. Jarvis. “Cryptolocker ransomware, 2013”, *SecureWorks*, pp. 30–31, 2014.

[14] C. Johnson. “Kenzero virus blackmails those who illegally download anime porn”. *BBC* report, 2016.

[15] B. L. Joseph, C. Chen. “Evolution of exploit kits exploring past trends and current improvements”, *Trend Micro White paper*, 2015.

[16] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, E. Kirda. "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 International Publishing, pp. 3-24, 2015.

[17] D. Kim, S. Kim. “Design of Quantification Model for Ransom Ware Prevent”. *World Journal of Engineering and Technology*, III (3), pp. 203-207, 2015.

[18] R. Leong. “Understanding Ransomware and Strategies to Defeat it”. *McAfee Labs part of Intel security*, 2015.

[19] F. Mbol, J. M. Robert, and A. Sadighian. “An Efficient Approach to Detect Torrentlocker”. In *International Conference on Cryptology and Network Security*. Springer International Publishing, pp. 532–541, 2016.

[20] McAfee Labs. “Threat Predictions Ransomware Infographic”. *McAfee Labs Threats Predictions 2017 report*, 2017

[21] N. Neelima, L. S. Siddhartha, C. Meghana, S. Sameer, S. Ashika, V. N. Chandramouli. “Security In Manets Using Cryptography Algorithms”, 2017

[22] F. Mercaldo, V. Nardone, A. Santone, C. A. Visaggio. “Ransomware Steals Your Phone. Formal Methods Rescue It”. In *International Conference on Formal Techniques for Distributed Objects, Components, and Systems*. Springer International Publishing, pp. 212-221, 2016.

[23] Avast. “Ransomware Decryption Tools”, *Avast Software*, 2016

[24] P. Monika, D. Zavarsky, Lindskog. “Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization”, *Procedia Computer Science*, 94, pp. 465- 472, 2016

[25] A. Moro, A. Valero, D. Garcia. “Malware Panda Security”, *Panda Security* report, 2016.

[26] S. Nakamoto. “Bitcoin: A peer-to-peer electronic cash system”, Consulted, I (MMXII), pp. 28, 2008.

[27] O’Gorman, G. McDonald. *“Ransomware: A Growing Menace*”, Symantec Corporation, 2012.

[28] D. Palmer. “Virlock ransomware can now use the cloud to spread, say researchers”, 2016

[29] M. L. Polla, F. Martinelli, D. Sgandurra. “A Survey on Security for Mobile Devices”, *IEEE Communications Surveys & Tutorials*, XV (1), 2013.

[30] Microsoft. “Malware Protection Center: Ransom:Win32/Goopic.A”. *Microsoft Security Threat*, 2017.

[31] H. Luo, Z. Chen, J. Li, A. Vasilakos. “Preventing Distributed Denial-of-Service Flooding Attacks with Dynamic Path Identifiers”, *IEEE Transactions on Information Forensics and Security*, 2017.

[32] D. Sancho. “Police Ransomware Update”, *Trend Micro Incorporated Research Paper*, 2012

[33] N. Scaife, H. Carter, P. Traynor, K. R. B. Butler. "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data". In *Distributed Computing Systems (ICDCS), 2016 IEEE 36th International Conference on*. IEEE, 2016.

[34] D. Sgandurra, L. Muñoz-González, R. Mohsen, E. C. Lupu. “Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection”, *arXiv preprint arXiv:1609.03020,* 2016.

[35] D. F. Sittig, H. Singh. “A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks”, *Applied Clinical Informatics, Schattauer*, VII (2), pp.624, 2016.

[36] S. Song, B. Kim, S. Lee. “The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform”, *Mobile Information Systems*, MMXVI, 2016.

[37] Symantec Security Response. [Online]. Available https://www.symantec.com/security_response/landing/azlisting.jsp?azid=W, 2016

[38] Symantec. “An ISTR Special Report: Ransomware and Businesses”. *Symantec Whitepapers ISTR2016*, 2016

[39] Trend Micro. “Ransomware Recap: New Families and Updated Variants in June”. *Trend Micro Incorporated Labs report*, 2016
[40] Trend Micro. “Ransomware”. *Trend Micro Incorporated Labs report,* 2016
[41] US-CERT. “Ransomware and Recent Variant”, September 2016
[42] S. Mansfield-Devine. “Ransomware: taking businesses hostage”, *Network Security*, MMXVI(10), pp. 8-17, 2016
[43] C. Darie, E. Balanescu.“*Receiving Payments Using PayPal”,* Apress, pp. 249-266, 2008.
[44] G. Yorkdale “Criminals Continue to Defraud and Extort Funds from Victims Using CryptoWall Ransomware Schemes”, *Federal Bureau of Investigation*, 2015.
[45] C. Dwyer, A. Kanguri. “Malvertising-A Rising Threat To The Online Ecosystem”. In *Proceedings of the Conference on Information Systems Applied Research ISSN,* MMCLXVII, pp. 1508, 2016
[46] R. Richardson, M. North. “Ransomware: Evolution, Mitigation and Prevention”, *International* Management Review, XIII (1), pp. 10, 2017.
[47] C. C. Joseph. “After Angler: Shift in Exploit Kit Landscape and New Crypto-Ransomware Activity”, *Trend Micro White paper*, 2017.
[48] Ali, Azad, R. Murthy, F. Kohun. "Recovering From The Nightmare Of Ransomware–How Savvy Users Get Hit With Viruses And Malware: A Personal Case Study." *Issues In Information Systems,* XVII (4), 2016.
[49] E. Duon. “New Ransomware Alert: Kozy.Jozy, and Another That Targets Zimbra Servers”, *Trend Micro Incorporated report*, 2017
[50] Zimba, Aaron. “Malware-Free Intrusion: A Novel Approach to Ransomware Infection Vectors”. *International Journal of Computer Science and Information Security* XV(2), pp. 317, 2017.

Author Biographies

Sana Aurangzeb received her Master’s degree in Computer Science from University of Lahore, in 2014. She is currently doing M.Phil. from Capital University of Science and Technology, Islamabad, Pakistan Her research focus is malware analysis and security services..

Muhammad Aleem received his PhD degree in computer science from the Leopold-Franzens-University, Innsbruck, Austria in 2012. His research interests include parallel and distributed computing comprises programming environments, multi-/many-core computing, performance analysis, Cloud computing, Big data processing, and scheduling.

Dr. Muhammad Azhar Iqbal received PhD degree in Communication and Information Systems from Huazhong University of Science and Technology, Wuhan, P.R. China in 2012. His research areas include: coding-aware routing in Vehicular Ad hoc Networks, energy-efficient MAC for Wireless Body Area Networks, large-scale simulation modeling and analysis of computer networks in Cloud.

Muhammad Arshad Islam completed his doctorate from University of Konstanz, Germany in 2011. His dissertation is related to routing issues in opportunistic network. His current research interests are related to online privacy and security, DTNs, Social-aware routing and Graph Algorithms.