ISSN:0975-9646

A study on Defacing Ransomware: Are we aware and ready?

Naman Gupta[#1], Vidyavati Ramteke[#2]

#Symbiosis Center for Information Technology, Symbiosis International University, Pune, Maharshtra, India

Abstract- **Hardly a day passes by when we do not hear about a ransomware locking data and demanding the ransom. Ransomware is the most opportunistic type of malware, affecting from a single user to an entire organization. This pilot study conducted targeted on the issues related to ransomware, the classifications and what the organizations are not doing to stop it. It also focusses on the readiness and the awareness amongst the people for such a growing malware. Not only this will help in understanding the mindset of the people about this gigantic threat but will also help in calculating the footprints of what has been the cause to it.**

Keywords- **Ransomware, Crypto Drop, Bitcoins**

i. INTRODUCTION

Ransomware is a popular kind of Trojan, which can disrupt the normal use of users' data assets and computers resources by harassment, intimidation and even kidnapping user files to extort money from users. The data assets include documents, e-mails, databases, source code, images, and compressed files and so on. The ransom includes real currency, Bitcoin and other virtual currencies [2]. Typically, the author of ransomware will set a specific period for payment, and the number of ransom will be raised over the time.

The guideline behind ransomware is devastatingly straightforward, regardless of the possibility that the specialized subtle elements around new variations develop more perplexing and complex by the day.[2] The thought is that offenders square access to a framework or its information until a specific measure of cash is paid by the victim. Ransomware's barricade can be accomplished by encoding documents or envelopes, ruining framework access to the hard drive, or even by controlling the ace boot record to interfere with the framework's boot procedure. New techniques for upsetting clients' get to manifest routinely, yet generally, crypto ransomware overwhelms the field.

Further with this research, we have focused on the anatomy of the attack, types and classifications of ransomware and what measures can be taken at organization level in order to stop the same.

A. DISTRIBUTION

Similar to common Trojans, ransomware are spread by the following scenarios:

1. Usually spread using Web Trojans once users visit malicious websites and they are downloaded and run in the background,
2. Package or a Bundle release with some other tools or malicious software,
3. Delivered in the email attachments,
4. It is also spread by the removable storage medium.

B. ORIGINATION OF RANSOMWARE MALWARE

The earliest and the most easy to avoid known ransomware, named as Trojan/DOS.AidsInfo or PC Cyborg, was designed by Joseph Popp in 1989. This malware is somehow injected and transferred into a system as an AIDS Information boot disk, and replaces AUTOEXEC.BAT to count when the computers start. Once the system boot times is up to 90 times, the Trojan will start hiding multiple directories of the disk, and names of all the files in C disk will be encrypted (the system failing in startup). Also there would be a message popping on the screen at the moment, saying that the software license has expired and the user needs to pay "189 dollars" to Panama for unlocking the system. The author quibbled that this illegal action was for AIDS research when he was indicted.

C. ANATOMY OF A RANSOMWARE ATTACK

The most common attack vector is a phishing email where the victim is tricked into clicking on a link in what appears to be a legitimate email message.([5], [6], [12]) Below are the 6 stages of ransomware attack. The last three steps use TOR (anonymous proxy) if it has not blocked by the organization [9].

a) Selection of a Victim,
b) Getting the payload to a victim's computer,
c) Contact with the command and control,
d) Download the Public keys,
e) Encrypt the Public Files,
f) Extortion of the Money
g)

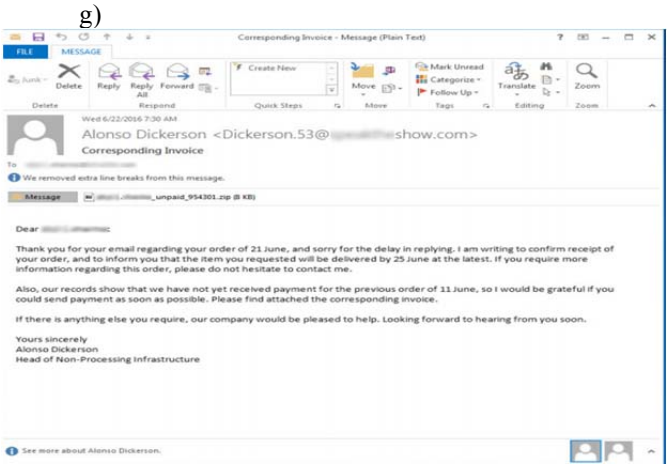


Fig. 1 Source: Trend Micro

i. Selection of the Victim

Attacker comes into contact with the victim by war driving or target attack technique.

War Driving

A ransom attack is always launched on a huge scale to the complete target base, usually via a phishing email to a mailing list containing thousands of emails addresses or the victim visits the malicious or compromised website and downloads the infected executable or vulnerability on their computer is exploited. Usually, an insecure organization with untrained users and unpatched client-side software can be a victim of war driving attack[5].

Targeted Attack

In targeted attacks, the attacker hand-picks a single or set of chosen targets. Recently, we encountered one such attack. When attackers realized (based on job advertisement) that McAfee products are being extensively used in the company, they sent a phishing email to get an employee into a chat session using a known Remote

Support Access Provider.

ii. Getting the Payload to the Victim's computer

There are many ways to drop a generic ransomware, and a phishing email attack is the most popular. For example, in the traffic infringement notice in figure 6, both the invoice and view camera images links redirect you to the attacker's website.

iii. Contact with Command and Control

The first step after installation of ransomware is to contact the command-and control(C&C) server in order to get further instruction or encryption key. Most antivirus software block the malware by preventing its execution at first instance if it has a known detection signature. AV, IPS (Intrusion Prevent System) and Firewalls maintain a list of malicious Proxies and C&C IP addresses and thus detect the presence of malware when a malicious program attempts to communicate. This method is not a very efficient as it is not possible to build a comprehensive list of all malicious destinations.

iv. Download the Public Keys

An attacker may decide to use the infected system as a ransomware launching pad to spread the infection across the network. Once the attacker is satisfied with the number of infections in a particular organization, the public keys are delivered to all the bots.

v. Encrypt the Files

The earlier versions of crypto-locker would just encrypt the files on the local computer. However, new variants try to encrypt the backup first. They specifically scan the local computer and remote file shares named in date format (keeping in mind 90% of backup folder/files names include date e.g. sql20150619.bak) and encrypt all the contents of these folders then it encrypts specific file types only. Encryption in-progress can be detected and interrupted by an incident response team, so it is critical for an attacker to prioritize the files to be encrypted, ensuring important files are encrypted first. Commonly, ransomwares start with files/folder with most recent access date.

vi. Extortion of Money

The next step is to notify the victim about the damage and facilitate the trial recovery by providing the new crypto-locker software in case newly installed AV has deleted it. Common AV uninstall/exclusion steps are communicated along with payment instructions. Once the ransom is paid and verified by the hackers manually (which may take a 2 to 48 hours), the private key may be delivered, and automatic decryption starts.

D. Types of Ransomware

In today's main arena of ransomware there are majorly 2 types of ransomware which are *encrypting* and *non-encrypting*.[1]

The former one systematically encrypts files on the system's hard drive, which becomes difficult to decrypt without paying the ransom for the decryption key. Payment is asked for using Bitcoin, MoneyPak, and PaySafeCard, Ukash or a prepaid (debit) card.

Although the later one employs fairly simple techniques to restrict access to the system and prominently displays a pornographic image, or

a scam message from law enforcement and asks users for payment using premium-rate SMS, or using the same methods noted for encrypted ransomware, to receive a code to unlock the machine[13].

Ransomware also can be classified into the following broad categories:

a) Winlocker
b) MBR ransomware
c) File encryptors
d) Rar compressed, password protected

i. Winlocker

Winlocker is a variant which locks the computer and asks the user to make payments. It uses two different strategies to seek payments:

a) SMS ransomware
b) Fake FBI ransomware

Source: Symantec

a) *SMS ransomware*

This variant locks the screen and displays a message including a phone number with the input code, such as the one shown below. To unlock the machine, the user must send the input code to the premium number to receive the corresponding unlock code.

b) Fake FBI ransomware

Ransomware authors quickly realized that antivirus vendors can easily provide a solution to unlock the machine without sending an expensive SMS. Thus they changed gears and adopted a different method.

This variant asks the user to make the payment via an online payment service. In reality, it is not feasible to track the recipient of the ransom amount. The warning messages in this version are delivered based on the geolocation of the user.

ii. MBR ransomware

This type infects the Master Boot Record (MBR) of the operating system and asks for a ransom to be paid through a specific payment system. It shows a fake message claiming that all files on the user's system are encrypted. In reality, they are not encrypted. It asks the user to pay ransom via the VISA QIWI Wallet payment processing system. It works by replacing the original MBR code with its own ransom MBR code.

iii. **File encryptors**

This variant locks the user's screen as well as encrypting the user's files, excluding system related files. Below are examples of the more common variants:

a) GpCoder
b) Cryptors using custom encryption

iv. **Rar compressed-password protected**

This type of ransomware doesn't encrypt files instead it uses a different encryption technique. It generates a key which is used as a password for rar compressed user files. There are different methods used to generate the required keys.

a) A simple hardcoded key combined with an ID unique to the machine.

b) Two different keys are used. One of the keys is sent to the C&C server, without which it's not feasible to recover the rar compressed user files.

E. What is there to worry about?

i. Incomplete Backups

While many organizations do have backup recovery plans in place, the execution of these plans may not be complete enough to cover the exigencies of a ransomware attack. For example, backups of certain endpoints may be incomplete or irregular, particularly in the case of remote workers or BYOD endpoints. Even if the data is not mission critical, its loss or temporary unavailability could greatly impact affected users' productivity.

ii. Employees May Pay Ransom Covertly

Whether it is because a big project needs to be completed within a couple of hours, or the employee is too embarrassed to approach IT with the problem, there's a very real threat that an employee could pay the ransom without alerting the organization.

In such cases, the employee might bear the cost themselves, or hide it in an expense report as some sort of miscellaneous charge, thus avoiding the hassle of IT intervention.

iii. Ransomware's Deletion of Backups

Increasingly, new ransomware variants are finding ways to target backup files as a part of their attack patterns. The more sophisticated extortionists recognize that they lose an opportunity for strong-arming victims when backups are in play, and they're adding this new tactic as a way to maximize their gains.

II. IS IT POSSIBLE TO GET BACK THE DATA WITHOUT PAYING RANSOM?

A. Recover the file from backup

The most efficient and effective way to get back the data is to restore data files from a backup. In most corporate environments files are backed up regularly so recovery should not be a problem. Normally a backup is made for shared and mapped drives. User desktop data is rarely saved.[4]

Users should backup the files to a network drive or USB drive and disconnect it after the backup. Almost all ransomwares encrypt the network drives.

B. Use built-in file versioning services like Windows Volume Shadow Copy

Windows Volume Shadow Copy can be enabled on any drive. It keeps the version history of all the files on the drive and makes it possible to go back on the timeline. However, newer ransomwares try to delete all the shadow copies using a Windows command"C:\Windows\Sysnative\vssadmin.exe" Delete Shadows /All /Quiet". It is an interesting fact that the Volume Shadow Copy feature is also used by malware to store a malicious code and overwriting it with some innocent content to evade the anti-virus scanning even with an updated signature. This malicious code is later recovered and executed when needed.[3]

C. Recover the most critical data using forensic techniques

When a file is opened for editing, almost all applications create a temporary copy of the original file. All the changes are made to the temporary file which overwrites the original file when saved. This is how Microsoft Office recovers files if the application closes abruptly. Once a user exits the application, the temporary file is deleted. On Windows, deleting a file means deleting the pointer to the file (not the contents) in NTFS/FAT/EFS file system.

D. Find flaws in the implementation of encryption

Most of the attacks against encryption are successful due to programming or architectural flaws in the encryption routine, such as using a repetitive, predictable seed, or misinformation about the strength of cryptographic routines etc. A crypto-locker variant, Racketeer, which spread through a fake Energy Australia bill email, used a flawed process of generating an RSA key pair on a victim's machine, which was then cracked during analysis and the private key was recovered using brute force technique.

E. Law Enforcement tracks down criminals and seizes private keys.

Ransomware is a consistent threat, and governments and IT Vendors have to join forces to bring the criminals to justice. One notable combined effort by the private and government sector is “OperationTovar” against the botnet Gameover Zeus. Gameover Zeus was a peer to peer botnet network and it was widely used as a launching pad for cryptolocker attacks. In 2014, US Law Enforcement officials announced the success of Operation Tovar and intercepted thetransfer of 500,000 private keys. The creator of Game over Zeus botnet, nicknamed“lucky12345” was identified as a Russian man, Evgeniy Bogache[12].

III. AWARENESS & IMPACTS

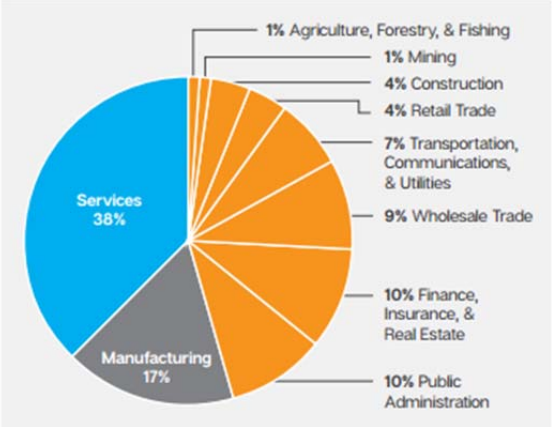
Almost every sector has been affected by ransomware in recent years, but some types of organizations appear to be harder hit than others.

In a recent survey conducted, it was proved that 99% people are not even aware of the term ransomware and if they are aware they don’t know whether they have been impacted because of it or not.

Analysis of infections in known sectors has found that between January 2015 and April 2016, the Services sector, with 38 percent of infected computers, was by far most affected by ransomware[6]. Manufacturing, with 17 percent of infections, along with Finance, Insurance, and Real Estate, and Public Administration (both on 10 percent) also figured highly. Rounding out the top 10 were Wholesale Trade (nine percent), Transportation, Communications, and Utilities (seven percent).

In a recent survey conducted by barkly inc. this year with over 330 IT pros, 81 percent were confident backup would provide them with complete recovery from a ransomware attack. But less than half of those who had actually experienced an attack were able to fully recover their data with backup.

One of the shocking reveal of this survey was that More than 60 percent of attacks took more than 9 hours to remediate which means complete loss of goodwill, customers and money.



Source: Symantec

According to the survey conducted, 73% people have agreed that out of all the devices that they have, laptops have been the mostly affected device. While other people agree that their iPads, Mobiles and Desktops have been affected.

Also almost 46% people have declared out of the complete lot who were being surveyed have laid their confidence on nature of attack to be e-mails. Because of this mischievous attack 60% people/organizations have ended up paying over 1000$.

Fifty-eight percent of respondents in a recent survey still primarily rely on antivirus software to protect their data and assets. This is based on a survey Trend Micro conducted from February to April 2016, wherein organizations—represented by 278 online respondents—were asked to rate the effectiveness of their own security posture. [10]

Of the total number of respondents, more than half (54%) admitted that their organizations would suffer a great deal of damages in case the files stored in their servers get compromised or encrypted. This is why it is crucial for organizations to consider investing in solutions that focus on email and web reputation for gateways, as well as application control for endpoints. In case of a local infection, behavior monitoring can help contain the issue before it spreads.

Almost 60% of the respondents belong to organizations that allow the use of personal mobile devices to access company data. A whopping 58% of the respondents admitted to not having any form of mobile device management strategy in place.

IV. BUSINESSES: THE NEXT BIG TARGET

Realizing the potential for higher profits, cybercriminals are increasingly targeting the business space. We have seen this trend emerge in other attack campaigns, such as:

- Business email compromise (BEC) scams, which attempt to trick C-level executives into making large wire transfer payments[6].
- Bug-poaching attacks, which involve attackers compromising corporate servers, stealing data (as proof of compromise), and requesting a fee for information on how the attack was carried out
- The Carbanak gang, which target banks directly rather than bank customers.

Ransomware gangs have become the latest to follow the trend. Holding businesses to ransom can significantly raise attackers' return on investment. Symantec has seen a steady increase in the number of organizations targeted with ransomware in recent times. Most of these new victims are hit in indiscriminate campaigns, where employees have opened a malicious spam email or visited a malicious website. However, a growing number are victims of far more dangerous, targeted campaign[6]. Many of these targeted ransomware attacks use similar tactics to advanced persistent threats (APT) such as:

- Using freely available, dual-use tools to help gain a foothold and move through a network
- Obtaining administrator credentials and using them for lateral movement
- Conducting reconnaissance to gain information that could help criminals extort money from the target organization.

V. IMPACT OF RANSOMWARE

The average ransom demanded by attackers has once again risen this year. The average ransom discovered to date in 2016 stands at US$679, up from $294 in 2015. The steady rise in ransom demands indicates that attackers may think there is more to be squeezed from victims. This year has also seen a new record in terms of ransom demand, with a threat known as 7ev3n-HONE$T (Trojan.Cryptolocker.AD) requesting a ransom of 13 bitcoin per computer ($5,083 at the time of discovery in January 2016).

A. Scale of Losses

It is impossible to accurately measure how much money ransomware victims have paid to attackers. Few victims disclose whether they have paid the ransom. Attackers rarely disclose how much money they have made and payments are difficult to trace since each infection usually has a unique crypto currency wallet [6]. Ransom payments are frequently siphoned through a chain of wallets and "tumbler" services before the attacker's cash out. However, some law enforcement agencies have published statistics that provide an insight in the scale of losses. The FBI has reported that it received more than 2,400 complaints regarding ransomware in 2015, with a reported loss of more than $24 million. This was up from 2014 when over 1,800 complaints were filed and losses were reported at $23 million.

B. The True Cost of an Attack

In early February 2016, the Hollywood Presbyterian Medical Center (HPMC) in the US was compromised with ransomware. The hospital admitted to paying the attackers' demand of US$17,000 to restore its systems, some of which provided access to patient medical records. However, $17,000 is likely a small fraction of the potential costs, both monetary and reputational, that an organization could incur for this type of incident. Some of the potential impacts that an organization could face after a ransomware attack include the following:

Downtime costs: Organizations may be forced to shut down systems to deal with the infection. Customers may be affected as the targeted organization's services may be impacted. Because of this downtime, the company could experience financial losses and reputational damage. In the case of utility companies, loss of power or water can potentially impact millions of people and may cause accidents leading to injury or, even worse, deaths.

Financial cost: Companies may have to pay for incident response and other security-related solutions in response to ransomware. Organizations could also be hit with large legal bills if customers are affected. Fines and other penalties may also apply. For example, US hospitals that violate the Health Insurance Portability and Accountability Act (HIPAA) can be charged up to $1 million.

Data loss: Loss of data due to files being encrypted and/or stolen can have a huge impact on businesses. The loss of company records, customers' personally identifiable information (PII), or intellectual property can significantly impact the organization's finances, brand, and reputation. The cybercriminals behind the attack may threaten to

publish stolen data online in an attempt to extort more money from the victim (we have already seen this tactic used by the authors of Chimera). Even if a victim pays the ransom and the cybercriminals decrypt the files, there is still a risk that data may be corrupted in the decryption process.

Loss of life: In the case of a hospital or other medical organization, patients' lives may be put at risk as essential medical equipment may be affected. Patient records including medical history may also be inaccessible, leading to delays in treatment or even incorrect medication being administered.

VI. PROTECTION AGAINST RANSOMWARE

Adopting a multilayered approach to security minimizes the chance of infection. There are number of organizations that have a strategy that protects against ransomware in three stages[6];:

A. Prevent
B. Contain
C. Respond

A. PREVENT

Preventing infection is by far the best outcome so it pays to pay attention to how infection can be prevented. Email and exploit kits are the most common infection vectors for ransomware. Adopting a robust defense against both these infection vectors will help reduce the risk of infection.

i. **Email Security**

Email-filtering services such as Symantec Email Security. Cloud can help to stop malicious emails before they reach users. Symantec Messaging Gateway's Disarm technology can also protect computers from this threat by removing malicious content from attached documents before they even reach the user. Email. Cloud technology includes Real Time Link Following (RTLF) which processes URLs present in attachments, not just in the body of emails. In addition to this, Email. Cloud has advanced capabilities to detect and block malicious JavaScript contained within emails through code analysis and emulation.

ii. **Intrusion Prevention**

Intrusion prevention system (IPS) technology can detect and block malicious traffic from exploit kit activity, preventing the installation of ransomware.

iii. **Exploit Protection**

Symantec exploit protection technology recognizes a range of malicious behaviors that are common in exploit attacks and blocks them from executing.

B. CONTAIN

In the event of an infection, a critical step is to limit the spread of the attack. Symantec's file-based technologies ensure that any payload downloaded on the computer will not be able to execute its routines. Symantec has a 24/7 Security Technology and Response (STAR) team responsible for ongoing development and improvement of generic signatures for ransomware. The team carries out continuous monitoring of ransomware families and their delivery chain in order to harvest new samples and ensure robust detection.

i. **Advanced Antivirus Engine**

Many IT companies uses an array of detection engines including an advanced signature-based antivirus engine with heuristics, just-in-time (JIT) memory-scanning, machine-learning engines and Malheur.

ii. **SONAR Behavior Engine**

SONAR is real-time behavior-based protection that blocks potentially malicious applications from running on the computer. It detects malware without requiring any specific detection signatures. SONAR uses heuristics, reputation data, and behavioral policies to detect emerging and unknown threats. SONAR can detect encryption behaviors common to ransomwar[6].

C. RESPOND

There are a number of steps organizations can take to ensure a speedy recovery from ransomware infections.

i. **Incident Response**

Symantec Incident Response (IR) can help organizations with responding to attacks and with making decisions on what to do next. Help identify the primary infector and contain further spread: Determining the primary attack is critical to understanding what the attacker's primary campaign is targeting and ensures that you aren't missing the actual attack by focusing solely on the ransomware.

Provide incident-specific recommendations to prevent success of future similar attacks: We can assist the customer with implementing controls to prevent any further outbreaks as well as assisting them to enhance their endpoint protection environment. In previous incidents, it has taken us as little as 72 hours to significantly improve the security environment at organizations who've been repeat victims of ransomware attacks. We can analyze the malware to determine how data was encrypted to help victims create a data recovery plan: In many cases, the malware writer makes mistakes in implementation that can be exploited by incident responders to recover data more easily.

VII. CONCLUSION

The advancement in ransomwares is going at a very high pace. With no apparent hurdle, it can become a crisis in few years. Ransomware can hit mobile devices and Internet of Things (IoT). The day is not far when ransom will become a major threat to Privacy and Personally Identifiable Information (PII) data. Criminals will not only encrypt the data but they will also exfiltrate a copy of data from our computers, mobile devices and (possibly) cloud storage. This data will be used to blackmail the users and collect ransom in periodic installments. Intelligent cars, automated homes, and personal wearables record every aspect of our life. Most of the users do not know that their hi-tech life is being recorded with accurate timestamps including all the secrets that we would protect at any cost. We need to understand the value of our personal data, realize the risk associated with it and actively devise ways to manage, track, monitor and secure personal data interactions and transactions.

REFERENCES

[1] Kharraz, W. Robertson, D. Balzarotti, L. Bilge and E. Kirda, "Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks", Detection of Intrusions and Malware, and Vulnerability Assessment, pp. 3-24, 2015.

[2] 2017. [Online]. Available: http://swdsi.org/swdsi08/paper/SWDSI%20Proceedings%20Paper%20S400.pdf. [Accessed: 16- Mar- 2017].

[3] N. Veerasamy and B. Taute, "Introduction to emerging threats and vulnerabilities to create user awareness", Researchspace.csir.co.za, 2017.[Online]. Available: http://researchspace.csir.co.za/dspace/handle/10204/3534. [Accessed: 16- Mar- 2017].

[4] A. Gazet, "Comparative analysis of various ransomware virii", Journal in Computer Virology, vol. 6, no. 1, pp. 77-90, 2008.

[5] "Awareness Education as the Key to Ransomware Prevention: Information Systems Security: Vol 16, No 4", Tandfonline.com, 2017. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/10658980701576412?journalCode=uiss19&. [Accessed: 16- Mar- 2017].

[6] "Cite a Website - Cite This For Me", Igi-global.com, 2017. [Online]. Available: http://www.igi-global.com/viewtitlesample.aspx?id=20635&ptid=479&t=Ransomware:%20A%20New%20Cyber%20Hijacking%20Threat%20to%20Enterprises. [Accessed: 16- Mar- 2017].

[7] "Ransomware: threat and response", Network Security, vol. 2016, no. 10, pp. 17-19, 2016.

[8] 2017. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf. [Accessed: 16- Mar- 2017].

[9] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge and E. Kirda, "Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks", Detection of Intrusions and Malware, and Vulnerability Assessment, pp. 3-24, 2015.

[10] M. Kasuya and K. Kono, "Screening Legitimate and Fake/Crude Antivirus Software", IPSJ Online Transactions, vol. 7, no. 0, pp. 43-51, 2014.

[11] "Ransomware claims more victims", Network Security, vol. 2016, no. 12, p. 2, 2016.

[12] "Ransomware - A Growing Enterprise Threat", Crowdstrike.com, 2017. [Online]. Available: https://www.crowdstrike.com/resources/white-papers/ransomware-white-paper/. [Accessed: 16- Mar- 2017].

[13] 2017. [Online]. Available: https://www.cise.ufl.edu/~traynor/papers/scaife-icdcs16.pdf. [Accessed: 16- Mar- 2017].

[14] 2017. [Online]. Available: https://assets.barracuda.com/assets/docs/dms/Best_Practices_for_Dealing_With_Phishing_and_Ransomware_-_Barracuda.pdf. [Accessed: 16- Mar- 2017].

[15] "Cite a Website - Cite This For Me", Swgfl.org.uk, 2017. [Online]. Available: http://swgfl.org.uk/magazine/NEW-ground-breaking-ransomware-protection-now-avai/Ransomware-White-Paper-October-2016.aspx. [Accessed: 16- Mar- 2017].