Ransomware Attack : India issues Red Alert

Simran Sabharwal
Computer Science and Engineering Department
Amity University, Uttar Pradesh
Noida, Uttar Pradesh, India

Dr. Shilpi Sharma
Computer Science and Engineering Department
Amity University, Uttar Pradesh
Noida, Uttar Pradesh, India

***Abstract*— WannaCry ransomware attack is the latest global cyber attack which usually strikes Microsoft Windows Operating systems and the payment is stipulated in the less traceable Bitcoin crypto currency. Business and Public Institutions have been one of the primary targets but the private individuals aren't unharmed now. The illegal activities come under the category of cybercrime. Ransomware, a type of Trojan virus, which like most computer viruses, often arrives in the form of a phishing email, or spam, or a fake software update – which infects the computer once the recipient clicks a link or opens an attachment, holds the computer captive by encrypting the data and demanding a ransom payment for decrypting everything.**

A cyber security firm Quick Heal Technologies reported that it has detected over 48,000 ransomware attack attempts in the country, with West Bengal witnessing the most incidents.

Ransomware attack is a breach of Right to personal liberty guaranteed under the Indian Constitution. It is an infringement of our Fundamental Right to Privacy covered under Article 21- *Right to Life* in Constitution of India. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 provides protection to personal information. Prior to these Rules, in India remedies for invasions of privacy exist under tort law and further the Supreme Court of India accorded limited constitutional recognition to the right to privacy (under Article 21).

India is a green field for cyber crime as ransomware does not come under the IT Act or under the Indian Penal Code. There is no national cyber security legislation that can elaborate the roles and responsibilities of stakeholders. As the threat has originated from beyond India, the investigations will end up at a dead end, In the present scenario where the cyber crimes are increasing to an alarming extent, the present need of the hour is to have broad-based convention dealing with criminal substantive law matters, criminal procedural questions as well as with international criminal law procedures and agreements. The IT Act, 2000 would be crippled without proper means and ways of implementing it.

Keywords*— *Ransomware Attack, Cyber Crime, Cyber Security, Crypto, Bitcoins, Malware attack, WannaCry

I. INTRODUCTION

In today's enterprises along with a keen peer competition in the business societies there are also an increasing number of sophisticated information security threats in the cyber world since business contracts and online presence are considered as a essential profit-driven alley and moreover as a necessary means for global competency.

The internet is facilitating business organizations to carry out business activities with great ease and this phenomenon has led organizations to store its critical business information on systems which are always connected to the internet. While individual users of personal computers are also no exceptions. Availability of high speed internet on mobile devices and laptops encourages individuals to keep their private information on mobile devices and laptops which might not be having adequate security. This wide spread and easily accessible internet systems have investigated that the malware programs such as Trojan Horse, worms, and spyware form a deluge of scientific viewpoints and different compatible strategies have been proposed to alleviate and expunge the cyber threats. [1]

Symantec experts studied a specific attack in more detail for a month and found that 2.9% of the compromised users paid ransom, allowing the offenders to likely earn $33,600 per day. It means the criminals would have easily made $394,000 in a month [2]. Thus the number of ransomware attacks have increased considerably.

Ransomware is primarily a sort of malware that makes the documents on a victim's computer remote and then demands the victim to pay a compensation (usually in the form of bitcoins) in order to attain access to the lost files [3]. This class of malware has existed for decades, but in recent years there has been a sharp hike in the number of such cases.

Widespread use in the recent years has caused loss of tens of millions of dollars in user losses every year[4]. Compounding to this predicament, an increasing number of law prosecution agencies have also been the victims of ransomware[5], [6] , losing valuable files and forcing such institutions to overlook their own instructions and pay the attackers.

The behavior of malware includes stealing data, sending credentials to attackers, and sending premium Short Message Services(SMSs) [7]. In order to conduct large scale attack and make profit from it, the malware developers tend to attack the Operating System with high market share. According to the article by the International Data Corporation (IDC) [8] , Android OS has monopolized the global smart phone Operating System Market with a 78% stake at the first quarter. Trojans also remain as the main mobile malware type. The Trend Labs Research reports predicted that in 2016, the number of threats will be more than twice of 2015.

II. LITERATURE REVIEW

The heinous AIDS Trojan [9] attack in 1990 was the first ever crypto ransomware attack. It was distributed through a disk handed over to the visitors at an international symposium about AIDS. The software first encrypted the file names from the system and then displayed a demand for ransom to a place in Panama. The perpetrator's motive was more of a reprisal on the conference organizers rather than monetary gains, but in any case the attack was indecisive since a program to restore the file names was soon published. But over the years the internet has made malware distribution uncomplicated. A few programs were available which used encryption to render a system counter productive and claim a ransom but were easily undone since they all used the same key for all encryptions and did not shield their keys well. Then in 1996, Adam Young and Moti Yung presented a paper [10] illustrating how to set up a exclusive encryption key for each system and then lodging it with a master public key enclosed in the virus software. The climax of their mechanism was that the infected machine did not need to interact with the enforcer until the ransom was paid.

Reference [11] concludes that the remediation speed by security teams around the world has been quite remarkable. Microsoft, at the same time released a patch which no longer backed Windows Server 2003, Windows 8 and Windows XP. Meanwhile, global security units hastened to patch the susceptible systems and shut the unprotected ports. While also the Recorded Future Intel Card for WannaCry are being reviewed so that we can promptly identify any associated IP addresses and hashes.

According to reference [12] patching is the most fundamental way to reduce cyber risk because it reduces the attack surface. If the AV has to defend against 1,000 vulnerabilities, it will be harder-pressed than if it has to defend against 10. However the companies should be patching this update and many others as quickly as possible, regardless of impact at this point. With the impact companies are seeing, if they do get infected, it’s better to update, plug the hole, and fix a broken application than to have your systems held for ransom.

According to the Kaspersky Lab's Global Research And Analysis Team, their System Watcher component has been quite essential in stopping these attacks. The System Watcher component has the dexterity to roll back the variations done by ransomware in the event that a pernicious sample manages to bypass the other defense setups. This is immensely helpful in case a ransomware sample slips past the defense and tries to encrypt the data on the disk. [13]

Reference [14] states that despite its capacity to proliferate so rapidly, the ransomware activities taken by the malware are not particularly novel. As discovered by security researcher Malware Tech and Talos, this malware was programmed to bail out upon a lucrative connection to that server, which would stop the malware altogether. We should all be obliged to Malware Tech for setting up the concavity, which caused this outbreak to slow down sooner than it otherwise would have.

This malware is easily modifiable. As mentioned above, other analysts are already finding variants in the wild. If you’re using Windows and haven’t patched yet, now is the high time to do it. And while you’re at it, make sure to test your backups to build some confidence that you won’t be forced at later stages to choose between paying up a ransom or losing data lest the worst happens to you or your organization.

According to Reference [15] the activity and the presence of two hardcoded IP addresses (192.168.56.20, 172.16.99.5) can be well used to identify the exploit using network encroachment prohibition systems. Server message block (SMB) packages also contain an encrypted payload, which dwells the exploit the shell code and the file launcher.dll. During the study, it was found that the malware is encrypted through a 4-byte XOR key, 0x45BF6313. As reported by many sources, the malware dropper contains code to check to two specific domains before executing its ransomware or the network exploit codes. Further more the WannaCry uses three Bitcoin wallets to receive payments from its victims. Looking at the payment activity for these wallets gives analysts an idea of how much money the attackers have made as of now. It has been estimated that the attackers have earned a little over BTC 15.44 (US$27,724.22). Although this is not much considering the number of infected machines, but these numbers are increasing and might become much higher in the coming days. According to the reports, multiple organizations across more than 90 countries have been impacted

Analyst Ian Johnston stressed it was “very important” to realize that the actions taken so far only stopped one sample of the ransomware. But there is nothing stopping them from erasing the domain check and attempting again, so it’s especially crucial that any unpatched system is patched as swiftly as possible. [16]

According to reference [17] cyber-extortion methods can be etched back to the late 1980s. However a modern wave of ransomware attacks began in 2005, it is a kind of malicious software (malware) that attackers are spreading with the intention of not just wrecking data as was done by the traditional attacks; but encrypting and charging ransom for the services to recover the data. Ransomware is a form of scareware that is the user is forced to pay the ransom in response to fear of losing their data. The manifestation of this type of malware is on a hike. It is a fruitful business model for the criminal organizations that set up these outbreaks. Payment is generally done via bitcoin, with appeals in the zone of 500 — 1000 USD. This supposedly ‘nominal’ price is set to hike as time goes on, making it look alluring to pay at the earlier stages. This is a remunerative business for the cyber criminals, certain computations suggest that a approximate figure of 200 million USD annually is extorted by the criminal groups. Opinion is often given not to pay the ransom, as this supports the criminal biz model, however it may be the only way to retrieve the lost data.

Ransomware is one of the blooming cyber threats which has attained attention and thinking in the recent years. It is a malware that swindlers attempt to install on your computer and use a variety of lock-out mechanisms to prevent you access to your computer data. It then forces you to pay certain amount of money to restore the functionality of your system. Sometimes the lock out message is displayed to be from the local law authorities stating that you have committed a crime like child pornography or unauthorized access to copyrighted information, forcing you to pay fine or else you are threatened to imprisonment.

Many of the novice users pay in fear of losing their valuable information and data. But it rarely happens that the attacker restore functionality of the system as per their promise. It is found to be a profitable activity for attackers.

Symantec experts have studied a specific attack in detail for a month and found that 2.9 percent of the compromised users paid ransom, enabling the criminals to potentially earn $33, 600 on a single day. It means criminals could have easily made $394,000 in a month. Thus the number of Ransomware attacks have increased considerably. Though with progresses made in the field of cyber security, the Ransomware attacks are found to be declining this year, its serious damage cannot be neglected. [18]

According to reference [19] malware is a threat that will always surround technology. What started out as software to just brake or make a system stop working, which had caused an inconvenience for the end users. Now it has become a lucrative business for criminals to collect personal information, and hold that information at stake for money. It comes down to a cat and mouse game to try to stop your personal data from becoming compromised and being stolen. While there is no 100% effective way to stop ransom-ware, steps can be taken to deter cyber criminals from deploying ransom-ware attacks. Malware can be prevented if the end users have a good understanding and take steps to protect themselves while online. Educating individuals in cyber security can be one of the best investments in stopping the spread of malware within an organization. Setting up security policies that can detect and stop ransom-ware from running and ruining their data, and developing new techniques on analyzing the potential threats that come from malwares, can give the users the confidence that the integrity of their data is not going to be compromised. Malware is like the flu it would always be around, but with education and steps to ensure network security, damages from malware can become more as an inconvenience rather than a catastrophe.

While precise details of how these ransomware outbreaks began are not well known, they often start when a user is misled into clicking a link or opening an attachment of some virulent email. A Software that is contemplated to damage or wreck the computer is then downloaded to the user's computer axiomatically, and it rapidly encrypts all of the data on that system and likely spreads out over the web to encrypt data on other machines as well, thus rendering all data unavailable. The victim is then presented a message reporting that all the files have been encrypted, and if they are unable to pay the demanded ransom amount within a short span of time, all the data would be lost.

Once an invasion has been launched, users have three primary options:

1) try to recover their lost data from a backup
2) pay the ransom amount
3) surrender their data to the attackers

Many users pay out the ransom amount due to fear of losing their data but yet are not easily handed over their data back. Thus organizations need to make efforts and generate awareness to prevent these attacks and recover quickly in case such a thing happens. [20]

According to Krishna Chinthapalli, a neurology registrar [21] the number of ransomware attacks have rose fourfold from 2015 to 2016, and so has the amount of money paid to hackers, to $1bn, according to the FBI. In the UK, a third of NHS trusts have reported a malware attack. Hospitals are the ideal targets for these companies. These hospitals have irreplaceable medico legal records and data for an increasing number of day to day functions, from patients' appointments to viewing imaging and reports. Hospitals are more likely than other organizations to pay for quick recovery of their data.

Hospitals and their workers need to maintain Digital hygiene— that is, keeping hardware and software as secure as possible. This includes employees becoming less "click happy" when reading emails and Frequent backups are also equally important. They can also use tape drives, which cannot be hacked digitally.

In other words ransomware is a classification of malware that possesses some digital assets from its victims and asks for restitution in the form of bitcoins for the release of their assets. Ransomware attacks were first witnessed in Russia in 2005–2006 and since then have largely changed their tricks and spots. The most recent upsurge of ransomware attacks is coveting targets in a very peculiar way—tracking their geographic locations and petrifying them with a hoax that fakes their respective countries' police forces while holding their whole system and data incommunicado. These attacks are known as the "Police Trojan" attacks. The social networking scam in this case is purporting as their local police force and informing the victim that his computer is suspicious of illegal activities and thus need to pay a ransom in order to re use it.

This phenomenon is becoming a portent landscape rather than a single detached malware incident. As the business model of ransomware attacks improves and that of fake antiviruses worsens, more criminal groups are rising on board.

Once the victim pool becomes too cognizant of this trap, the cybercriminals would most probably switch to a different trick.

Although technically, the Trojan is not very progressive, it has certain evident and interesting features. Most essentially, it has been drafted to be onerous to remove. Some variants cannot be handily uninstalled even on safe booting the computer. [22]

Reference [23] outlines a spectrum of budding challenges that the regulators and law imposition agencies would need to keep in mind. Key areas singled out include framework risks, the use of wireless and mobile technologies, more sophisticated malware, new identification and payment systems, computer facilitated frauds, exploitation of younger persons, cerebral property invasion, and industrial tailing. Successful prosecution and relevant punishments for these crimes would require apt policing and on-going jurisdictive amendments.

There is no single all-enveloping solution to responding to such technology aided crimes. Retaliating these perils is a multi-dimensional threat and requires competent coordination and synergic efforts on the part of a large range of government, law makers and the private sector objects. Possible briefing for action can include alluring the ICT security industry in the scheme of safe software and hardware and endowing task forces committed to the investigation and pursuit of technology-enabled scandal cases and further more upgrading the training and educational efficiency of police, prosecutors and IT professionals.

As the ICT sector continues to boost, there will be a upsurge in the opportunities for offenders to act illicitly. Serious and legitimate concerns exist about the ways in which modern technologies are likely to be exploited in the years to come. Technology-enabled scandals already range across a immense spectrum of activities. These include crimes that concern breaches of personal or corporate isolation, crimes committed by individuals that purposely modify the data within corporations or government firms for profit, personal or political motives, and crimes that engage attempts to rattle the operation of the internet.

Kaspersky, one of the prominent antivirus company has warned that ransomware is a severe menace, because there is no secure way to restore the encrypted data. Ransomware can thus be defined as a piece of noxious software that escapades a user's computer vulnerabilities to creep into the victim's system and encrypt all his/her files; then the attacker keeps the files sealed unless the victim agrees to pay the ransom. During a typical attack, the attacker gets into the compromised computer by probing his exposed system amenabilities. If the system was attacked previously by a worm or Trojan, the attacker can easily get into the weakly configured computer. Attackers then look for various types of decisive files with extension names such as .txt, .doc, .rft, .ppt, .chm, .cpp, .asm, .db, .db1, .dbx, .cgi, .dsw, .gzip, .zip, .jpg, .key, .mdb, .pgp .pdf. Knowing that these files are of supposedly pivotal importance to the victims, he then encrypts these files, making them difficult for the victim to access. Later, the traducer sends the victim an e-mail ransom or pop-up window making demand for the ransom that would decipher the frozen files. Probing system vulnerabilities, ransomware unfailingly tries to take control over the victim's files or computer till the victim acepts the attacker's demands, usually by transferring funds in the form of bitcoins to the christened online currency accounts such as eGold or Webmoney stores. The future attacks would presumably result from combining strong cryptanalysis with malware to raid information systems.[24]

III. EXPERIMENTAL

The research objectives have been postulated by analyzing the literature, the outcomes of various surveys and their corresponding results. The literature review focused on the development, transfer and mitigation methods of ransomware and the analysis of latest trends in criminology mindsets. Further the survey was validated with research papers written by renowned professionals.

The methodology followed in the same can be divide into 3 steps:

A. Survey And Interview Conduct

The first round of interview provided insights and inputs, which were used to finalize the survey questions to be questioned. Then, using social idea as the control group, volunteers were asked to anonymously fill out surveys, which included both victims and non-victims groups. Of these volunteers, their perceptions and views were recorded , along with their awareness and initial reactions to ransomware. A number of different mediums were used in an attempt to maximize the speed of the survey.

B. Maintaining The Integrity of The Specifications

The researches done on various mitigation strategies were combined with insights gained from relevant literature about ransomware delivery and mitigation methods. The demographic features like age, gender, level of education were studied explicitly to understand their dependence on the type of mitigation strategies, awareness and the losses expected or incurred. The questions were so designed to maintain the confidentiality of the information entered. The interviewees evaluated the survey and on the basis of their response, a modified survey was designed.

C. Scrutiny of the Survey Result

The survey results were inspected using statistical reasoning of all the variables affecting "LOSSES INCURRED". The co-dependence of the independent variables (for example, 'the type of delivery method' used and the 'type of company') is used to recommend some measures to control ransomware delivery and losses incurred during the same. These socio-demographics are chosen on the basis of literature recommendations. [25] This aims to help in recommendation for mitigation of ransomware or reducing losses by controlling or affecting the parameters with higher dependence.

IV. ANALYSIS

The malware analysis and detection methods can be classified into the following three categories:
→Static Analysis Method
→Dynamic Analysis Method
→Hybrid Approaches
Since most of the methods only detect ordinary malware which do not use variant techniques, recent researches have proposed several advanced detection techniques to improve the accuracy in malware detection. Following are the detection algorithms for malware variants:

1. Static Analysis

This approach includes the signature based, permit based and element based analysis. The signature based mechanism extracts the semantic arrangements or features [26] and creates a exclusive signature corresponding to a specific malware. Thus, it fails to detect the variant or unknown malware. While the permission-based method identifies dangerous permission requests to detect malware. The element based method dismantles the APP excerpt and analyzes the definition and byte code synergy elements to identify the vulnerabilities. [27] [28] [29].

2. Dynamic Analysis

In this technique, applications are set up and accomplished on an adversary or a controlled device to diagnose malicious behaviors. [30]
This manner models users' behavior and provides human-like inputs. Using this method directly in the devices may cause resource consumption.

3. *Hybrid Approaches*

They average the advantage of the static and dynamic analysis schemes both.

V. STAGES OF A RANSOMWARE ATTACK

The Ransomware threats have a variety of approaches to attack systems. However, there are common phases of ransomware in most of the processes. Ransomware is automated rather than receiving instructions from the host machine, infecting the system in a stealth mode. The major steps of a ransomware attacks have been broken down into major phases such as:

1. Campaign And Distribution

This is the first stage where ransomware attempts to deceive the victims to download and run attachments by using social engineering or pushing the users to visit weaponized websites, which lead the process to infection process.

2. Infection And Staging Process

In this step the file initializes an installation process in the system by itself. However, the executable files set key functions in the windows registry files in order to be efficient after the system reboot and file recovery. Also, the ransomware establishes connection with a random server, or C2 server from TOR or Dark net to communicate with the hacker's infrastructure, which is quite useful in sending back the information about infected machines. Last but not the least, these files attempt to delete the shadow copy files from the windows systems.

3. Scanning and Searching For Contents

In this stage the ransomware has already been installed and it starts to look for files, and documents both locally and from the network. However, many ransomware attacks prioritize network shares over local drivers. During the scanning process the ransomware codes leave some sort of notes from the files and directories. Moreover, it searches both mapped and unmapped network accessible systems over the networked areas for documents and shared files.

4. Encryption Process

This step is considered as one of the most challenging part, where in ransomware begins to encrypt all the files, which have been discovered during scanning process by using the encryption methods such as AES, and RSA. In the initial stages, the ransomware files check the PHP proxy server to start the encrypting process and in some cases the ransomware encrypts both the extensions and content of the file. However, it deletes copies of the original files immediately. During this process, the ransomware starts to establish new connections in C2 server on the TOR network in order to get more information from the hackers and send back encryption keys for the damaged files. In addition, the connections can be used for some other purposes such as sending the instructions for the victim, and navigating them as to how to get access back to their encrypted files.

5. Payday

After the attacked machine has been infected and the data has been encrypted, hackers then force the victims to pay the ransom within a stipulated period of time to restore their data. In most of the attacks victims are usually provided with instructions to pay the ransom by sending links or locking the screens in order to get the decryption keys. The digital currency used to pay ransom is called 'BITCOINS', where each bitcoin costs about 150 USD.

VI. RESULTS AND DISCUSSIONS

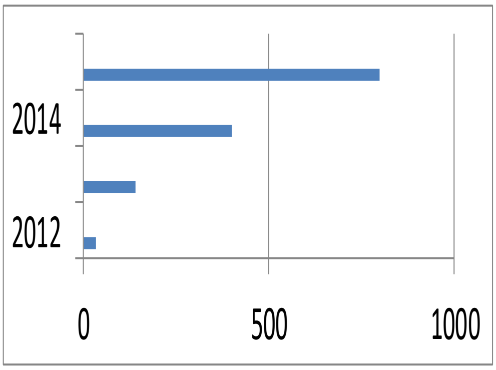
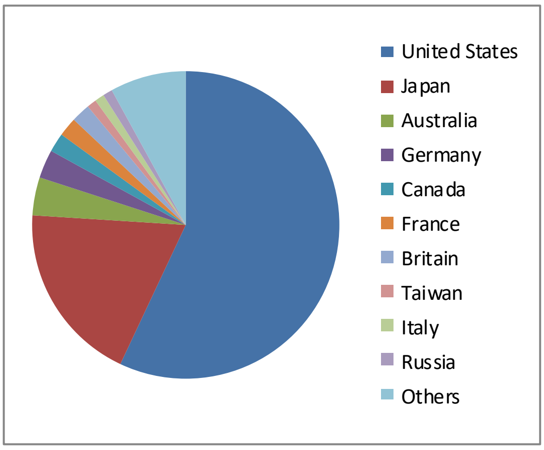


Fig 1: Graph depicting the number of threats between 2012-2015

The above graph (fig.1) is a depiction of cases the number of threats between 2012-2015. While there were observed 35% of ransomware attack in 2012 , it splurged over the years and rose to 800% by 2015. The number of threats doubled from the year 2014 to 2015. [31]

Fig 2: Pie chart depicting the ratio of countires effected by randomware.



The pie in the fig.2 indicates the country most affected by ransomware attacks in the year 2016. The United States, which is the most developed country in terms of computer infrastructures and is a home to most of the high end companies has been the most affected country giving people losses of data worth billions of dollars. Next most affected country is the Asian Country Japan. While on the other hand countries like Russia, Italy and Taiwan have been the least affected among the major countries.[32]

Malware examination is offered through a cloud service. It has built-in advantages of using pay-as-you-use services functioning over virtual platforms over the internet with world wide reach anywhere subordinately and not having to fear about any thing in house breach over the regional network attacking users and IT servers alike.

Cloud Infrastructure offers a upper hand of not being narrowed by the hardware or computing power, thus enabling highly scalable setup. This type of frame work related composition helps present anti malware services when enforced over periods of time, indicating and evaluating huge database and malware logs.

In addition to this, the service can be made customizable for the end users by equipping them the capacity to upload and amend logs/executable and even capture images of the infected systems. The geek users can also be offered a virtual test bed to perform their own lab analysis.

Another advantage with this system is its capability to apprise each user as soon as a new malicious payload is encountered.

VII. SUMMARY AND CONCLUSION

The paper has been designed as a assessment model based on social engineering methods to restrict ransomwares. In order to protect one's data from a ransomware attack, it is required to make pre-detection, rather than post-detection.

Nowadays, cyberattacks have been going global and have affected variety of organizations and end point users. While, hackers use different approaches and tools including ransomware threats to take control over the targeted systems which would eventually lead to a huge damage such as in business, healthcare system, industry sector, and other fields. "Ransomware is on track to be a $1 Billion crime in 2016. Also, over twenty-five variants of ransomware families have been identified and over four-thousand ransomware attacks happen on a daily basis since January 1, 2016. While ransomware isn't going away any time soon, you can surely defend yourself and your organization against it – if you are well prepared. "Under the light of this idea, we work to understand the common forms of ransomware threats: identifying the root and types of ransomware and also diagnosing effective types over different platforms. Also, how ransomware works in the systems and possible changes which can be made by ransomware.

Ransomware has become a lubricative business for cyber criminals over the course of time. The majority of countries that are a part of G20 have been hit by ransomware. New technological perils such as IoT and the hike in the wearable market demand has granted cyber criminals to target new areas with ransomware. It has demonstrated that attention to security is the prime thing in the present scenario. Combating ransomware is a challenge and all of us have to play a part in it. While intriguing, creating new technologies and products, considering that the normal use cases is not sufficient any longer. The primary challenge for product designers is to enhance security and by taking malicious activities and scenarios into deliberation. We need to train ourselves in the basic security practices to protect our data, such as avoiding to click on malicious links or attachments and patching credulous software vulnerabilities. We need to attain more knowledge about the threats of ransomware and correspondingly take steps to prepare for and curtail hazards from these attacks.

VIII. FUTURE STUDI ES

In today's world we are online and always connected through the internet. In the past threat from malware attacks was specifically limited to desktops and laptops. But now with the advent of mobile phones there is a urgent need that we start looking at these devices and how they might pose a threat to the security of our data. Watches too can now easily link to our smart phones over WiFi and Bluetooth networks and homes are becoming more integrated with technology. While most of these smart devices hold very less data and a factory restore would easily fix the infected part. But smartphones are becoming our all in one devices which store all our data from our pictures to credit card information and bank details. A highlight for the future studies would be to analyze how vulnerable are these devices to grant an attacker a back door into the system. The future that technology holds would enable us to get any information at the blink of an eye, but there is always a threat of the system getting infected and the data getting lost. [33]

IX. REFERENCES

[1] Thakkar, Samir. "Ransomware-Exploring the Electronic form of Extortion."

[2] Kharraz, Amin, et al. "Cutting the gordian knot: A look under the hood of ransomware attacks." International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Springer, Cham, 2015.

[3] Kelion, L. "Cryptolocker ransomware has infected about 250000 pcs." BBC, 12/2013 (2013).

[4] O'Gorman, Gavin, and Geoff McDonald. Ransomware: A growing menace. Symantec Corporation, 2012.

[5] Scaife, Nolen, et al. "Cryptolock (and drop it): stopping ransomware attacks on user data." Distributed Computing Systems (ICDCS), 2016 IEEE 36th International Conference on. IEEE, 2016.

[6] Fraga, Brian. "Swansea police pay $750" ransom" after computer virus strikes.[En línea] 15 de noviembre de 2013.[Citado el: 15 de diciembre de 2013.]."

[7] Ramu, Srikanth. "Mobile malware evolution, detection and defense." EECE 571B, term survey paper (2012).

[8] Song, Sanggeun, Bongjoon Kim, and Sangjun Lee. "The effective ransomware prevention technique using process monitoring on android platform." Mobile Information Systems 2016 (2016).

[9] Laffan, K. "A Brief History of Ransomware." Varonis (2015).

[10] Young, Adam, and Moti Yung. "Cryptovirology: Extortion-based security threats and countermeasures." Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on. IEEE, 1996.

[11] McCartney, Margaret. "Margaret McCartney: The NHS needs big, firm IT pants." *BMJ* 357 (2017): j2352.

[12] Sittig, Dean F., and Hardeep Singh. "A Socio-Technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks." *Applied Clinical Informatics* 7.2 (2016): 624–632. *PMC*. Web. 28 July 2017.

[13] Seshagiri, Prabhu, Anu Vazhayil, and Padmamala Sriram. "AMA: Static code analysis of web page for the detection of malicious scripts." *Procedia Computer Science* 93 (2016): 768-773

[14] Hass, Aida, Chris Moloney, and William J. Chambliss. *Criminology: Connecting Theory, Research and Practice*. Taylor & Francis, 2016.

[15] PATYAL, MANVEER, et al. "Multi-layered defense architecture against ransomware."

[16] Bradshaw, Samantha. "Combating Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity." (2015).

[17] Moore, Chris. "Detecting Ransomware with Honeypot Techniques." *Cybersecurity and Cyberforensics Conference (CCC), 2016*. IEEE, 2016.

[18] Thakkar, Samir. "Ransomware-Exploring the Electronic form of Extortion."

[19] Wilson, James, and Follow Following Unfollow James Wilson. "RANSOMWARE: Extortion Through Malware."

[20] Sittig, Dean F., and Hardeep Singh. "A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks." *Applied clinical informatics* 7.2 (2016): 624.

[21] Chinthapalli, Krishna. "The hackers holding hospitals to ransom." *BMJ* 357 (2017): j2214.

[22] Sancho, David. *Police ransomware update*. Technical report, Trend Micro Incorporated, 2012.

[23] Choo, Kim-Kwang Raymond, et al. *Future directions in technology-enabled crime: 2007-09*. Canberra: Australian Institute of Criminology, 2007.

[24] Luo, Xin, and Qinyu Liao. "Awareness education as the key to ransomware prevention." *Information Systems Security* 16.4 (2007): 195-202.

[25] Giri, Babu Nath, Nitin Jyoti, and McAfee AVERT. "The Emergence of Ransomware." 9th Annual Association of anti-Virus Asia Researchers (AVAR) International Conference–Digital Security: Prevention to Prosecution. Auckland, NZ. 2006.

[26] Feng, Yu, et al. "Apposcopy: Semantics-based detection of android malware through static analysis." Proceedings of the 22nd ACM SIGSOFT International Symposium on Foundations of Software Engineering. ACM, 2014.

[27] Fuchs, Adam P., Avik Chaudhuri, and Jeffrey S. Foster. Scandroid: Automated security certification of android. 2009.

[28] Lu, Long, et al. "Chex: statically vetting android apps for component hijacking vulnerabilities." Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012.

[29] Chin, Erika, et al. "Analyzing inter-application communication in Android." Proceedings of the 9th international conference on Mobile systems, applications, and services. ACM, 2011.

[30] Suarez-Tangil, Guillermo, et al. "Evolution, detection and analysis of malware for smart devices." IEEE Communications Surveys & Tutorials 16.2 (2014): 961-987.

[31] Hsieh, Wan-Chen, Chuan-Chi Wu, and Yung-Wei Kao. "A study of android malware detection technology evolution." Security Technology (ICCST), 2015 International Carnahan Conference on. IEEE, 2015.

[32] Hsieh, Wan-Chen, Chuan-Chi Wu, and Yung-Wei Kao. "A study of android malware detection technology evolution." Security Technology (ICCST), 2015 International Carnahan Conference on. IEEE, 2015.

[33] Wilson, James, and Follow Following Unfollow James Wilson. "RANSOMWARE: Extortion Through Malware."