THINK INDIA JOURNAL

ISSN:0971-1260

Vol-22- Issue-14-December-2019

A Brief Study On - Ransom Ware

Saqlain Loladia(Student)saqlainloladia@gmail.com

Gaurav Singh(Student)gaurav.singh77722@gmail.com

Mithila Chavan(Assistant Prof.)Mithila.satam@vsit.edu.in

Vidyalankar School of Information Technology

Wadala(E), Mumbai-400037

Abstract

The word itself is enough to mark its importance in the market.Yes,very rightly your data is caught for few dollars and the attacks behind it is nothing but Ransomware. Ransomware a malware designed to prevent access to the system until an attractive ransom is paid. This malware encrypts files and holds them hostage and can only be unlocked by certain decryption key until an amount is paid mostly in cryptocurrency, as cryptocurrency is entertained by cybercriminal/fraudsters. Ransomware works incognito it can do almost all the work without even contacting the fraudster through the internet, even if it does it uses encrypted channels for communicating with their controllers. This paper will discuss about its existence in the market,its presence in multiple fields like a corporate,small scale to large scale business and methods for Prevention, Detection, and Reaction.

Keywords: - *Cryptography, Cryptocurrency, C&C server, Intrusion Detection, Honeypot, Malware Phishing, Spamming WannaCry, BadRabbit.*

ISSN:0971-1260

Vol-22- Issue-14-December-2019

Ransomware

Introduction

In a world of digitalization, there are possibilities for data and security breaches. Such breaches are the result of different types of malware that include computer viruses, worms, trojan, spyware, etc. Ransomware is a type of malware that restricts the user from accessing their data. Here the data access is restricted by encrypting the data.

Ransomware is a Malware(Malware is an abbreviation for Malicious Software) made by Cybercriminals to exploit the device and extract resources. Data access is restricted by encrypting the data. Some ransomware is just for display while some are lethal threats. Phishing sites are mostly used for spreading Malware. Ransomware generates over 25 million dollars in revenue for hackers each year, the total damage cost predicted for 2021 is 20 billion dollars. There are two types of ransomware malware that are Lock Based Ransomware Malware and the other one is Crypto Based Ransomware.

There are many numbers of ways through ransomware malware that can be deployed into your computer and gain access. The most common among them is phishing spam. Phishing spam is sending an attachment to the victim(s) in an email, disguised as some kind of file that the victim will download it and open it. Once the malware containing attachment is opened it will take over the victim's computer and gain access.

Origin

Origin of the Ransomware dates back to 1989 even before the Internet was found. It was known by the name 1989 AIDS Trojan later also gaining the name PS Cyborg. Joseph L. Popp, a biologist who had been trained at Harvard targeted The World Health Organization's international AIDS conference infecting 20,000 floppy disks forcing users to pay up to 189$

ISSN:0971-1260

Vol-22- Issue-14-December-2019

to gain access to their data. The culprit was caught and decryption tools were used to recover the locked information.

Locker Based Ransomware

Lock-based Ransomware locks you out of your computer i.e. encrypts your data and prevents accessing the data. Locker Ransomware Malware has a specific type through that it can be identified, the message displayed by Locker Ransomware is like “This is the Police, and you have been penalized because of illegal activities like piracy”, and then ask for a penalty or one can call it ransom. It was first posted on the internet on 5th September 2013. It targets users with Microsoft Window Operating System. The downloader that produces this is installed as a Windows service with a random filename.

Working

After gaining access to the computer this malware will scan the computer for important files and or all of them. Once the Malware has found the files it will encrypt those files and prevent the Computer’s OS and application from running as well as prevents the user from accessing anything. Mostly in this type of malware, the whole computer is encrypted or one can say locked. After the computer is encrypted the Ransomware malware will take hold of the computer and will restrict anything and everything in the computer and the users as well as from accessing it or doing anything. This file cannot be decrypted without a key, that is known to the attacker. After the encryption is done the user is presented with a certain type of message that claims that they are the law enforcement agency, and will blame the user for doing illegal activities like piracy, child pornography and many more, and demand the payment of a "fine" to scare the victim so that he doesn't report to the authorities, and this payment is done through cryptocurrency, steps of paying the ransom is listed in the message.

ISSN:0971-1260

Vol-22- Issue-14-December-2019

Crypto Based Ransomware

This Malware doesn't act, it will directly display the Note that you have been affected by the Malware, and if you want your data you must pay the ransom. The method of paying Ransom is in Cryptocurrency as it is hard to track. This Malware is more successful than the Locker one is because this Malware restricts everything from the device, and it spreads like a virus and affected other devices as well.

Crypto-based Ransomware's Working

Crypto-based ransomware is related to lock-based ransomware but it is more radical.

In Crypto-based Ransomware, the malware will gain access to the computer, and in the background, it will start the search for essential documents that can be used for money

ISSN:0971-1260

Vol-22- Issue-14-December-2019

extortion. Once it gains all the important files the Ransomware malware will encrypt all of your important files to gain access u will need a decryption key to unlock this. Once the encryption is done then it will take over the victim's computer and will show it's true colors. The malware will display a text to the user directly saying that it is his\her computer has been affected and to unlock this one must pay the ransomware, many malware has a timer on it if not paid in the limited time the amount will be increased or the data will be lost entirely, and while some of the ransomware malware threats the user that they will publicize the data and nobody wants their private data on the internet, the tactic used is Shock and Fear tactics.

The hackers display in the text what must the victim do if they want to pay the ransom, the method of payment is cryptography thus having the name Crypto-based Ransomware. Cryptocurrency is used by cybercriminals as it is tough to trace. Crypto ransomware can sometimes work without any use of communication with the attacker but some malware communicates with the attacker through URL.

ISSN:0971-1260

Vol-22- Issue-14-December-2019

C&C server

The URL that attackers use is the C&C server, it is necessary for the attacker to keep this confidential that is he will make sure that the location of these servers stays undetectable. To keep this confidentiality newer generation ransomware attacks are made via encrypted HTTPs protocol or the Tor network. The use of completely encrypted channels such as Tor and HTTPs makes the creation of the signature of the attack in advance impossible. But Tor network is not used for attacks of large scales as it can be detected by IPS and IDS devices. In addition to that, C&C servers use Dynamic DNS service, which allows a different IP address assignment by the ISP to a domain after a certain value.

Encryption Method

The ransomware uses many encryption algorithms that vary from RC4 to RSA+AES and ECDH+AES. While the attackers used only symmetric encryption methods with the advent of the ransomware threat, they now prefer the use of a hybrid encryption mechanism, which utilizes both symmetric and asymmetric encryption methods.

Nowadays newer generation of ransomware malware only sends the public key to the infected machine as shown in the image above. The cryptographic key created from the server and the private key that is never let out from the server. Therefore once affected, that device is gone for.

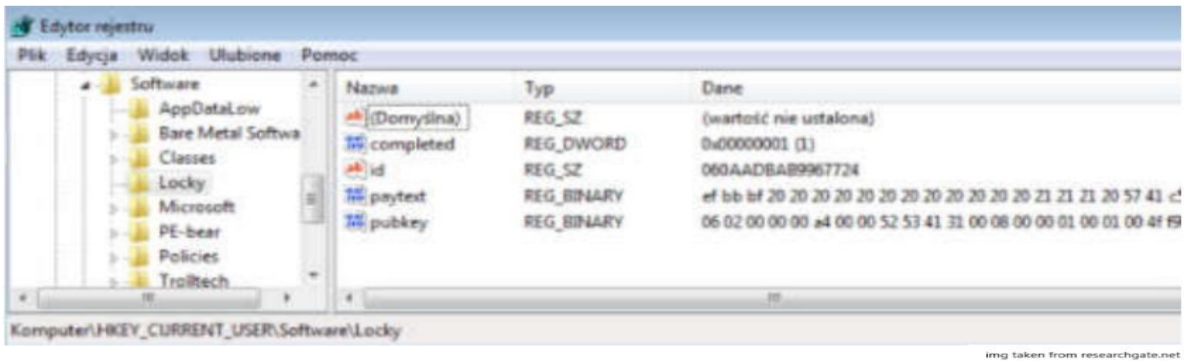


Figure 2.3: The image of Locky ransomware in registry.

ISSN:0971-1260

Vol-22- Issue-14-December-2019

Detection

The detection of malware is extremely critical. No matter what level of protection of system has it can be compromised with a greater level of motivation and skills. There is no "Knight in Shining armor" in Cybersecurity. A defense mechanism should be employed that when penetrated warns the sounds an alarm. There are many tools available for detection of ransomware, for example, Bitdefender Anti-Ransomware Tool is a component of Bitdefender Antivirus Plus, this was designed to stop the infection from your computer that is by not letting it through any network kind of isolating the device. This tool work on Machine learning which allows it to discover the pattern of the ransomware and identify it. The Bitdefender Antivirus plus fools the Ransomware malware by making your computer files appear as they have already been affected, because of this it will save your files from another encryption that you won't be able to decrypt.

Cyber sight, Ransom Stopper is also a type of anti-ransomware malware protection this one is a free stand-alone product that helps to detect existing and new ransomware malware and stop further actions, and more Anti-ransomware Malware like Trend Micro RansomBuster, Check Point Zone Alarm, Crypto Drop, etc.

Detection Methods

The classification of three algorithms that are used in the detection of Ransomware, Random Forest, Decision Trees (J-48), and Naive Bayes. These algorithms are selected based upon their suitability and better performance for general malware classification. However, in cases where complex obfuscation and packing techniques are used, simple static analysis may not be able to extract all the required features. It is required to apply the anomaly-based analysis technique as well to detect malicious functionalities of ransomware.

ISSN:0971-1260

Vol-22- Issue-14-December-2019

Static-based detection

Detection of ransomware malware based on static based analysis is analyzing the application's code before its execution to determine if it is capable of any malicious content, if found any then it will be stopped from launching. Signature Based detection depends on specific patterns such as byte sequences in network traffic, or known malicious instruction sequences used by malware.

Signature-based ransomware detection methods only detect that malware whose signature is previously stored in the database, i.e. it will fail to detect a new, previously unseen threat. Thus this method is not reliable, as signature stored in the database is only based on regular expressions and string matching.

Anomaly-based detection.

In an Anomaly-based detection method, it is important to know whether the software is harmful or not. This Anomaly-based detection method was made to detect unknown attacks. Rule sets are used to determine when the software has established gentle, kind and valid behavior. the drawback of this method is defining its rule sets. But it will keep on working as long as the rule sets are well defined before.

What Anomaly-based Detection does is it uses Machine learning to create a pattern that is trusted by the anti-malware after the pattern is constructed then it compares new behaviors against this model, as these models can be programmed according to the application and hardware configurations machine learning-based method has more probability of working efficiently then signature-based detection.

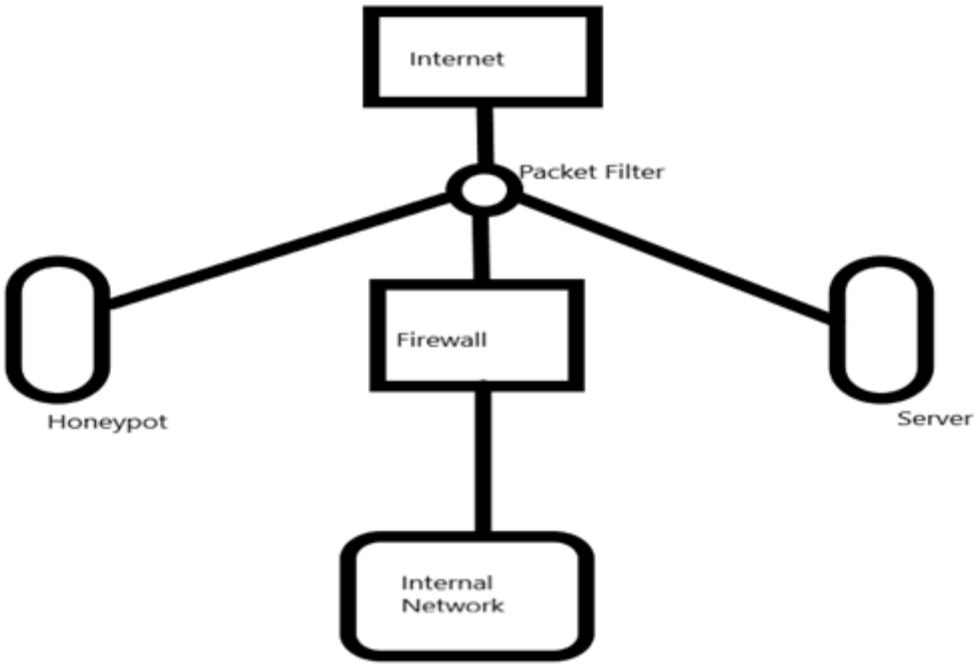
The efficient selection of algorithms makes the classification process used in anomaly-based detection method more reliable.

ISSN:0971-1260

Vol-22- Issue-14-December-2019

Honeypot

Honeypot is a method in which u set up decoy files for the ransomware to attack. honeypot creates a trap for the malicious software to attack, honeypot makes safety alarms disguised as important documents and waits for the malicious software to attack this files once these files are attacked, it will ring the alarm that your device has a malware inside it and then further actions must be taken.



Prevention and Action

There are a number of ways to protect your system from Ransomware. It is essential to follow these methods if you want to protect your system from getting infected by Ransomware.

First and foremost one should always **keep a backup**, if any backup is present one can roll back to there backup thus saving money, time and effort, not giving to the attackers will is the

ISSN:0971-1260

Vol-22- Issue-14-December-2019

key. **Keeping your devices up-to-date**, keeping one's device up-to-date nowadays is an important issue at hand as any company won't like if their customers face any inconvenience with their cyber-security, thus well-known company keeps updating their software and watches out for loopholes, bugs, serious threats and etc. **Having a good antivirus,** antimalware for countering is a great idea, nowadays windows have this security system and help protect one's device by detection and stopping the Ransomware Malware of any kind of malware.**System restore** or recovery points are like backups but it restores every setting, so if u are attacked by some serious malware then format that particular pc and restore it using the recovery points. Make sure your firewall is on as it helps filters websites that might be shady and contains malware in it.

This malware can also spread through emails. Emails from unknown senders can contain links to websites that can inject malware into your system. You need to make sure that you don't click on the links inside the emails from unknown senders. **Frequent scans** of the device can help you detect the problems that are inside the system, one must do a full scan frequently. **Restricting permissions to users and application.** Restricting access to things they don't need is a great idea to protect the device, and some applications can make changes in your system without your permission so restricting permission takes care of this as well.

After getting infected it is difficult if not impossible to recover your data. First and the most crucial step is to **isolate the infected device.** Restrict any and every type of contact with any other devices or network so that it won't spread. Second **report the authorities** that can deal with that particular problem at hand as this has to be taken care of on a higher level as it is a serious cybercrime. If there is no possible solution then you can always **erase everything** and start from scratch if the stolen data is not that important. Try finding those **restore points** if you had created them in the first place if not then you will have to **rely on your backup**.

ISSN:0971-1260

Vol-22- Issue-14-December-2019

One should try using antivirus/antimalware but the chances of antivirus working after the device are affected is less than the antivirus ruining the whole goddamn thing, as in many cases antivirus conflicts with the malware and causes for the whole device to be inoperable.

WannaCry:

Image taken from hypenet.com

WannaCry is a type of ransomware that affected organizations worldwide in around 150 countries including Russia, China, the USA and almost all of Europe. In May 2017, initially, it struck a number of important and high-profile organizations including the National Health Service (NHS). It exploited a vulnerability called Eternal Blue which was leaked by a hacker group called The Shadow Brokers a few months prior to the attack in Windows and which was later discovered by USA's National Security Agency. Microsoft released emergency patches to fix the exploit. Most of the systems which were affected by this ransomware were still operating an outdated version of Windows. It mostly affected countries like India and

ISSN:0971-1260

Vol-22- Issue-14-December-2019

Russia because they were still widely running Windows XP versions of Windows which was most at risk. The attack affected around 200,000 systems worldwide and was believed to cause damages ranging from millions to billions of dollars. The ransomware was believed to be originated from North Korea. In December 2017, the US, UK, and Australia formally asserted that North Korea was behind the attack.

WannaCry is a type of Encryption Ransomware. It encrypts the data on the user's system and displays information on how much ransom is to be paid and the payment is done in Bitcoin cryptocurrency.

ISSN:0971-1260

Vol-22- Issue-14-December-2019

Bad Rabbit:

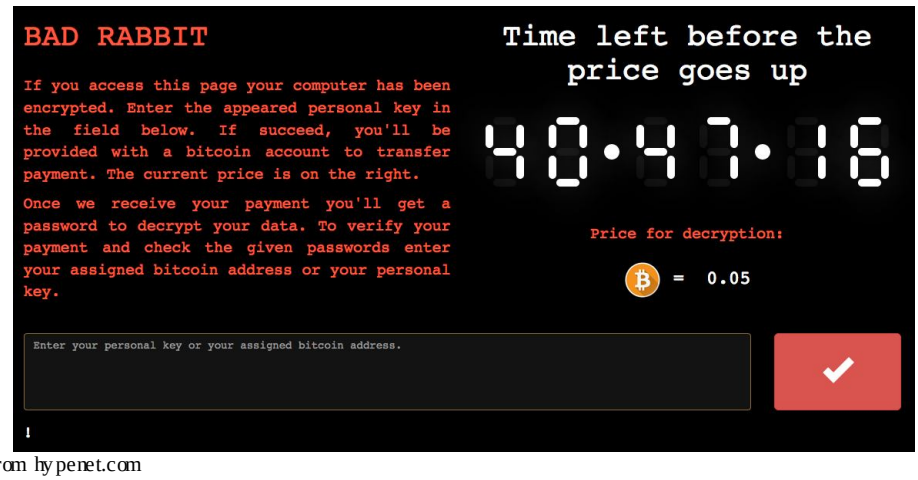


Image is taken from hypenet.com

This Ransomware first started infecting systems on October 24th, 2017. Unlike WannaCry it infected systems indiscriminately and was said to have infected around 200 systems. This cyber-attack mostly infected organizations in Russia and Eastern Europe. It did not exploit any vulnerability like Eternal Blue but it spreads with drive-by downloads on hacked websites. The visitors are told they need to install an Adobe Flash update which is actually a dropper for the malware. It is said to have been based on Petya which was another ransomware attack in 2016. It is suspected that the same hacker group which was behind Petya is behind Bad Rabbit. The victims of the Bad Rabbit are presented with a ransom note telling them that their files are no longer accessible and they need to pay the ransom for decrypting their files. The victim is directed to a Tor payment page where there is a timer for 40 hours or so and the price for the ransom is displayed which is 0.05 BTC which is around 289 $. If the victim fails to pay the ransom in the allotted time the price may go up is one of the messages displayed on the page. The encryption uses DiskCryptor, which is open source

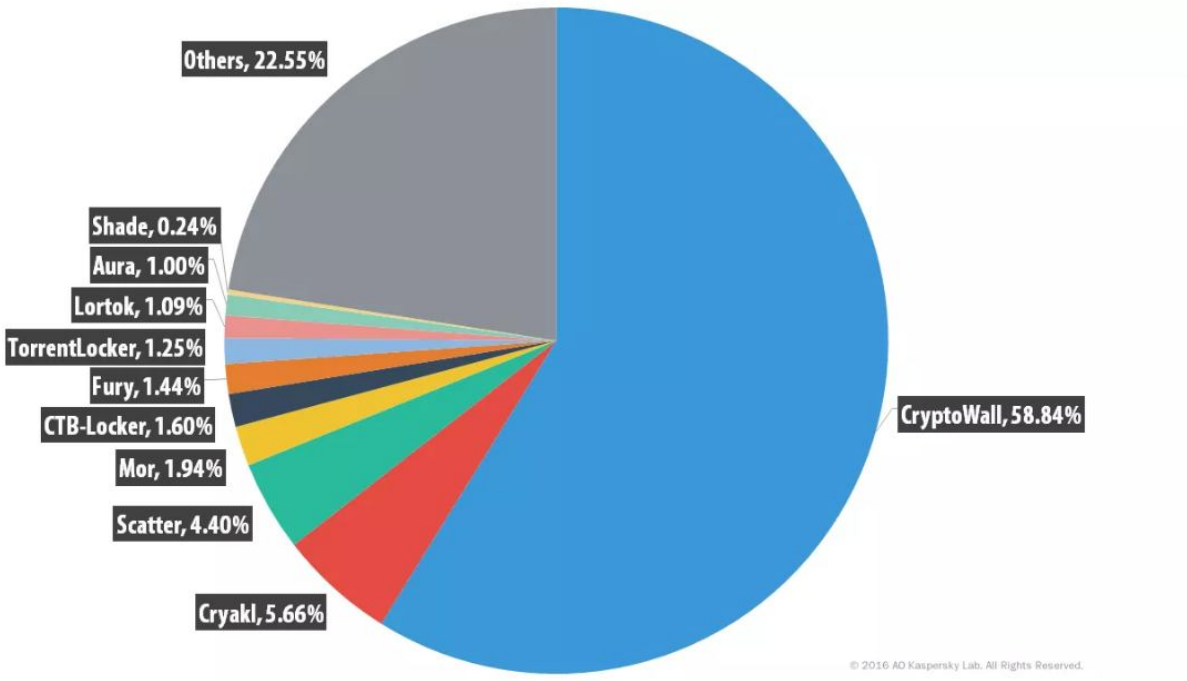
ISSN:0971-1260

Vol-22- Issue-14-December-2019

legitimate and software used for full drive encryption. Keys are generated using CryptGenRandom and then protected by a hardcoded RSA 2048 public key.

Statistics

The Evolution Of Ransomware



Percentage distribution of ransomware variants observed by Kaspersky Labs, 2014-2015. Image originally taken from SecureList.

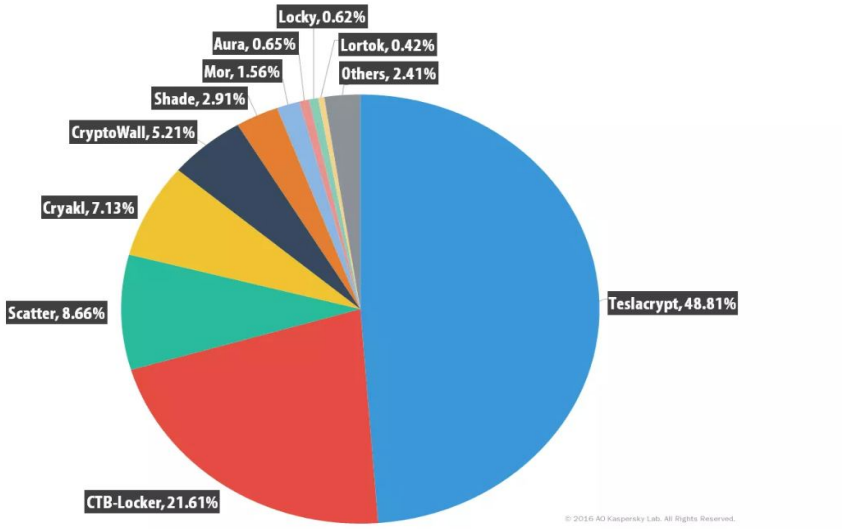
The first ransomware attack was in 1989 a minimal one and reports indicate that it had many flaws and remained uncommon till the 2000s, but this was a building block for the other malware to develop, Ransomware has gotten pretty face during this period of time. Recently a ransomware worm got through many devices disguised as Windows Product Activation notice thus making it more difficult for the user to distinguish between the genuine one and the false one.

ISSN:0971-1260

Vol-22- Issue-14-December-2019

Earlier attackers wrote their own encryption code according to an article published by Fast Company, but nowadays attackers use spear-phishing rather than phishing emails, which are taken care of by the email filter.

Some attackers have developed toolkits that can be used by noob attackers with less technical skills. some of theseransomware malware are Crptowall, WannaCry. The total loses faced through attacks using these kinds of malware has generated more than $320 million in revenue.



Percentage distribution of ransomware variants observed by Kaspersky Labs, 2015-2016. Image originally taken from SecureList.

By 2015-2016 ransomware developed quite a bit multiple variants impacting different platforms and thus came into the picture creating chaos around the world. Kaspersky's SecureList reports that from April 2014 to March 2015, the most prominent one among this malware was CryptoWall, Cryakl, Scatter, Mor, TorrentLocker, etc. Between this period of time, the report states that Ransomware Attacked 101,568 users around the world, i.e. 77.48% of all users attacked with crypto-ransomware.

ISSN:0971-1260

Vol-22- Issue-14-December-2019

	Number of ransomware attacks in millions
2014	3.2
2015	3.8
2016	638
2017	184
2018	204.24

Conclusion

In conclusion, ransomware attacks have made their impact and can be quite devastating to small business owners and organizations. Ransomware can target people randomly or it can be aimed towards a particular organization.

According to the FBI, one must not pay the ransom as one does not know whether the hostage data will be released or not i.e. an activation key is given or not. Paying ransom does not guarantee that the user will have access to their data, but also encourages the ill doers they might not provide you with the encryption key. Therefore, systems need to be up-to-date with the latest security patches for prevention against Ransomware because once infected it is going to be next to impossible to recover your data without paying the ransom.

References

1. Sanatinia, A., Park, J., Blass, E.-O., &Mohaisen, A. (n.d.). . A Privacy-Preserving Longevity Study of Tor's Hidden Services. Retrieved from https://arxiv.org/pdf/1909.03576.pdf
2. Atapour-Abarghouei, A., Bonner, S., & McGough, A. S. (n.d.). A King's Ransom for Encryption: Ransomware Classification using Augmented One-Shot Learning and Bayesian Approximation. A King's Ransom for Encryption: Ransomware

ISSN:0971-1260

Vol-22- Issue-14-December-2019

Classification Using Augmented One-Shot Learning and Bayesian Approximation. Retrieved from https://arxiv.org/pdf/1908.06750.pdf

3. McLaren, P., Buchanan, W., Russell, G., & Tan, Z. (n.d.). Discovering Encrypted Bot and Ransomware Payloads Through Memory Inspection Without A Priori Knowledge. Retrieved from https://arxiv.org/abs/1907.11954
4. LaPiedm, J. (n.d.). The Information Security Process Prevention, Detection and Response . Retrieved from https://www.giac.org/paper/gsec/501/information-security-process-prevention-detection-response/101197
5. Kok, S. H., Abdullah, A., Jhanjhi, N. Z., &Supramaniam, M. (n.d.). Ransomware, Threat and Detection Techniques: A Review. Retrieved from http://paper.ijcsns.org/07_book/201902/20190217.pdf
6. M. Paquet-Clouston, B. Haslhofer, and B. Dupont, "Ransomware Payments in the Bitcoin Ecosystem,"
7. D. Nieuwenhuizen, "A behavioural-based approach to ransomware detection,"
8. https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/attack-list-cities-government-agencies/
9. https://www.nakivo.com/blog/methods-tools-ransomware-detection/
10. https://link.springer.com/chapter/10.1007%2F978-3-030-32150-5_59
11. https://www.thesecuritybuddy.com/data-breaches-prevention/what-is-honeypot/
12. Vidyarthi, D., Kumar, C., &Rakshit, S. (2019). Identifying Ransomware - Specific Properties using Static Analysis of Executables. *Ijarcce*, *8*(4), 358–366. doi: 10.17148/ijarcce.2019.8461
13. https://hyphenet.com/ransomware-screenshots/

ISSN:0971-1260

Vol-22- Issue-14-December-2019

14. https://securelist.com/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/78351/
15. https://www.equities.com/news/ransomware-detection-methods
16. Deloitte, Holding Your Data Hostage. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-ransomware.pdf
17. Deloitte, Taking data hostage: The rise of ransomware. Retrieved fromhttps://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-risk-Ransomware_POV_noCM_AODA.PDF