International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 07 | July 2020 www.irjet.net p-ISSN: 2395-0072

A Study of Ransomware Detection and Prevention at Organizations

Saurabh Kumar Sen[1], Nidhi Chourey[2]

Saurabh Kumar Sen, Department of Information Technology (Cyber security), Vikrant Institute of Technology and Management, Indore (M.P) India.
Nidhi Chourey, Professor, Dept. of Information Technology, Vikrant Institute of Technology and Management, Indore (M.P) India.

Abstract - *Today ransomware has a serious threat to the online world. Most of the software firms, universities, companies, and organizations in the world are trying to take alert decisions to save from ransomware attacks. A joint statement was issued by both governments of the United States and about ransomware attacks insistence users to stay alert and take precautions. Recently on May 19th, 2017, the Swiss government observed the Ransomware Info Day, to spread awareness regarding ransomware and its effects. Ransomware in India as well is on the rise.*

Even expert computer users can be hit and be afflicted by ransomware attacks. In this case, awareness is very beneficial [8]. This study lays the foundation for additional research to find solutions to the ransomware attack problem at organizations. IT security experts and Researchers are aware of chart representations to depict cycles. This paper puts the problem that is faced by organizations on similar representation to show the work of ransomware. Through combining research, illustrating the personal experience of a ransomware attack, Cyber Security tool experience and graphically representing the work of ransomware, society at large will be better informed about the risk of a ransomware attack.

Key Words:- Ransomware, Vulnerability, Malware, Encryption, Decryption, Wannacry, Eternal Blue, Machine Learning, Symantec, Trend Micro.

1. INTRODUCTION

A Ransomware is a type of malware that locks your files, data or the pc itself and extorts money from you to provide access. This can be another way for malware developers to 'collect funds' for their ill-conceived exercises on the web. Once ransomware contaminates a network device, it begins scrambling records, organizers, and whole hard drives partitions utilizing encryption algorithms like RSA or RC4.

Types of Ransomware attacks

Ransomware used to display a message or Readme text stating that the user has done something criminal activities and they are being fined by the police or the government agency based on cyber policy. To get rid of these false 'charges', users were asked to pay these fines.

But, a ransomware attack in two ways. It either locks the computer screen or encrypts certain records with a secret passwords.

The ransomware is partitioned into two types: Lock Screen Ransomware and Encryption Ransomware

Lock screen ransomware locks system and demands a ransom for letting you access it once again. The second type, i.e. the Encryption ransomware, modify the files in your system and demands a ransom to decrypt them again.

The other types of ransomware are:

1. Master Boot Record (MBR) ransomware.

2. Ransomware encrypting web servers.

3. Android mobile device ransomware.

4. IoT Ransomware.

Microsoft distributed information specifying how numerous machines (clients) were influenced by ransomware assaults over the world. It was found that the United States was on the best of Ransomware assaults. Here are the top 20 countries that are majority affected by ransomware attacks.

Countries	Machine count
U.S	320948
Italy	78948
Canada	45840
U.K	38068
Spain	35992
Turkey	32714
Australia	25949
Brazil	24953
Taiwan	20448
Germany	19984
Republic of Korea	19842
Netherlands	18594
Mexico	16525
Russian Federation	13980
India	13783
Korea	13347
South Africa	10830
Romania	10220
Japan	9738

Examples:

1. Advanced ransomware like Spore, WannaCrypt (moreover known as WannaCry). And Petya (moreover known as NotPetya) spread to other computers through network shares or exploits. Spora drops ransomware duplicates in organizing shares.
2. WannaCrypt abuses the Server Message Block (SMB) Powerlessness CVE-2017-0144 (too called Eternal Blue) to contaminate other computers [10].
3. A kind of ransomware family petya exploits the same vulnerability, in addition to CVE-2017-0145 (also known as Eternal Blue), and stolen credentials to move across networks.

Older ransomware like Reveton locks screens rather than scrambling files. The attacker shows a full-screen picture approximately ransom attack and disable Task Manager. During this, Records are secure but viably blocked off. The picture contains a message claiming to be from law requirement that illuminates the computer has been utilized in unauthorized cybercriminal activities and must be paid. Because of this, Reveton is nickname "police Trojan" or "Police ransomware". Ransomware family-like Cerber and Locky encrypt specific file types, typically media and document files. After completion of encryption, the malware displays a ransom note using text, image, or an HTML file with the information to pay a ransom to decrypt files.

Awful Rabbit ransomware was found endeavoring to spread over systems utilizing hardcoded usernames and passwords in brute force attacks.

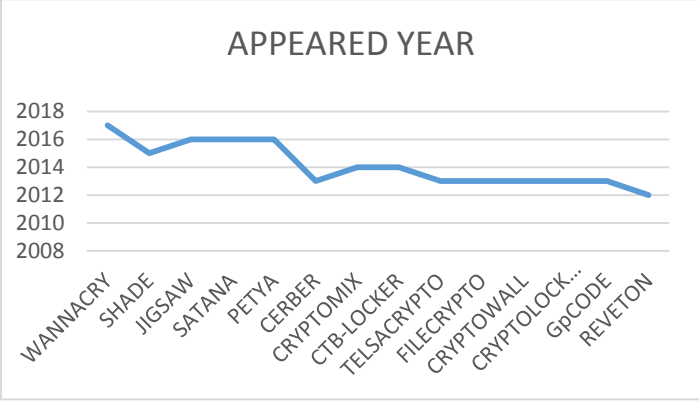

Figure 1.Ransomware attack with appeared year

Above appeared ransomware families have different propagation strategies. The propagation strategies are the way and method of ransomware propagation in a particular organization. Below the table of ransomware propagation strategies.

Table 1: The list of ransomware families, different families and Propagation Strategies.

FAMILIES	PROPAGATION STRTEGIES
WANNACRY	Samba Vulnerability
SHADE	Spam Email
JIGSAW	Word Document with Javascript
SATANA	E-mail Attachments
PETYA	Link in an E-mail indicating to be a job application
CERBER	Compromised websites and e-mail attachments
CRYPTOMIX	Spear phishing Email
CTB-LOCKER	Email attachments
TELSACRYPTO	Compromised websites and email attachments
FILECRYPTO	Compromised websites and e-mail attachments
CRYPTOWALL	Compromised websites and email attachments
CRYPTOLOCKER	Compromised websites and e-mail attachments
GpCODE	Email attachments
REVETON	Accused of illegal activities

In India, around 67 percent of the surveyed entities were hit by ransomware last year. Around 37 incidents of ransomware attacks were reported to the Indian Computer Emergency Response Team (CERT-In). Of these, 34 incidents were found of WannaCry and Petya ransomware. WannaCry ransomware attacks were to begin with Detailed on 12th May 2017 and Petya on 27th June 2017. **Note that add up to no. of ransomware occurrence has been detailed to CERT-In within the past:**

- 2015:2
- 2016:26
- 2017 (till June):37

More than 27,000 cybersecurity risk occurrences within the to begin with half of 2017 alone detailed by CERT-In [3]. These incorporate extend of threats like phishing attacks, websites intrusions and defacements or harms to information as well as ransomware attacks. As per CERT-In's data, the number of cybersecurity incidents reported in the past 3 years:

- 2017:44,679
- 2015:49,455
- 2016:50,362
- 2017 (till June): 27,482

Machine learning

Machine learning is a form of artificial intelligence (AI) which gives systems the ability to learn and improve automatically from experience without explicit programming. ML focuses on designing Scripts, computer programs that are able to access and use data to think for themselves.

The method of learning begins with observations or information, such as cases, direct experience, or instruction, to search for designs in information and make better choices within the future based on the cases that we offer. The essential point is to permit the computers to memorize consequently without human mediation or help and adjust activities appropriately.

Where conventional file-based security detection technology fails, machine learning algorithms succeed neural networks and profound learning algorithms can detect unknown ransomware samples when properly trained and modified to produce a small number of false positives. Enhance cloud-based detections with machine learning and genetic algorithms are also effective in resist the excessive growth of ransomware caused by its polymorphic behavior.

A major benefit of using machine learning models to spot ransomware is that it increases the number of possible ransomware files it can detect, if enough ransomware features are presents in an unknown ransomware sample, the file is likely ransomware.

The second benefits are that machine learning models are extremely small, usually, around 1 kilobyte, which makes them easy to deploy across the entire user base. The only drawback of utilizing machine learning models to identify ransomware is that they have to be broadly tried before deployment to maintain a strategic distance from inaccurately labeling clean records as malicious.

A few machine learning algorithms can indeed recognize suspicious URLs that are either utilized to spread ransomware or act as command and control servers. Using Natural Processing (NLP) algorithms and different clustering methods to decode texts, they can prevent victims from accessing new or unknown connections, preventing the specific payload of ransomware from entering the computer...

Machine learning algorithms for ransomware identification can be used as a proactive method for combating ransomware threats, regardless of whether they are designed for PCs, mobile devices or even IoTs. The main advantage of machine learning is that it can be used as a tool to increase established safety layers, giving them proactivity, effectiveness and efficiency.

Ransomware remains here: protection is the same. It is highly unlikely that ransomware will soon go away, particularly because digitalization has resulted in increased interconnectivity between systems. With a proven and tested business model and financial gains in the billions of dollars, ransomware is likely the biggest mass-market threat to both end-users and organizations. However, machine learning algorithms can augment all security layers to detect and plug threats at pre-execution, on-execution, and post-execution, making ransomware less of threats and more of a nuisance.

2. LITERATURE REVIEW

According to the review literature about Ransomware, a brief history of how it works developed and some popular stories from an Organization that is infected with ransomware malware and related information. For three years, the number of organization victims being targeted by ransomware is increasing. When it attacks any organization, first it spread in the network, slowly encrypts files and demands large amounts of money to restore encrypted files. But practically impossible to reverse the encryption or crack the files without the original encryption key.

Prominent Research Work

According to the comprehensive review of previous research work.

1. A brief study of wannacry threat: Ransomware attack 2017. The focus of paper on the wannacry attack 2017, it explains about wannacry ransomware threat.
2. Detection and Avoidance of Ransomware (2017).This paper focus on detection and avoidance method for ransomware attack to reduce damage.
3. Ransomware: A research and a personal case study of dealing with this nasty malware-IISIT.ORG (2017)
4. Ransomware for the Internet of things-ARNE MAXIMILLIAN KAUL. (2017
5. Detection and Prevention of Crypto-Ransomware-Daniel Gonzalez Fordham center Cybersecurity, Fordham University, New York, NY, USA (2017).

6. Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization (2016). The focus of the paper is on ransomware families evolved in windows and android environments. We analysis of ransomware families, focusing on their evolution and characterization.
7. A Novel method for Recovery from Crypto-Ransomware infections. (2016)Using the crypto-ransomware method not only covers prevention but also focuses on how to recreate the files. Using Lock, Tesla Crypto and CTB locker successfully infected the system and easily and automatically be restored and encrypt the data. Disadvantage- the local hard drive would become unusable or damaged on the file system level; the proposed method will not work without first repairing the structure of the damage.
8. Detecting Ransomware with Honeypot techniques. (2016).These research techniques to implement a honeypot to detect ransomware activity. When activated, the research produced a staged response to attacks on the device along with thresholds. Disadvantage-there is no guarantee the malware would attempt to invade these areas, and a honeypot free from attack alerts is not an indicator that other areas are not being targeted.

Motivational Approach

In the last five years, most Organizations were affected by a ransomware attack all over the world. In India, several companies in the cities of Mumbai, Hyderabad, Bengaluru, and Chennai were also affected. These cyber-attack dangerous for the digital world, which motivates me for Risk analysis, malware detection, prevention, troubleshooting at organizations with the help of Security tools and Machine learning technology. So, a prominent comprehensive review of related literature and professional reports of Research paper that helps me to work in the cyber-attacks.

Predicate: Understand risk, know attack surface and Uncover weak spots.

Prevent: Minimize the attack surface, prevent incidents.

Respond: data breaches, mitigation, analyze and learn.

Detect: Recognize, identify and handle events and threats.

3. PROBLEM STATEMENT

Ransomware attack hacks confidential business and personal data and asks for ransom in the return of hacked or encrypted data. Around the world, Ransomware attacks cost businesses millions and millions of money.

WannaCry recently attacked for money, as they asked for ransom in return for decryption keys, but later Petya encrypted and deleted all data.

Table 2: Affected Organisation sector in India

Organization sector	Affected
Services	38%
Manufacturer	17%
Public Administrative	10%
Finance, Insurance & Real Estate	10%
Wholesale Trade	9%
Transportation, Communications & Utilities	7%
Retail Trade	4%
Construction	4%
Mining	1%
Agriculture, Forestry & Fishing	1%

Problems occur during attacks:

1. Productivity loss during downtime: 50 percent
2. Corporate revenue generation per hour: $24,000
3. 21 hours of downtime until full recovery

Ransomware attack effect on organizations:

1. 50 per cent risk of workers experiencing loss of productivity
2. 30 per cent chance the company will temporarily shut down
3. 20 per cent chance of loss of corporate revenue.

4. ANALYSIS REPORT

With the help of Symantec Endpoint Protection and Trend Micro Officescan at PSU Organization, we analyze:

1. Daily Detected wannacry ransomware in Organization Network.
2. With Symantec Endpoint Protection, Ransom.wannacry detected
3. Mostly found Wannacry in extensions in Trend Micro Officescan like:
    1. Ransom_WCRY.DAM,
    2. Ransom_WC

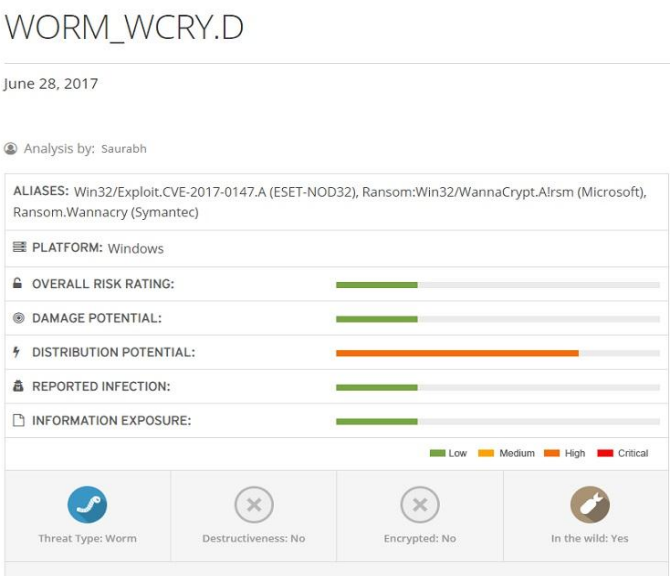

Figure 2.Wannacry Detection

Prevention Tool Used:-

TrendMicro Ransomware Screen Unlocker tool.

Microsoft Enhanced Mitigation and Experience toolkit (EMET).

Malwarebytes Anti-Ransomware (formally Crypto Monitor).

5. METHODOLOGY

Best Practices to prevent ransomware attacks:

1. Keep up to date with the new updates on the operating system, third party software (MS Office, Browsers, and Browser plugins).Disable remote Desktop Connections.
2. Enable a personal firewall on workstations.
3. Maintain updated Antivirus software on all systems.
4. Strict External Device (USB drive) usage policy.
5. Restrict permissions for users to install and run inappropriate software applications. Block the attachments of file types: exe/pif/tmp/url/vb/vbe/scr/reg/cer/pst/cmd/ bat/dll/hlp/hta/js/wsf.
6. Check the contents of backup files of databases daily for any unauthorized encrypted contents of data records or external elements, backdoors, malicious scripts.
7. Configure access controls with file, directory and network share permissions with least privilege.
8. Configure installing Enhanced Mitigation Experience Toolkit or similar Host-level anti-exploitation tools.
9. Disable macros in Microsoft products.

Specific countermeasures to prevent Ransomware attack:

Organizations IT administrators are advised to use the following preventive measures to protect their computers from ransomware malware attacks:

1. Symantec and TrendMicro offices cannot be supported in Windows XP. Up-to-date with the latest operating system.
2. To apply Microsoft security patches to prevent ransomware infection such as Microsoft Security Bulletin MS17-010.
3. In Windows XP, Vista, Server 2003, Server 2008, Microsoft patches not supported.
4. Regularly backup of critical data to prevent data loss.
5. Disable SMBv1 or block SMB port (UDP 137, 138 and TCP 139,445).
6. Enable IDS/IPS feature of Firewall and Antivirus to prevent attacks.

6. Conclusion & Future Scope

In this research, the goal to improve malware detection, prevention, and mitigation. Using the method to reduce damage caused by ransomware attacks and techniques to minimize the ransomware attack loopholes in the network.
In the Future, It will help to find malware more effective way with upcoming new technology and easy to minimize organization losses due to ransomware. Also, this report motivates new researchers and analytics for the decryption of infected files.

The main goal of this thesis is to implementing risk with the help of machine learning and Python language according to organization research.

References

1. A Brief Study of Wannacry Threat: Ransomware Attack 2017- IJARCS Savita Mohrule,Manisha patil, MITACSC, Alandi, Pune, India.
2. Fundamental of Machine Learning for Predictive Data Analytics: Algorithms, Worked Examples, and Case Studies by John Kelleher, Brian Mac Namee, and Aoife D'Arcy.
3. Ransomware: A Research and a personal case study of dealing with this nasty malware-Azad Ali, Indiana University of Pennsylvania.

4. Detection of ransomware on windows operating systems-Jaan Priisalu, TALLINN UNIVERSITY OF TECHNOLOGY.
5. Sanggeun Song, Bongjoon Kim, and Sangjun Lee. "The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform", Hindawi Publishing Corporation Mobile Information Systems Volume 2016, Article ID 2946735, 9 pages.
6. Nikolai Hampton, Zubair A. Baig, "Ransomware: Emergence of the cyber-extortion menace",The Proceedings of [the] 13th Australian Information Security Management Conference, held from the 30 November – 2 December, 2015 (pp. 47-56), Edith Cowan University Joondalup Campus, Perth, Western Australia.

Websites:

1. http://www.catalog.update.microsoft.com/Search.asp?q=KB4012598
2. https://www.csoonline.com/article/3212260/the-5-biggest-ransomware-attacks-of-the-last-5-years.html
3. https://www.us-cert.gov/Ransomware
4. https://support.symantec.com/us/en/article.howto124710.html
5. https://www.symantec.com/connect/blogs/report-organizations-must-respond-increasing-threat-ransomware
6. https://blog.malwarebytes.com/malwarebytes-news/2016/01/introducing-the-malwarebytes-anti-ransomware-beta/
7. https://esupport.trendmicro.com/en-us/home/pages/technical-support/1105975.aspx
8. http://iisit.org/Vol14/IISITv14p087-099Ali3400.pdf
9. https://www.medianama.com/2017/08/223-ransomware-india-wannacry-petya/
10. https://docs.microsoft.com/en-us/windows/security/threat - protection/intelligence/ransomware-malware.