International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT206670

A Study on Behavioural Analysis of Specific Ransomware and its Comparison with DBSCAN-MP

Dr. V. Vinodhini[1], Dr. C. Kumuthini[2], Dr. K. Santhi[3]
[1]Professor, Department of Information Technology, Dr. N.G.P. Arts and Science College, Dr. N.G.P. Nagar, Kalapatti Road, Coimbatore, Tamil Nadu, India
[2,3]Associate Professor, Department of Information Technology, Dr. N.G.P. Arts and Science College, Dr. N.G.P. Nagar, Kalapatti Road, Coimbatore, Tamil Nadu, India

Article Info
Volume 7, Issue 1
Page Number: 01-06
Publication Issue :
January-February-2021

Article History
Accepted : 01 Jan 2021
Published : 04 Jan 2021

ABSTRACT

Ransomware attack is known to as WCRY or WannaCry. This ransomware is intriguing advantage of a recently disclosed Microsoft vulnerability ("MS17-010 – "Eternalblue") coupled with the Shadow Brokers tools release. After a computer is fouled, WannaCry ransomware targets and encrypts 176 file types. Some of the file types WannaCry targets are database related files, multimedia and archive related files, as well as Microsoft Office documents. In its ransom note, which supports 27 languages, it initially demands US$300 worth of Bitcoins from its fatalities—an amount that increases incrementally after a definite time limit. The victim is also given seven days before the pretentious files are deleted.

The WannaCry Ransomware consists of multiple components. It arrives on the ruined computer in the form of a dropper, a self-reliant program that extracts the other application mechanism embedded within it. Those components include:

- An application that encrypts and decrypts data
- Files containing encryption keys
- A copy of Tor

The program secret code is not obfuscated and was relatively easy for security pros to analyze. Once it is launched, WannaCry tries to access a hard-coded URL (the so-called kill switch); if it can't, it proceeds to investigate for and encrypt files in a slew of important formats, ranging from Microsoft Office files to MP3s and MKVs, leaving them completely inaccessible to the user. It then displays a ransom notice, demanding numbers in Bitcoin to decrypt the files.

Keywords: WannaCry, WCRY, Eternalblue, GPO, Bitcoin

I. INTRODUCTION

Factors to prevent menace of infection

- Patch and update the systems, or deem a virtual patching solution.

- Facilitate firewalls as well as intrusion detection and prevention systems.
- Proactively monitor and validate traffic going in and away of the network.
- Put into action on security mechanisms for entry attackers , such as email and websites.
- Deploy application control to foil suspicious files from executing on top of behaviorial monitoring that can thwart unwanted modifications to the system.
- Employing data categorization and network segmentation to mitigate further exposure and harm to data.
- Render inoperative SMB (v1) on vulnerable machines – using either GPO or by following the instructions provided by Microsoft.
- Ensure that all of the most recent patches (if possible using Virtual Patching solution) are applied to pretentious operating systems.

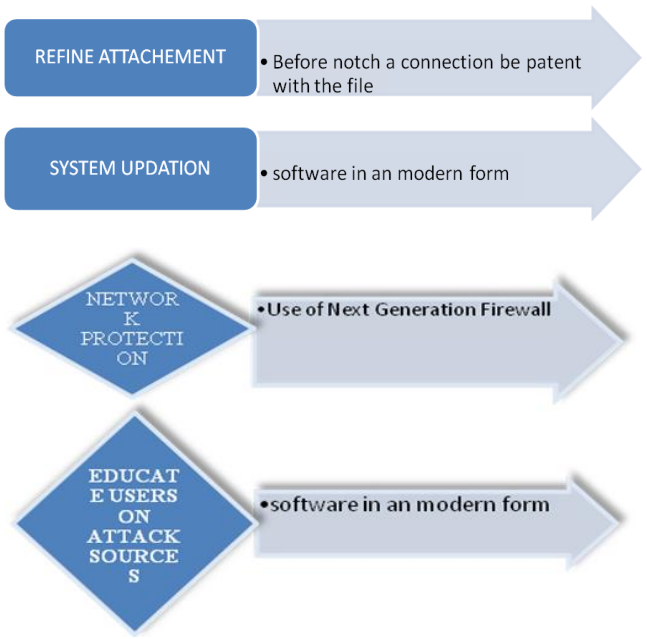

Fig : 1 - Conception to realize the unsurpassed practices

REFINE ATTACHMENT

- Before opening a attachment be clear with the file and the person from who did you receive the mail.
- **SYSTEM UP TO DATE** Keep all the software in your system up to date including Antivirus, Javafiles, Fkashplayer etc
- **VPN** Use VPN for secure emailing which prevents you from the unwanted spam mails with the suspicious .exe files and block them in their servers
- **AI DETECTION** Ai Detection software to monitor the system activities and detect the malfunctioning files.
- Secure your Windows Firewall with an up to date update on it without any lope holes in it. It helps to get protect from the suspicious activities- **FIREWALL**
- Make sure that you must have to disable file sharing in your PC with any other devices and the remote access with the devices- **DISABLE FILE SHARING AND REMOTE SERVUCES**
- Give an aware of the attacking sources what are all the ways that get affected from ransomware- **EDUCATE USERS ON ATTACK SOURCES.**
- Take layer approach with the security infuse from the endpoint of Email to DNS layer. Use next Generation firewall- **PROTECT YOUR NETWORK**
- Limit the resources to be access by others to prevent the dynamic access by the attackers- **SEGMENT NETWORK ACCESS**
- Always have a backup of the data what we use for the organisation in a separate server to prevent from loss of data- **BACKUP DATA**

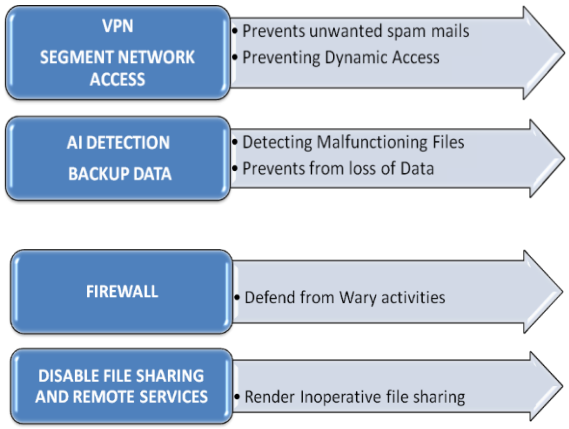

Fig : 2 - Conception to realize the unsurpassed practices

Security approach using Trend Micro

Trend Micro recommends a covered security loom on - endpoint, messaging, and gateway, to ensure that all potential entry and conciliation against these types of terrorization,

- ✓ Updated Configuration and Next Generation Technology
- ✓ Smart Scan Agent Pattern and Official Pattern Release
- ✓ Trend Micro Web Reputation Services (WRS)
- ✓ Trend Micro subterranean detection Inspector
- ✓ Trend Micro Tipping Point
  - ✓ Trend Micro Endpoint Application Control (EAC)
  - ✓ Trend Micro Endpoint Application Control (EAC)
  - ✓ Trend Micro Cloud Edge and Smart Home Network

Modernized Configuration and Next cohort Technology

Trend Micro customers using the hottest versions of OfficeScan and Worry-Free Business Security should guarantee that they have both Predictive Machine Learning (OfficeScan, Worry-Free Services) and all pertinent Ransomware protection features enabled in their artefact.

- **Elegant Scan Agent Pattern and bureaucrat Pattern Release**

- ➢ Trend Micro has additional known variant and component detections .The smart Scan patterns includes, Smart Scan Agent Pattern , Official Pattern Release
- ➢ (conventional) These patterns are the minimum optional ones that contain protection for this menace.
- ➢ The classy sophisticated ransomware such as Spora, WannaCrypt (WannaCry),
  and Petya (NotPetya) spread to other computers via network shares or exploits.
- ➢ Spora drops ransomware copies in network shares.
- ➢ WannaCrypt exploits the Server Message Block (SMB) severe vulnerability CVE-2017-0144 (EternalBlue) to taint other computers.
- ➢ A Petya variant exploits the same severe vulnerability, in addition to CVE-2017-0145 (EternalRomance), and uses stolen testimonial to budge laterally across networks.
- ➢ Older ransomware like Reveton locks screens instead of encrypting files. Ransomware like Cerber and Locky search for and encrypt specific file types, typically document and media files.
- ➢ The newer apparatus and variants being revealed it is important that customers ALWAYS obtain the latest pattern files to ensure up-to-date protection.

- **Trend Micro Web Reputation Services (WRS)** has added exposure for notorious demand and control (C&C) servers.
- **Trend Micro Deep Security and Vulnerability Protection**

In earlier times the IDF plug-in for OfficeScan) customers with the hottest IPS convention have an efficient layer of Virtual Patching protection for manifold Windows operating systems, as well as some that have reached end-of-support . Distinctively, Trend Micro unconfined the following IPS convention for proactive protection. Intrusion Prevention System

1008224, 1008228, 1008225, 1008227 includes exposure for MS17-010 and some explicit protection against Windows SMB remote code execution vulnerabilities

- **Trend Micro Deep Discovery Inspector**

Patrons with the hottest convention also have an additional layer of protection against the vulnerabilities coupled with the feat. Distinctively, Trend Micro has unhindered the following certified rule for proactive protection

- **Trend Micro Tipping Point**

Trend Micro Tipping Point is a Network Protection , the Patrons with the subsequent filters have updated protection. NGIPS (Next Generation Intrusion Protection System) which protects crucial transportation, data and vulnerable applications in real –time from recognized to unfamiliar vulnerabilities without negatively affecting network performance. ThreatDV Filter which helps to mitigate outbound C2 communication. **Policy Filter** - provides additional protection against suspicious SMB fragmentation.

TippingPoint delivers incorporated superior Threat Prevention to shield the network from the periphery to the data center to the cloud with real-time, inline enforcement and programmed remediation of vulnerable systems.

- Inspect and wedge inbound, outbound, and lateral network traffic in real-time.
- Deploy pre-emptive zero-day coverage using intelligence based on elite insight into undisclosed vulnerability data from the Zero Day Initiative
- Distribute scalable performance up to 100 Gbps inspection throughput with lowlatency, Drive vulnerability threat prioritization with absolute network visibility
- Afford immediate and ongoing threat protection with out-of-the-box suggested settings

- **Trend Micro Endpoint Application Control (EAC)** administrators utilizing the product's "Lockdown" approach - which allows only pre-specified application programs to scuttle - also provides fortification against this threat.

Trend Micro extremely recommends that vendor crucial patches are functional as soon as possible upon release. Customers and partners who may require some additional information or have questions are encouraged positively to contact their authorized Trend Micro technical maintain agent for additional assistance.

- **Useful tools to help detect and prevent infection**

Trend Micro also has some standalone tools available for assessing and addressing probable WCRY menace and infections on end-user technology.

- Trend Micro Anti-Threat Toolkit (ATTK): users facing issues with their endpoint fortification can do downloading ATTK to examine a significantly compromised machine for malware (including WCRY).
- Trend Micro WCRY Simple Patch Validation Tool: This tool has two functions – (1) checks a local machine to observe if Microsoft's MS17-010 patch has been productively functional; and (2) offers to and allows the user to easily immobilize SMB v1 on the local machine via registry key. It is designed as a rapid tool for users that may not have former easy means to authenticate the system patch
- Trend Micro Ransomware Decryption: It has added restricted decryption support for WCRY polluted machines Based on internal testing, the highest success rate has been pragmatic on ruined machines running Windows XP (x86)
- **Data Encryption: A Key Component of Malware**

Ransomware, in its on the whole basic form, is self-explanatory. Data is captured, encrypted, and held for ransom until a fee is paid. The two most general forms

of ransomware liberation are through email and websites.

Even though ransomware attack has been around in the globe some form or another for decades--the very first familiar attack is believed to have occurred in 1989--it has more recently become the modus operandi of cyber criminals transversely the globe. Ransomware has been endlessly evolving in the past decade, in part due to sophisticated advances in cryptography. The extensive accessibility of critically advanced encryption algorithms RSA and AES ciphers ended this ransomware more robust. While estimates vary, the number of ransomware attacks continues to rise. The Verizon 2017 Data Breach Investigations Report certainly estimates that (pre WannaCry) ransomware attacks around the globe grew by 50 % in the last few years.

Comparison Study

- Comparing performance of DBSCAN-MP to original DBSCAN algorithm
- The performance of DBSCAN-MP is compared with original DBSCAN by using different epsilon values that is found in training phase for all clusters. The result shows that
- Maximum detection rate of original DBSACN is lower than DBSCAN-MP, and false positive rate is higher compare to DBSCAN-MP.
- The following are the family name and its corresponding id of the attempted dataset samples which has the family name of non ransomware with the id 0 and the variety of ransomware family names with the Ids ranging from 1 to 11.

Table 1: Comparison study of DBSCAN-MP

Family Name	ID
Goodware	0
'Critroni'	1
'CryptLocker'	2
'CryptoWall'	3
'KOLLAH'	4
'Kovter'	5
'Locker'	6
'MATSNU'	7
'PGPCODER'	8
'Reveton'	9
'TeslaCrypt'	10
'Trojan-Ransom'	11

- The following dataset has the correspondence of the local IDS that is used in the dataset with the SHA1 and MD5 of the software analysed (both non ransomware and ransomware). The description of the header in that file is the following:
- ID: local identifier used in our dataset.
- SHA1: SHA1 hash identifier for the software.
- MD5: MD5 hash identifier for the software.
- Ransomware: 1 if it's ransomware / 0 for Goodware.
- Ransomware_Family: numeric identifier for the ransomware family (same codification is as explained above).

II. CONCLUSION

Ransomware has become an gradually more common and effectual attack disturbing enterprises, impacting efficiency and preventing users from accessing files and data. Some uses behavioural intelligence to hasten the process by quickly analyzing endpoints channel within an enterprise and alerting team so that conducting an exploration and scope the compromise in real-time.

III. REFERENCES

[1]. Nolen Scaife, Henry Carter, Patrick Traynor, Kevin R.B. Butler." CryptoLock (and Drop It): Stopping Ransomware Attacks on User

Data",2016, IEEE 36th International Conference on Distributed Computing Systems.

[2]. MattiasWeckstén, Jan Frick, Andreas Sjöström, Eric Jarpe, "A novel method for recovery from Crypto Ransomware infections", [5]. Computer and Communications (ICCC), 2016 2nd IEEE International Conference.

[3]. N. Andronio, S. Zanero, and F. Maggi, "HelDroid: dissecting and detecting mobile ransomware," 2015, in Research in Attacks, Intrusions, and Defenses, vol. 9404 of Lecture Notes in Computer Science, pp. 382–404, Springer.

[4]. Pathak, P B."Malware a Growing Cybercrime Threat: Understanding and Combating Malvertising Attacks",2016.

[5]. https://www.proofpoint.com/us/blog/threat-protection/providing-healthcare-organizations-visibility-latest-ransomware-attacks

[6]. https://www.zdnet.com/article/ransomware-an-executive-guide-to-one-of-the-biggest-menaces-on-the-web

Cite this article as :

Dr. V. Vinodhini, Dr. C. Kumuthini, Dr. K. Santhi, "A Study on Behavioural Analysis of Specific Ransomware and its Comparison with DBSCAN-MP", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 1, pp. 01-06, January-February 2021. Available at doi : https://doi.org/10.32628/CSEIT206670
Journal URL : http://ijsrcseit.com/CSEIT206670