ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 9, September 2017

A Study of WannaCry Ransomware Attack.

Dr Supreet Kaur Sahi

Asst Prof, SGTBIMIT

Abstract - **The problem with Cyber security is continuously evolving nature of security threats. The traditional approach focused on high demand resources ignoring less important components at dangerous risks. Such an approach is insufficient in current environment and biggest example of this is WannaCry Ransomware attacks. This article highlights different characteristics of security threats. The globe has experienced a Ransomware cyber-attack "WannaCry" that has infected thousand computers worldwide. WannaCry has ability to spread through network by exploiting a critical vulnerability. This article also highlights preventive steps against the attack. Finally a formula is discussed to enhance Network Security.**

I. INTRODUCTION

Breaking of computer is called hacking. Hackers are used to solve unsolved problems. They have legal authorization to hack. Hacking can be done for purpose of discoveries, scientific research, testing, or political and defense reasons. Cracking is illegal hacking. Information security is different from security needs of other areas [1].

There are different types of security attacks. Malware is software package that hackers used to take control of systems. Worms, Viruses, Trojans, Zombies, Ransomware are some form of malware attack. Worms are self-propagating program. Different examples of worms include ILOVEYOU, NIMDA. Virus replicates itself to attack system. Trojan offers users attractive benefits. Social engineering is also used to attain information. It is
psychological manipulation for information gathering, frauds and system access [2][3].

In order to secure system risk management need to be done. Users need to be careful about downloading or clicking any link. Rule of thumb is to know importance of information. Digital information, personal identity, software details, intellectual property, account information are assets which needs to be secured. Black market is full of theft information, which will be used against users. Risk exposure is also function of vulnerability of assets [2].

Cyber security information is of three forms:
1. Physical
2. Administrative
3. Technical and control

Data traveling beyond local firewall needs to be encrypted. Key management is issue.
Three things with key:

- Self managed key (data not protected if key loss)
- Cloud provider (change in cloud provider)
- Third party provider who are specialized.

Once the threats is identified different measures need to be followed [4]:

- Disaster recovery
- Automated data centers
- Wrapping data into multiple layers.

If some security threat incident occurs incident response teams should come to picture and handle the situation [5]. There are different digital forensics labs available that deals at following levels:

- Network
- Computer
- Mobile
- Database
- Live
- How evidences need to be handled

The WannaCry attack started on May 12, 2017 and within one day it has infected more than 2,30,000 computers in 150 countries. It is an example of the security incidents happened recently [6].

2. SURVEY ON WANNACRY

According to news analysis from Malwarebytes [7] The WannaCry Ransomware threat is not because of malware infected phishing mails. It begins by scanning for vulnerable TCP 445 port (Server message Block) on public Internet. The WannaCry Ransomware was a

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 9, September 2017

worldwide cyberattack, which has targeted systems running on Microsoft windows operating system by encryption of data and claiming ransom payments in Bitcoin Cryptocurrency. The important point to note that it not only scans internal ranges to identify point of spread, it is also capable of spreading using Internet.
Even though Microsoft provided patch for older system versions on the day of outbreak, still the count of attacked systems are rising. New versions and variants of this malware are constantly released which are making mitigation difficult [8][9]. The first attack happened on May 12, 2017 and malware identified is as follow:

• VARIANT 1:. wcry

• VARIANT 2: WCRY (+ .WCRYT for temp)

• VARIANT 3: .WNCRY (+ .WNCRYT for emp)

Another version with changed kill switch domain is found on May 14, 2017. This domain has been registered and points to a sinkhole as well. Only 2 letters differ [8]:

www.iuquerfsodp9ifjaposdfjhgosurifaewrwergwea.com

becomes

www.iffuerfsodp9ifjaposdfjhgosurifaewrwergwea.com

According to Cisco WannaCry [10] has used DOUBLEPULSAR. It is used for accessing and executing code on previously compromised systems. It further makes possible activation and installation of other software like malware. This malware has also used ETERNALBLUE module for initial exploitation of the SMB vulnerabilities. If successful it will implant the DOUBLEPULSAR backdoor and utilized it for installing malware otherwise if fails and DOUBLEPULSAR is already installed the malware will used it for installing Ransom ware payload[10].

Ransom ware can infect both home users and trades that can result in

- Loss of sensitive information
- Regular operations disruption
- Financial losses incurred
- Harm to organization reputation

Payment does not guarantee that encrypted files will be released. Similarly decrypted file doesn't mean that malware is removed from system [11].

Ransom ware can infect both home users and trades that can result in

- Loss of sensitive information
- Regular operations disruption
- Financial losses incurred
- Harm to organization reputation

Payment does not guarantee that encrypted files will be released. Similarly decrypted file doesn't mean that malware is removed from system [11].

3. PROTECTIVE MEASURES

Protective measures to lessen Ransomware threats includes:

· Ensuring anti-virus software is up-to-date.

· Implementation of data back up and recovery plan for maintaining copies of sensitive or proprietary data in secure location.

· Scrutinizing links in emails, and never opening attachments in unsolicited emails.

· Downloading free software from trusted sites.

· Enabling automated patches for operating system and Web browser.

Network value= network benefits- network cost-cost of security-expected lost. Benefits need to be increase to maximize network value. Increasing investment on security can reduce hacking losses. It is need of hour that organizations ensures security incident response teams should always be ready with business continuity plan. Appropriate backups must be there to restore data in case of security attacks [12].

4. CONCLUSION

The purpose of this study is to analyze different characteristics of WannaCry attack. Threats like WannaCry can be reduced by following preventive measures. Once such type of attack occurred, Disaster Recovery teams should come to picture with countermeasure steps. It is difficult to stop cracker from

launching attacks, but exercising defensive measures can prevent attacks. Investment on network security needs to be increased in order to increase network security and losses due to cyber attacks.

REFERENCES

[1] Rodriguez, Chris; Martinez, Richard. "The Growing Hacking Threat to Websites: An Ongoing Commitment to Web Application Security" (PDF). Frost & Sullivan. Retrieved 13 August 2013.

[2] Gordon L A, Loeb M P, Lucyshyn W, Richardson R, CSI/FBI Computer Crime and Security Survey, 2006.

[3] Bosworth, S. and Kabay, M.E. (Eds) (2002), Computer Security Handbook, 4th ed., John Wiley, New York, NY. [Google Scholar]

[4] Baskerville R. (993). Information systems securitydesign methods: Implications for information systems development. ACM Computing Surveys, 25(4), 375–414. 10.1145/162124.162127

[5] D. D. Dudenhoeffer, M. R. Permann, S. Woolsey, R. Timpany, C. Miller, A. McDermott, M. Manic, "Interdependency modeling and emergency response", Proc. 2007 Summer Computer Simulation Conference, pp. 1230-1237, July 2007.

[6] Wong, Julia Carrie; Solon, Olivia (12 May 2017). "Massive Ransomware cyber-attack hits 74 countries around the world". The Guardian. Retrieved 12 May 2017.

[7] Adam McNeil "How did the WannaCry Ransomworm spread?" May 30, 2017 retrieved fromhttps://blog.malwarebytes.com/cybercrime/2017/05/how-didwannacry- ransomworm-spread/

[8] CERT-MU Whitepaper, "THE WANNACRY RANSOMWARE"; May 2017.

[9] Savita Mohurle, Manisha Patil, "A brief study of Wannacry Threat: Ransomware Attack 2017", Volume 8, No. 5, May-June 2017, International Journal of Advanced Research in Computer Science, ISSN: 0976-5697.

[10] Senad Arc , Nils Roald , "Cisco Advanced Malware Protection against WannaCry"

[11] Nolen Safe , 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

[12] 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.

[13] Millar, Sheila A.,Marshall, Tracy P., Cardon, Nathan A., "WannaCry: Are Your Security Tools Up to Date?", The National Law Review, Keller and Heckman LLP, Retrieved 9 July 2017.