BEST: International Journal of Management Information Technology and Engineering (BEST: IJMITE)
ISSN (P): 2348-0513, ISSN (E): 2454-471X,
Vol. 6, Issue 4, Apr 2018, 1-4

THE WANNACRY RANSOMEWARE, A MEGA CYBER ATTACK AND THEIR CONSEQUENCES ON THE MODERN INDIA

ASHOK KOUJALAGI[1], SHWETA PATIL[2] & PRAVEEN AKKIMARADI[3]

[1]Assistant Professor & Postdoctoral Researcher, P. G Department of Computer Science, Basaveshwar Science College, Bagalkot, Karnataka, India

[2,3]Assistant Professors, P. G Department of Computer Science, Basaveshwar Science College, Bagalkot, Karnataka, India

ABSTRACT

Wanna cry Ransomware is a type of vulnerable software which blocks access to the computer's data and threatens to delete important data until a ransom amount is being paid. The computers which are targeted and running on Windows, Microsoft operating systems by demanding payments in the Bitcoin cryptocurrency. It was Possible through EternalBlue, by The Shadow Brokers a few months before the attack. The Microsoft had stopped giving services to the specific operating systems. But almost all the Windows systems that were past their end-of-life. Wanna Cry also took advantage of installing backdoors onto infected systems

KEYWORDS: Ransomware, Wanna Cry, Encrypt, Decrypt, Preventive Measures, Threat & Security

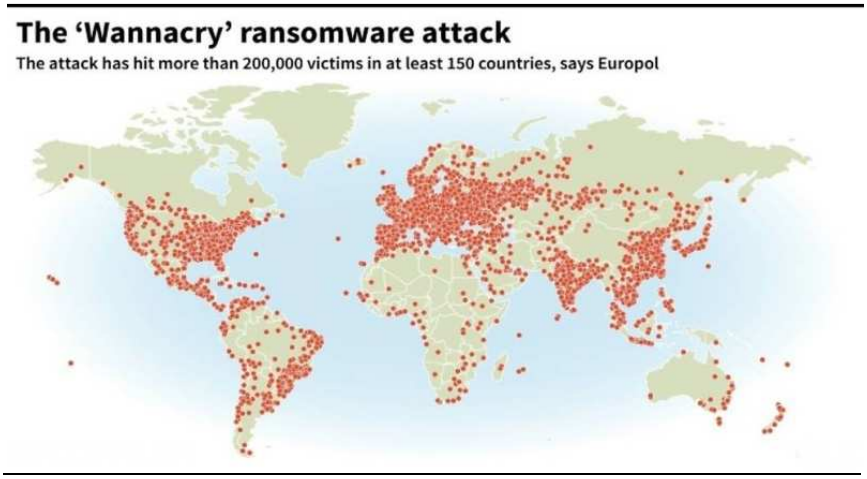
INTRODUCTION

A Wanna cry Ransomware cyber attack occurred in wide range On May-2017, Wanna Cry malicious has spread to over 300,000 systems in over 150 countries. Targeting machines which are running on Microsoft Windows operating systems. This Malicious software contained a URL, and victim's system gets infected using phishing emails, Wanna Cry spreads through SMB (Server Message Block protocol) operating the ports 445 and 139, used by Windows machines to communicate with file systems over a network. Once malicious is installed successfully, then ransomware scans for disk devices. Wanna Cry checks to see if any backdoors are available to enter into the machines. Here mainly two things are using 1. DoublePulsar and 2. EternalBlueto exploits the SMB.

Everything is done smoothly on one click, effortlessly and efficiently maintained. Digitization has improved the lifestyle of the computer users. But still, it creates a problem of security for personal and confidential information of an individual. Wanna Cry was having only one agenda to extort ransom, from victims until then nothing is being released extortive malware took control of files, disks and locks computers. The malware demanded a ransom of $300-600 to be paid within three days in return for decrypting the files and disks.

Figure 1: Wana Decrypt0r 2.0 Lock Screen

CONSEQUENCES ON THE MODERN WORLD



Map shows Wanna Cry Infections around the World in May 2017

TECHNICAL ANALYSIS OF THE ATTACK

The hacker and creator of the Wanna Cry have made world technical experts think in different ways to protect their data from such a massive cyber attack. Which targeted vulnerable Windows PCs around the world using the "EternalBlue" SMB exploit and DoublePulsar is a malicious backdoor malware developed by the NSA to install Wanna - Cry on the systems which are vulnerable.

Eternal Blue the Piggybacking System is an SMB protocol exploit in Windows systems. And this is how it all starts with the EternalBlue exploit.

Eternal Blue home runs a script on the targeted Windows computers executing the following commands:

- Sends an SMB echo request to the target machine with an intent time limit.
- Set up the environment to exploit the vulnerable systems which are running on the Microsoft Windows Operating System.

- Completes SMB protocol fingerprinting.
- Attempts to the exploit attack with proper and well planning.
- If successful, checks for DoublePulsar malware.
- Pings DoublePulsar for an SMB, soon after it replies to the hackers

Along with Eternal Blue, DoublePulsar Malware is also played a very big part in the supportive tool of blue eternal to hack a targeted machine. Which bypasses the authentication of systems and creates a backdoor entry for remote access. Without any user intervention. Double Pulsar transfers the control of your system in the hands of the hackers successfully. Double Pulsar allows hackers to install any malicious code they choose. Example like Wanna cry on the exploited System.

WANNACRY CYBER ATTACKCONSEQUENCES ON THE MODERN INDIA

Wanna Cry attack known as a Mega Cyber Attack which is already a global phenomenon**.** The impact of the malware on India appears to be minimal, as compared to worldwide reports. Our Study shows that there is zero impact on India because 70 percent of Indian computers use unlicensed software.

A report from cyber security company F-Secure suggests that Russia and China were the biggest victims of the attack. Survey says that India was almost safe from data.

CONCLUSIONS

The best way to protect our data against such malicious attacks is to have all files backed up completely in a separate system. Malicious Ransomware can be sent through various sources like Emails, Advertisement, by creating websites and many more things that can share the malicious ransomware to the computer users. Ensure that vulnerability management of always is on high priority, including patch management and vulnerability scanning is very much necessary to keep our data and system safe. Stay safe and don't forget the best protection is always a backup!

REFERENCES

1. Hiran V. Nath and Babu M. Mehtre, "Static Malware Analysis Using Machine Learning Methods", International Conference on Security in Computer Networks and Distributed Systems, 2014.
2. Kharraz A., Robertson W., Balzarotti D., Bilge L., Kirda E., "Cutting the
3. Gordian Knot: A Look under the Hood of Ransomware Attacks"". In: Almgren M., Gulisano V., Maggi F. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA. Lecture Notes in Computer Science, vol 9148. Springer, Cham, 2015.
4. MattiasWeckstén, Jan Frick, Andreas Sjöström, Eric Järpe, "A novel method for recovery from Crypto Ransomware infections", Computer and Communications (ICCC), 2016 2nd IEEE International Conference.
5. Pathak, P B**."**Malware a Growing Cybercrime Threat: Understanding and Combating Malvertising Attacks",2016,

6. 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

7. 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