WannaCry Ransomware Jeopardises the World

Twishish Shrimali[1], Dhruv Kapoor[2], Shagun Malhotra[3]

[1]*Software Developer, R&D Department, Vinytics Peripherals Pvt. Ltd, New Delhi, India*

[2]*System and Network Engineer, TNS Networking Solutions, New Delhi, India*

[3]*Electronics Design Engineer, R&D Department, Vinytics Peripherals Pvt. Ltd, New Delhi, India*

Abstract- **This paper attempts to discover the furtive features of ransomware. It intends to analyze the Ransomware attack Wannacry that unnerved many countries and cyber security specialists on May 2017, and to help academic researchers and IT Specialists in understanding the characteristics of the attack .As the ransomware attacks have become more sophisticated and use complex algorithms, it can be intractable to decrypt the data without having the decryption key. This article will suggest necessary precautions that will benefit the users and the organizations in the long run.**

Index Terms- **Cyber Security, Ransom ware, Wanna Cry.**

I. INTRODUCTION

What is Ransomware?

Ransomware is a type of malicious software that blocks the access to victim’s data until a ransom is paid. It block’s the access to victim’s data. Ransomware can lock the victim’s computer, prohibiting the access to all the data whereas some more advanced malwares use crypto virology. Crypto virology is the study of designing powerful malicious software to infect the victim’s computer by encrypting the data.

It is very difficult to trace the attacker as the ransom taken by the victim is in the form of cryptocurrency, Bitcoin being the most popular amongst all. Ransomware attacks are carried out with the help of Trojans. The attack is disguised as a legitimate file and once it is opened in the target computer, all the files get encrypted. An example of Ransomware attack is below.

II. ECONOMICS OF RANSOMWARE

For professional attackers, developing a ransomware and deploying it is a challenging and dangerous task. But the intrepid attackers ignore the risks due to the potential high profits from the attack. The ransom the attackers charge can go more than $200 USD from a single computer. The outcome can be catastrophic if the entire network is infected and multiple computers have been compromised. According to Symantec, estimates provided by Europe based financial institution depict high earnings by ransomware.

III. SHOULD YOU PAY THE RANSOM?

Necessary precautions should be taken so that the victim is not stuck in a cobweb during the attack. It is strictly not advisable to pay the ransom to the attacker unless no options are left. Also, it is not necessary that paying the ransom will give the access to the data. The following flowchart explains when an individual or an organization should consider paying the ransom.

IV. WANNACRY

WannaCry ransomware attack infected the world in May 2017. It target the Microsoft Windows operating systems by encrypting the data and demanding the ransom from the victims. Some of the Conglomerates like FedEx, Spain’s Telefonica and Deutsche Bank were infected along with innumerable other reported and unreported victims. Marcus Hutchins, 22 year old web security researcher from England discovered an effective kill switch by registering a domain name he found in the ransomware. This slowed down the spread of the attack, but later versions had no kill switches. Though, Microsoft detected this vulnerability and patches for Windows Vista, Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2012 and Windows Server 2016 were released on March 14, 2017. Even after two months of the released users didn't updated the patches and were infected by the ransomware. WannaCry used the vulnerability Eternal Blue to spread itself. Microsoft released and emergency update on next day of the attack for Windows 7 and Windows 8. Microsoft even released the security patch for some of its older operating systems Windows XP and Windows Server 2003. The majority of the victim's computer were running unpatched version of Windows 7. WannaCry left crippled computers in more than 150 countries, earning billions of dollars in bitcoin currency. The ransomware was shared in the form of an email attachment. Once the attachment was clicked, the data was encrypted and a notice with time period to pay the payment was displayed. While it is believed that the attacker may be from Ukraine, there is no substantial evidence to support and the identity of the attacker is still obscured.

V. PRECAUTIONS

Though the scars of WannaCry may not fade quickly, learning from it can save from similar attacks in future. Some of the precautions are discussed below.

1. Operating System Updated

The operating system should always be updated to the latest version. Just keeping the operating system updated can save it from many attacks.

2. Antivirus Installed

An antivirus should be installed and it should be updated frequently to keep the algorithms of the antivirus updated so that computer is secured.

3. Monitor Online Behaviour

The online behaviour of the user or employees should be monitored. It should be made sure that no unknown links or attachments are to be opened or downloaded. Connecting to unknown networks should also be avoided.

4. Avoid Piracy

Usually the pirated software contains Trojans, Key loggers, Viruses etc. which can share the information with the hackers and they can misuse it. It is strictly advisable to stay far away from Piracy.

5. Immediate Shutdown

In case the attack has been initiated, the users should immediately shutdown the system and disconnect it from network so that no information is shared with anyone.

6. Data Backups

There are various software that automatically take backup of the desired files. A small investment in these software is necessary. Backups should be encrypted by the user and should be stored at multiple locations. It should be stored on flash drives and cloud simultaneously. Keeping multiple copies will increase your chances of recovery during the attack.

VI. CONCLUSION

Microsoft releases a one-time patch for old systems that are vulnerable including Windows XP. User will always safe if he updates his computer regularly as Microsoft have also released different new tools that can decrypt your files and keep your computer safe from different types of ransomwares. Another important point is that user should always keep a backup of their important data to avoid these types of attacks.

ACKNOWLEDGEMENT

We take this opportunity to thank all those who motivated us to research on Ransomware and publish our paper. We also want to thank Symantec Security Response for sharing their invaluable information about Ransomware with the public.

REFERENCES

[1] Geoff McDonald, Gavin O'Gorman – Ransomware a growing menace

[2] The Wall Street Journal, America – www.wsj.com

[3] https://thehackernews.com/2017/05/wannacry-ransomware-unlock.html

[4] https://www.infosecurity-magazine.com/news/microsoft-xp-patch-wannacry/

[5] Wikipedia - The Free Encyclopaedia https://en.wikipedia.org.