RANSOMWARE AND ITS IMPACT IN INDIA - A LITERATURE STUDY

Kv Saiphani*1  G Venugopal*2
*1 Assistant Professor, Computer Science Engineering
*2 Nalla Narasimha Reddy Educational Society’s Group of Institutions

Abstract— In these days many countries in the world are suffering by one of the most popular cybercrime called ransomware attack. Through a literature study, this paper discusses effects of wannacry ransomware, the type of ransomware attack in India. In emerging economies like India where the government is running digital programs as flagship schemes to digitally empower society and knowledge economy, Ransomware attacks have become a grave threat. It can affect both, the safety and well-being of users. In this needy web world, how critical is to use a non-secure connection and how it will track a normal user or unaware user into the catch of hacker and after that losing money in terms of bit-coins. The damage cause by the latest attack of ransomware in India is due to the company professionals and security researcher’s unawareness and they didn’t take precautions even after seeing the effected countries like UK and Russia etc. By this reason India was one among the three countries worst affected by the attack.

Keywords— Ransomware, bit-coins, Wanna-Cry 2.0, malware, worm, victim’s, payment.

I. INTRODUCTION

Ransomware: Ransomware is a program that gets into your computer, either by clicking on the wrong thing or downloading the wrong thing that is Ransomware is a type of malicious software from crypto-virology [1] that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While more advanced malware uses a technique called crypto-viral extortion, in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them [1] this whole strategy of Ransomware is shown in figure 1.

Wannacry 2.0: Wanna-Cry, also known as WanaCrypt0r 2.0, Wanna--Cry and W-Cry, is a form of "ransomware" that locks up the files on your computer and encrypts them in a way that you cannot access them anymore.

Malware: "Malware" is short for malicious software and used as a single term to refer to virus, spy ware, worm etc. Malware is designed to cause damage to a standalone computer or a networked pc.

Bit-Coin: It is the form of crypto-currency; it means they do not have any physical form. The main advantages of bit-coins are they are stored in anonymous digital wallets. It can be transferred anywhere in the world via the Internet. It can be paid from anywhere, to anywhere with full anonymity. It is commonly abbreviated as BTC [3].

II. COMMON TYPES OF RANSOMWARE:

1) Locker Ransomware: This is also known as computer locker. This ransomware doesn't encrypt the files of the victim but instead, it denies the access to the device. This locks the device's user interface and then demands the victim for the ransom [4]. “Reveton” [3] is the example of this type.
2) Crypto Ransomware: Crypto ransomware is as simple as weapon using strong encryption against victims to deny them access to those files. Once the ransomware infiltrates the victim's device, the malware silently identifies and encrypts valuable files. Only after successfully accessing to target files has been restricted does the ransomware ask the user for a fee to access their files. The types this Crypto Ransomware are Crypto-Locker, Crypto-Wall, CTB-Locker, Wanna-Cry etc., all are shown in fig 2 [3] [4].

3) Mac Ransomware:

a) KeRanger: KeRanger is believed to be the first piece of ransomware to successfully infect Mac computers running OS X. KeRanger was injected into the installer of an open source bittorrent client called Transmission, so users who downloaded the infected installer were infected with the ransomware when they ran it. Once infected, the ransomware waits three days and then encrypts about 300 different file types, downloading a text file containing a ransom demand of one Bitcoin and instructions on how to pay [4].

III. IMPACT OF WANNACRY RANSOMWARE IN INDIA:

A massive ransomware attack, which security researchers say “used a Windows exploit first developed by the United States National Security Agency, shut down computer systems across several countries, including India”. The malware encrypts all the data on a computer system and decrypts it only after the computer user/owner agrees to pay a ransom, usually in bit-coin.

The ransomware - Wanna-Cry - demanded payments between $300 (around Rs 19,000) and $600 (around Rs 39,000) in bit-coin to unlock data on a single system, news agency Reuters reported. Figure 3 shows the message that displayed by the Wanna-Cry Ransomware.

What we know so far:

1. Anti-virus provider Kaspersky conducted an analysis of the cyber-attack and noted that India was among the three countries worst affected by the attack. Around five per cent of the computers infected by Wanna-Cry 2.0 were in India.

2. Gujarat: In Gujarat, over 120-odd computers connected with GSWAN (Gujarat State Wide Area Network) were affected by the Wanna-Cry ransomware attack. However, no “crucial data” has been lost in the cyberattack, claimed the state government officials [5].

3. Odisha: A government-run hospital in Ganjam district, Odisha, was targeted by the Wanna-Cry ransomware virus. The data and information management system at Berhampur City Hospital, which is located nearly 170 kilometres from Bhubaneswar, was infected by the virus which in turn affected its e-medicine and data services [5].

4. West Bengal: At least 10 computers at customer care centres of West Bengal State Electricity Distribution Company Limited (WBSEDCL) were attacked in West Midnapore, South Dinajpur and East Midnapore districts [5].

5. Andhra Pradesh: According to the Ministry of Electronics and Information Technology (MeitY), few computers of the Police Department in Andhra Pradesh were disabled due to the attack, reported PTI [5].

6. Maharashtra: The Maharashtra Police department was also partially hit by the Wanna-Cry
ransomware. Other isolated incidents were reported in Mumbai and Pune as well.

7. Kerala: Computers in two panchayat offices in Wayanad and Pathanamthitta districts too were disabled by the cyber-attack. Four computers at Thariyathodu panchayat in Wayanad and two computers at Aruvappulam panchayat in Pathanamthitta district were hit [5].

8. Tamil Nadu: Few isolated incidents were reported from the southern state.

9. Delhi: The national capital also reported incidents of the attack as well [5].

10. Railways: Computers of the Southern Railways’ Palakkad division came under attack on Tuesday, but luckily was limited to those in the personnel department that deals with staff matters such as appointments, transfers and promotions etc. The Railways said 23 of the 500 systems located in various departments of the office were targeted.

IV. HOW IT WORKS:

1. Wanna-Cry uses a Microsoft Windows exploit that was made public after a group of hackers called Shadow Brokers released files and hacking tools purportedly belonging to the American NSA, US's premier signals intelligence agency.

2. The malware, Wanna-Cry, uses an exploit named Eternal-Blue to infect computers running versions of Windows operating systems. Eternal-Blue was first made public after Shadow Brokers released a bunch of exploits and hacking tools developed by the US NSA. According to tech website Ars Technica, the NSA used Eternal-Blue to hack and remotely take over computers running Windows.

3. Wanna-Cry works by encrypting all the data on a computer system by changing file extension names to ‘.WNCRY’. The malware then displays a window informing users that their files have been encrypted and that they can be recovered in lieu of a pay-ment made in bit-coin. The window is accompanied by two timers - one counting down to a certain time after which the ransom amount will be raised while the other warns of the time after which users’ files will be gone for good.

5. Responding to cyber-attack, Reuters reported Microsoft saying that it was pushing out automatic updates to defend Windows systems from the Wanna Cry attack. "Today our engineers added detection and protection against new malicious software known as Ransom: “Win 32. Wanna-Crypt”: a Microsoft spokesman said in a statement.

VI. HOW CAN PEOPLE PREVENT ATTACKS LIKE THESE?

Users should regularly back up their data and ensure that security updates are installed on your computer as soon as they are released. Up-to-date backups make it possible to restore files without paying a ransom. The below table 1 suggest some solutions for different peoples to protect them from that threat.

<table>
<thead>
<tr>
<th>FOR ORGANIZATIONS</th>
<th>FOR EMPLOYEES</th>
<th>FOR IT ADMIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block SMB (Server Message Block) port access and RDP (Remote Desktop Protocol) to all systems from the web Port 445 and 139 for SMB and 3389 for RDP must be blocked.</td>
<td>Do not open attachments from unknown sources and don’t open/download unauthorized software.</td>
<td>Redistribute network shares with write permissions.</td>
</tr>
<tr>
<td>Disconnect from the web and take backup of all the data on an encrypted, removable hard drives.</td>
<td>Give a notice to all employees to not open unknown messages and emails too if in doubt read them on mobiles.</td>
<td>Update end point security solution, enable anti-malware sections.</td>
</tr>
<tr>
<td>Block SMB within the organization through a group policy or other any endpoint security solution.</td>
<td>Don’t check personal emails on firm computers as most free email services will not have any advanced scanning.</td>
<td></td>
</tr>
</tbody>
</table>
Some technical details on how to protect against Wanna-Cry:

1. Apply Windows update MS17-010.
2. Disable the outdated protocol SMBv1.
3. Add a rule on your router or firewall to block incoming SMB traffic on port 445.
4. Enable Windows Defender Antivirus to detect this ransomware. (It identifies the ransomware as Ransom:Win32/WannaCrypt as of the 1.243.297.0 update)
5. Use Office 365 Advanced Threat Protection, which can block dangerous email threats, such as the emails carrying ransomware using its machine-learning capability.

VII. THE IDEA FOR STOP SPREADING OF WANNACRY RANSOMWARE:

Firstly, we want to know that is that Wanna-Cry is so special? Yes, Wanna-Cry is not just a ransomware program, it's also a worm. This means that it gets into your computer and looks for other computers to try and spread itself as far and wide as possible. Ransomware has a habit of mutating and so it changes over time in order to find different ways to access computers or to get around patches (operating system updates that often include security updates). Many security firms are already aware of Wanna-Cry in past forms and most are looking at this one right now to see how it might be stopped.

The troublesome ransomware did have its impact globally but a small mistake by the cyber-criminals helped a young security researcher discover a "kill switch" that can disable all functionality of the "WanaCrypt0r 2.0" (or Wanna-Cry or W-Cry) ransomware and stop it from spreading further, at least for now, according to an International Business Times report.

After running the ransomware on a victim's computer, the Wanna-Cry ransomware tries to connect to an unregistered domain. The 22-year-old researcher came across this domain and found that registering the domain name prevented it from spreading.

According to the researcher, "a bit of analysis" led him to the discovery of this unregistered domain, but finding the kill switch was accidental.

VIII. CONCLUSION:

Although cyber extortion cases have been rising for several years, they have to affected small-to-mid sized organizations, disrupting services provided by hospitals, police departments, public transportation systems and utilities. Now ransomware is affecting larger companies with more sophisticated security operations. So there is a chance that the cyber criminals start to target big corporations but some of them may not be well prepared for such attacks. The paper will provide wrathful information about ransomware and its working, prevention techniques to help such types of corporations. IX. FUTURE STUDY: This paper will provide countermeasures for the ransomware, but in this fast growing digital awareness in India, there may be a new cyber attack introduce at any moment. So, in future as the new attack introduces we will back with the countermeasures of it too.

REFERENCES


@IJRTER-2017, All Rights Reserved 276