A STUDY ON WANNACRY RANSOMWARE ATTACK

K.V.G.N.NAIDU¹ AND P.SIREESHA²

¹Assistant Professor, Department of CSE, SoET, SPMVV, Tirupati, A.P, India
²Assistant Professor, Department of CSE, NIST, JNTUA, Rajampet, Ap, India

Abstract- The WannaCry ransomware attack is one of cyber attack, this ransomware warm effecting the Windows Operating System users, this warm encrypring data and demanding ransom payments in the form of Bitcoins.

Keywords— WannaCry, ransomware, bitcoins

I. INTRODUCTION

A cyberattack is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyber attacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft.

Cyberattack is also known as a computer network attack (CNA). Cyberattacks may include the following consequences:

- Identity theft, fraud, extortion
- Malware, pharming, phishing, spamming, spoofing, spyware, Trojans and viruses
- Stolen hardware, such as laptops or mobile devices
- Denial-of-service and distributed denial-of-service attacks
- Breach of access
- Password sniffing
- System infiltration
- Website defacement
- Private and public Web browser exploits
- Instant messaging abuse
- Intellectual property (IP) theft or unauthorized access

The WannaCry ransomware attack is one of the largest ever cyber attacks affecting computers across the globe, Ransomware is a particularly nasty type of malware that blocks access to a computer or its data and demands money to release it.

WANNACRY ROUNDUP: ALL THAT HAPPENED:

On 12th May 2017, media reports started highlighting that a ransomware attack had brought down computer systems in UK hospitals. It soon emerged that the attack was global with reports of affected computers coming in from all over the globe.

The ransomware - WannaCry - infected computers and encrypted all the data stored on the hard drives. In lieu of decrypting the data, WannaCry demanded payment ranging between $300 (around Rs 19,000) to $600 (around Rs 39,000) in bitcoin.

As of 13th May 2017, no hacker or hacker group had come forward to claim responsibility for the cyber attack, which used an exploit first developed by the US NSA. The European Cybercrime Centre said, "The recent attack is at an unprecedented level and will require a complex international investigation to identify the culprits.

Some experts said the threat had receded as of 14th May 2017, in part because MalwareTech registered a domain that he noticed the malware was trying to connect to, limiting WannaCry's spread. Microsoft also issued emergency security patches for a range of Windows versions. The Indian Computer Emergency Response Team (ICERT or CERT-In) was said to be monitoring the situation continuously. Earlier on 13th May 2017 CERT-In was reported to have issued an advisory asking computer users in India to upgrade their systems to the latest Windows patch level.
the social security system had to disconnect its computers and cancel public access. The state-owned oil company Petrobras and Brazil's Foreign Ministry also disconnected computers as a precautionary measure, and court systems went down, too. In Russia, government agencies insisted that all attacks had been resolved. Russian Interior Ministry, which runs the national police, said the problem had been "localized" with no information compromised. Russia's health ministry said its attacks were "effectively repelled." Germany's national railway said on 13th May departure and arrival display screens at its train stations were affected, but there was no impact on actual train services. Deutsche Bahn said it deployed extra staff to help customers. French carmaker Renault's assembly plant in Slovenia halted production after it was targeted. Radio Slovenia said Saturday the Revoz factory in the southeastern town of Novo Mesto stopped working Friday evening to stop the malware from spreading. Elsewhere in Europe, the attack hit Spain's Telefonica, a global broadband and telecommunications company, and knocked ticketing offline for Norway's IF Odd, a 132-year-old soccer club.

"I believe many companies have not yet noticed," said William Saito, a cyber security adviser to Japan's government. "Things could likely emerge on Monday" as staff return to work. China's information security watchdog said "a portion" of Windows systems users in the country were infected, according to a notice posted on the official Weibo page of the Beijing branch of the Public Security Bureau on 13th May. Xinhua state news agency said some secondary schools and universities were hit.

II. HOW IT WORKS

Most ransomware is spread hidden within Word documents, PDFs and other files normally sent via email, or through a secondary infection on computers already affected by viruses that offer a back door for further attacks. When a computer is infected, the ransomware typically contacts a central server for the information it needs to activate, and then begins encrypting files on the infected computer with that information. Once all the files are encrypted, it posts a message asking for payment to decrypt the files – and threatens to destroy the information if it doesn’t get paid, often with a timer attached to ramp up the pressure. WannaCry is asking for $300 worth of the cryptocurrency Bitcoin to unlock the contents of the computers. Over 200,000 systems around the world were affected in the Wanna Cry attack. Wanna Cry ransomware attack is largest ever cyber attack in 2017, it wrecked havoc and shut down tens of thousands of computer systems across 104 countries.

Fig: Phases of Ransomeware attack
Wanna Cry, researchers say, uses an exploit first developed by the United States National Security Agency. The exploit called EternalBlue was first made public in April 2017 after a group of hackers called Shadow Brokers released data and hacking tools purportedly belonging to the NSA. NSA is the US's premier signals intelligence agency that has for long been associated with both offensive as well as defensive cyber capabilities. The attack fueled concerns that the international intelligence community, specially the US's NSA, often does not make public information about vulnerabilities in technology products.

![Screen which appear after ransomeware attack](image)

**Fig:** Screen which appear after ransomeware attack
cyber security expert Edward Snowden said, "Despite warnings, (NSA) built dangerous attack tools that could target Western software," Snowden said. "Today we see the cost".

<table>
<thead>
<tr>
<th>Table: List of organization Affected by WannaCry ransomware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Andhra Pradesh Police</td>
</tr>
<tr>
<td>Automobile Dacia</td>
</tr>
<tr>
<td>Chinese public security bureau</td>
</tr>
<tr>
<td>Cambrian College</td>
</tr>
<tr>
<td>CJ CGV</td>
</tr>
<tr>
<td>Deutsche Bahn</td>
</tr>
<tr>
<td>Dharmais Hospital</td>
</tr>
<tr>
<td>Faculty Hospital, Nitra</td>
</tr>
<tr>
<td>FedEx</td>
</tr>
<tr>
<td>Garena Blade and Soul</td>
</tr>
<tr>
<td>Government of Kerala</td>
</tr>
<tr>
<td>Government of West Bengal</td>
</tr>
<tr>
<td>Government of Gujarat</td>
</tr>
<tr>
<td>Harapan Kita Hospital</td>
</tr>
<tr>
<td>Renault</td>
</tr>
<tr>
<td>Russian Railways</td>
</tr>
<tr>
<td>Sandvik</td>
</tr>
<tr>
<td>São Paulo</td>
</tr>
<tr>
<td>Court of Justice</td>
</tr>
<tr>
<td>Saudi Telecom Company</td>
</tr>
<tr>
<td>Sberbank</td>
</tr>
<tr>
<td>Telefónica</td>
</tr>
</tbody>
</table>

so that such vulnerabilities can be used by the agencies for offensive purposes.
RansomWare like WannaCry works by encrypting most or even all of the files on a user’s computer. Then, the software demands that a ransom be paid in order to have the files decrypted. In the case of WannaCry specifically, the software demands that the victim pays a ransom of $300 in bitcoins at the time of infection. If the user doesn’t pay the ransom without three days, the amount doubles to $600. After seven days without payment, WannaCry will delete all of the encrypted files and all data will be lost.

### III. HOW TO PROTECT

- New ransomware variants appear on a regular basis. Always keep your security software up to date to protect yourself against them.
- Keep your operating system and other software updated. Software updates will frequently include patches for newly discovered security vulnerabilities that could be exploited by ransomware attackers.
- Email is one of the main infection methods. Be wary of unexpected emails especially if they contain links and/or attachments.
- Be extremely wary of any Microsoft Office email attachment that advises you to enable macros to view its content. Unless you are absolutely sure that this is a genuine email from a trusted source, do not enable macros and instead immediately delete the email.
• Backing up important data is the single most effective way of combating ransomware infection. Attackers have leverage over their victims by encrypting valuable files and leaving them inaccessible. If the victim has backup copies, they can restore their files once the infection has been cleaned up. However organizations should ensure that backups are appropriately protected or stored off-line so that attackers can’t delete them.
• Using cloud services could help mitigate ransomware infection, since many retain previous versions of files, allowing you to roll back to the unencrypted form.

IV. CONCLUSION

In our opinion, any sort of crime (online or offline) should never be tolerated. The safety and well-being of citizens should be safeguarded. Everyone deserves a right to live in a secure environment, no matter in real-life or on the Internet.

After doing my research on this issue, I understand the motives of cyber-criminals. To a certain extent, I see why some choose to take their political/religious protests online:

- global reach of the Internet
- support is quickly gained
- online protests are sure to get attention
- protestors are less likely to get caught

However, we find cyber-crime more serious than real-life crime, for the sole reason that it usually affects millions of web users at once (as compared to perhaps one bank or store in a real-life robbery). When online business activities are disrupted, its leads to great inconvenience for customers and companies.

With technology being such a big part of our lifestyles today, cyber-crime has no place in it.we fully support measures and plans to battle cyber-crime. For instance, the Philippines made official the Cybercrime Prevention Act of 2012 - a list of laws relating to illegal computer activities. we believe that if more countries follow suit, it would make more cyber-criminals think twice before committing crime. we also agree with this article, which says that co-operation between companies and the police is important in fighting cyber-crime. I feel that the police has to first understand how cyber-criminals operate before they can catch them.

Another point raised in the article is the need for companies to keep up with the developing technology. we see this as a necessary step against cyber-crime. Why because Cyber-criminals come up with more effective hacking methods day-by-day, So Companies have to make sure their security measures are kept updated and consistent.

To conclude, I hope that with the combined efforts of companies, banks and the authorities, we can see a drop in cyberattacks

REFERENCES