"WannaCry",a Ransomeware that changed the status of world's cyber security

NSA's powerful Windows hacking tools leaked online – CNN (April15, 2017)

Created By
Sayeed Bin Mozahid
ID: 151-35-843
Department of Software Engineering
Daffodil Intertaional University

August 15,2017

Contents

1 Case Story

'WannaCry' is a malware which is a scary type of Trojan virus is called "Ransomware". This malware in effect holds the infected computer hostage demands that the victim pay a ransom in order to regain access to the files on his or her computer.

In May 2017, Worldwide Cyberattack by wannacry, where only Microsoft Windows Operating System's computers are suffered. WannaCry encrypt the infected computer file and demanding ransom payments in the Bitcoin cryptocurrency. This attack began on Friday, May 2017 and within a day was reported to have infected more than 2,30,000 computers in over 150 countries. Part of the United Kingdom's **National Health Service (NHS)** was infected where Doctor appointments and operations were canceled and patients' lives were at stake. Other major attacks were made on Spain's **Telefonica**, **FedEx** and **Deutsche Bahn**.

The initial infection was likely through an exposed vulnerable **SMB(Server Message Block)** port, rather than email phishing as initial assumed. Initial stage, the malware executed a computer when it fail to find out "kill switch" domain name and encrypts the computer files, then it try to exploit the SMB vulnerability to spread out to random computers on the Internet and "laterally" to computers on the same network. After encrypted data, it give a message to user and demands a payment of around $300 bitcoin within three days or $600 bitcoin within six days otherwise after seven days, they will destroy all data. As of 14 June 2017, totaling $130,634.77 has been transferred where total of payment 327.

Shortly after the attack began, a young Web Security Researcher from North Devon in England who was named Marcus Hutchins then known as **MalwareTech** discovered an effective 'Kill switch' by registering a domain name which he found in the code of the ransomware.It really slowed the spread of the infection, effectively halting the initial outbreak on Monday, 15 May 2017, but new versions have since been detected that lack the kill switch.

WannaCry malware was first discovered by the United States **National Security Agency (NSA)**. But they used it to create own offensive work, rather than report it to Microsoft. This flaw and the tool to exploit it with malicious software were publicized recently by a hacker group by the name 'Shadow Brokers'.

In 14 March 2017, Microsoft eventually discovered the vulnerability and they issued security bulletin MS17-010 which detailed the flaw and announced that **patches** had been released for all Windows versions that were currently supported at that time.

This Cyber Attack mainly occurs for SMB vulnerability though it began by email phishing. When user updated their computer and removed vulnerability then the infected is slowed. If Microsoft knew this vulnerability before this attack then this incident never happened.

2 Offenses

List to offenses done by the hacker is given below:

1. Hacker has transferred malware by unauthorized email.
2. Hacker was demanding ransom payments.
3. Full Operating System hacked by hacker.
4. Hacker unauthorized access to the computer.
5. Hacker encrypted all confidential data.
6. Hacker tampering with computer source code.

3 Attack on me

Suppose, I am a Windows 7 Operating System user and I am attack by **WannaCry**. After attack, When I turn on my computer then it shows me a message where was written **'Your important files are encrypted. If you want to decrypt, you need to pay.**
You only three days to submit the payments. After that, the price will be double. Also if you don't pay in seven days, you won't be able to recover your file forever and you can pay only by *Bitcoin*'. I didn't find any way to decrypt my data and it has forced to me for paying the ransom.

4 How to Avoid

After this attacked, Microsoft give us some guideline for stay safe:

- Be careful NOT to click on harmful links in your emails.
- Try to avoid visiting unsafe or unreliable sites.
- Don't click on a untrusted link which takes away to an unsafe website.
- If you receive a message from your friend with a link, ask him before opening the link to confirm, (infected machines send random messages with links).
- Keep your files backed up regularly and periodically.
- Use anti virus and Always make have the last update.
- Make sure your windows have the last update close the gap.

5 Reference

- URL: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
- URL: http://edition.cnn.com/2017/05/14/opinions/wannacrypt-attack - should-make-us-wanna-cry-about-vulnerability-urbelis/index.html
- URL: https://answers.microsoft.com/en-us/windows/forum/windows_10 - security/wanna-cry-ransomware/5afdb045-8f36-4f55-a992-53398d21ed07?auth=1
- URL: https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/

All website visiting time on August 14, 2017, at 11:30 am to on August 15, 2017, at 9:20 pm.