Academic Task Title:

WANNA-CRY RANSOMWARE

By

Sr. No.	Registration No	Name of Students	Roll No	Total Marks	Marks Obtained	Signature
1	11816103	Hikmatullah Nasiri	70			
2	11719931	Ibrahim Shehu Sagagi	43			
3	11815937	Muhammad Sabir	69			
4	11700262	Mohammad Rashid Rasooli	04			

Submitted To Ms. Swati

Lovely Professional University
Jalandhar, Punjab, India.

Table of Contents

Introduction

WannaCry is a type of ransomware attack that infected the National Health Service (NHS) and government institutions in China, Russia, the US and most of Europe including other organizations across the globe. India was among the countries worst affected by the WannaCry attack. NHS England was also the victim of a massive ransomware attack resulting in some patients' operations being cancelled.

The attack occurred after the USA's National Security Agency discovered a vulnerability in Microsoft's software called Eternal Blue. This exploit was leaked by a hacker group called the Shadow Brokers earlier that year but the vulnerability was patched by Microsoft as soon as it happened. The problem comes from older versions of Windows or those without Windows Updates, as these were not patched by Microsoft and were left open to attacks. Russia and India were hit particularly hard because Microsoft's Windows XP-one of the operating systems most at risk- was still widely used in these countries.

The attack was halted within a few days of its discovery due to emergency patches released by Microsoft and the discovery of a kill switch that prevented infected computers from spreading WannaCry further. The attack was estimated to have affected more than 200,000 computers across 150 countries, with total damages ranging from hundreds of millions to billions of dollars. Security experts believed from preliminary evaluation of the worm that the attack originated from North Korea or agencies working for the country. In December 2017, the United States, United Kingdom and Australia formally asserted that North Korea was behind the attack. A new variant of WannaCry forced Taiwan Semiconductor Manufacturing Company (TSMC) to temporarily shut down several of its chip-fabrication factories in august 2018. The virus spread to 10,000 machines in TSMC's most advanced facilities.

Ransomware

What is Ransomware?

Ransomware is a malware that stealthily gets installed in our PC or mobile device and holds our files or operating system functions for ransom. It restricts the user from using their device and from accessing their files and demands that the victim has to pay some ransom within three days and if the user fails to do so then WannaCry will delete all of the encrypted files and all data will be lost.

Who is a target for ransomware?

There are several different ways attackers choose the organizations they target with ransomware. Sometimes it's a matter of opportunity: for instance, attackers might target universities because they tend to have smaller security teams and a disparate user base that does a lot of file sharing, making it easier to penetrate their defenses.

On the other hand, some organizations are tempting targets because they seem more likely to pay a ransom quickly. For instance, government agencies or medical facilities often need immediate access to their files. Law firms and other organizations with sensitive data may be willing to pay to keep news of a compromise quiet and these organizations may be uniquely sensitive to leak ware attacks.

What does a Ransomware attack look like?

Ransomware targets our pictures, documents, files, and data that are personally invaluable. We can tell that we are under attack when we see any of the following:

- Ransomware note
- Encrypted files
- Renamed files
- Locked browser
- Locked screen

What are several ransomware types?

Ransomware has shaped into different forms as it incorporates people’s computing habits and use recent technologies. There are two types of ransomware –

- **Lock screen ransomware** shows a full-screen message that prevents us from accessing our PC or files. It says we have to pay money (a “ransom”) to get access to our PC again.

- **Encryption ransomware** changes by encrypting our files so we can't use them. Now, we know WannaCry is a type of Encryption ransomware.

How does WannaCry work?

WannaCry works by encrypting data on a computer that has been infected and then tells the user that their files have been locked and displays information on how much is to be paid and when payment is taken through Bitcoin (a payment medium).

When can a ransomware attack start?

Potential victims can fall into the ransomware trap if they are:

- Browsing untrusted websites.
- Not careful about downloading or opening file attachments which are known to contain malicious code from spam emails. Some possible attachments can be: Executables (.ade, .adp, .ani, .bas, .bat, .chm, .cmd, .com, .cpl, .crt, .hlp, .ht, .hta, .inf, .ins, .isp, .job, .js, .jse, .lnk, .mda, .mdb, .mde, .mdz, .msc, .msi, .msp, .mst, .pcd, .reg, .scr, .sct, .shs, .url, .vb, .vbe, .vbs, .wsc, .wsf, .wsh, .exe, .pif, etc.)
- Office files that support macros (.doc, .xls, .docm, .xlsm, .pptm, etc.).
- Installing pirated software, outdated software programs or operating systems.
- Using a PC that is connected to an already infected network.

How big is the ransomware problem?

Ransomware is a global problem. The US, Italy, Russia, Korea, and Spain saw the most ransomware encounters in 2016.After exploding in the past couple of years, ransomware encounters seem to have begun to decline. However, this trend is not a reflection of the email and exploit kit campaigns that try to install ransomware on computers. All in all, millions of computers still encountered ransomware in 2016.

In 2016, over 200 ransomware families were tracked. Over half of these families were discovered only in 2016, which means that cybercriminals are constantly releasing new ransomware in the wild.

Description

is a ransomware crypto worm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in Bitcoin. The worm is also known as WannaCrypt, Wana Decrypt0r 2.0, WanaCrypt0r 2.0, and Wanna Decryptor. It is considered a network worm because it also includes a "transport" mechanism to automatically spread itself. This transport code scans for vulnerable systems, then uses the eternal-blue exploit to gain access, and the double pulsar tool to install and execute a copy of itself. WannaCry versions 0, 1, and 2 were created using visual C++.

Eternal Blue is an exploit of Windows' server message block (SMB) protocol released by the shadow brokers. Much of the attention and comment around the event was caused by the fact that the U.S. National Security Agency (NSA) (from whom the exploit was likely stolen) had already discovered the vulnerability, but used it to create an exploit for its own offensive work, rather than report it to Microsoft. Microsoft eventually discovered the vulnerability, and on Tuesday, 14 March 2017, 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, these being windows vista, windows 7, windows 8.1, windows 10, windows server 2008, windows server 2008 r2, windows server 2012, and windows server 2016.

Double Pulsar is a backdoor tool, also released by The Shadow Brokers on 14 April 2017. Starting from 21 April 2017, security researchers reported that there were tens of thousands of computers with the Double Pulsar backdoor installed. By 25 April, reports estimated that the number of infected computers could be up to several hundred thousand, with numbers increasing every day. The WannaCry code can take advantage of any existing Double Pulsar infection, or installs it itself.

On 9 May 2017, private cybersecurity company Risk Sense released code on the website github.com with the stated purpose of allowing legal “white hat” penetration testers to test the CVE-2017-0144 exploit on unpatched systems.

When executed, the WannaCry malware first checks the "kill switch" domain name; if it is not found, then the ransomware encrypts the computer's data, and then attempts to exploit the SMB vulnerability to spread out to random computers on the Internet and "laterally" to computers on the same network. As with other modern ransomware, the payload displays a message informing the user that files have been encrypted, and demands a payment of around US$300 in bitcoin within three days, or US$600 within

seven days. Three hardcoded bitcoin addresses, or "wallets", are used to receive the payments of victims. As with all such wallets, their transactions and balances are publicly accessible even though the cryptocurrency wallet owners remain unknown. Several organizations released detailed technical write-ups of the malware, including a senior security analyst at Risk Sense, Microsoft, Cisco, Malwarebytes, Symantec and McAfee.

Attack

The attack began on Friday, 12 May 2017, with evidence pointing to an initial infection in Asia at 07:44 UTC. The initial infection was likely through an exposed vulnerable SMB port, rather than email phishing as initially assumed. Within a day, the code was reported to have infected more than 230,000 computers in over 150 countries.

Organizations that had not installed Microsoft's security update from April 2017 were affected by the attack. Those still running unsupported versions of Microsoft Windows, such as Windows XP and Windows Server 2003 were at particularly high risk because no security patches had been released since April 2014 for Windows XP (with the exception of one emergency patch released in May 2014) and July 2015 for Windows Server 2003. A Kaspersky Lab study reported however, that less than 0.1 percent of the affected computers were running Windows XP, and that 98 percent of the affected computers were running Windows 7. In a controlled testing environment, the cybersecurity firm Krypto Logic found that they were unable to infect a Windows XP system with WannaCry using just the exploits, as the payload failed to load, or caused the operating system to crash rather than actually execute and encrypt files. However, when executed manually, WannaCry could still operate on Windows XP.

Screenshot of the ransom note left on an infected

Defensive Responsive

Experts quickly advised affected users against paying the ransom due to no reports of people getting their data back after payment and as high revenues would encourage more of such campaigns. As of 14 June 2017, after the attack had subsided, a total of 327 payments totaling US$130,634.77 (51.62396539 BTC) had transferred.

The day after the initial attack in May, Microsoft released out-of-band security updates for end of life products Windows XP, Windows Server 2003 and Windows 8; these patches had created in February of that year following a tip off about the vulnerability in January of that year. Organizations advised to patch Windows and plug the vulnerability in order to protect themselves from the cyber-attack. The head of Microsoft's Cyber Defense Operations Center, Adrienne Hall said, that “Due to the elevated risk for destructive cyber-attacks at this time, we made the decision to take this action because applying these updates provides further protection against potential attacks with characteristics similar to WannaCrypt [alternative name to WannaCry].

Researcher Marcus Hutchins discovered the kill switch domain hardcoded in the malware. Registering a domain name for a DNS sinkhole stopped the attack spreading as a worm, because the ransomware only encrypted the computer's files if it was unable to connect to that domain, which all computers infected with WannaCry before the website's registration had been unable to do. While this did not help already infected systems, it severely slowed the spread of the initial infection and gave time for defensive measures to be deployed worldwide, particularly in North America and Asia, which had not been attacked to the same extent as elsewhere.

On 14 May, a first variant of WannaCry appeared with a new and second kill-switch registered by Matt Suiche on the same day. This was followed by a second variant with the third and last kill-switch on 15 May, which was registered by Check Point threat intelligence analysts. A few days later, a new version of WannaCry was detected that lacked the kill switch altogether.

On 19 May, it was reported that hackers were trying to use a Mirai botnet variant to effect a distributed attack on WannaCry's kill-switch domain with the intention of knocking it offline. On 22 May, Hutchins protected the domain by switching to a cached version of the site, capable of dealing with much higher traffic loads than the live site.

Separately, researchers from University College London and Boston University reported that their Pay Break system could defeat WannaCry and several other families of ransomware by recovering the keys used to encrypt the user's data.

It was discovered that Windows encryption APIs used by WannaCry may not completely clear the prime numbers used to generate the payload's private keys from the memory, making it potentially possible to retrieve the required key if they had not yet been overwritten or cleared from resident memory. The key is kept in the memory if the WannaCry process has not been killed and the computer has not been rebooted after being infected. This behavior was used by a French researcher to develop a tool known as WannaKey, which automates this process on Windows XP systems. This approach was iterated upon by a second tool known as Wanakiwi, which was tested to work on Windows 7 and Server 2008 R2 as well. Within four days of the initial outbreak, new infections had slowed to a trickle due to these responses.

What happened if the WannaCry ransom was not paid?

The attackers demanded $300 worth of bitcoins and then later increased the ransom demand to $600 worth of bitcoins. If victims did not pay the ransom within three days, victims of the WannaCry ransomware attack were told that their files would be permanently deleted.

The advice when it comes to ransom payments is not to surrender into the pressure. Always avoid paying a ransom, as there is no guarantee that your data will be returned and every payment validates the criminals' business model, making future attacks more likely.

This advice proved wise during the WannaCry attack as, reportedly, the coding used in the attack was faulty. When victims paid their ransom, the attackers had no way of associating the payment with a specific victim's computer.

There's some doubt about whether anyone got their files back. Some researchers claimed that no one got their data back. However, a company called F-Secure claimed that some did. This is a stark reminder of why it is never a good idea to pay the ransom if you experience a ransomware attack.

Impact

The ransomware campaign was never known before in scale according to Europol, which estimates that around 200,000 computers were infected across 150 countries. According to Kaspersky Lab, the four most affected countries were Russia, Ukraine, India and Taiwan.

One of the largest agencies struck by the attack was the National Health Service hospitals in England and Scotland, and up to 70,000 devices – including computers, MRI scanners, blood-storage refrigerators and theatre equipment – may have been affected. On 12 May, some NHS services had to turn away non-critical emergencies, and some ambulances were diverted. In 2016, thousands of computers in 42 separate NHS trusts in England were reported to be still running Windows XP. In 2018, a report by Members of Parliament concluded that all 200 NHS hospitals or other organizations checked in the wake of the WannaCry attack still failed cyber security checks. NHS hospitals in Wales and Northern Ireland were unaffected by the attack.

Nissan Motor Manufacturing UK in Tyne and Wear, England, halted production after the ransomware infected some of their systems. Renault also stopped production at several sites in an attempt to spread ransomware. Spain's Telefonica, FedEx and Deutsche Bahn were hit, along with many other countries and companies worldwide. The attack's impact is said to be relatively low compared to other potential attacks of the same type and could have been much worse had Marcus Hutchins not discovered that a kill-switch had been built in by its creators or if it had been specifically targeted on highly critical infrastructure, like nuclear power plants, dams or railway systems. According to cyber-risk-modeling firm Cyence, economic losses from the cyber-attack could reach up to US$4 billion, with other groups estimating the losses to be in the hundreds of millions.

A third of NHS hospital trusts were affected by the attack. Terrifyingly ambulances were reportedly rerouted, leaving people in need of urgent care in need. It was estimated to cost the NHS a whopping £92 million after 19,000 appointments were canceled as a result of the attack. The WannaCry ransomware attack had a substantial financial impact worldwide.

Ransomware protection

Now we understand how the WannaCry ransomware attack took place and the impact that it had, let's consider how we can protect yourself from ransomware.

Here are few Security Recommendations:

- Keep your Windows Operating System and antivirus up-to-date.
- Install internet security software
- Regularly back-up your files in an external hard-drive.
- Avoid unknown USBs
- Enable file history or system protection. In your Windows 10 or Windows 8.1 devices, you must have your file history enabled and you have to setup a drive for file history.
- Use OneDrive for Consumer or for Business.
- Beware of phishing emails, spams, and clicking malicious attachment.
- Use Microsoft Edge to get SmartScreen protection. It will prevent you from browsing sites that are known to be hosting exploits, and protect you from socially-engineered attacks such as phishing and malware downloads.
- Disable the loading of macros in your Office programs.
- Disable your Remote Desktop feature whenever possible.
- Use two step authentication.
- Use a safe and password-protected internet connection.
- Use a VPN when using public Wi-Fi

Conclusion

In conclusion ransomware attacks, has proved that their impact can be devastating to small business owners and organization. Ransomware is not only threats to small business and organization it has an impact on people as well. In its public service request report from the FBI, they urge anyone who's suffered a ransomware infection to never pay ransoms because it helps criminals refine their attacks and snare even more victims. The FBI says paying a ransom does not guarantee the victim will regain access to their data; in fact, some individuals or organizations are never provided with decryption keys after paying a ransom.

Cyberwarfare is not a thing of the future now it is here already and how we tackle it depends on the amount a country is willing to invest in its cybersecurity sector which is now seen as a separate division of its own now. Long gone are the days where the blood of millions are shed over a cause with cyber warfare a country can be devastated and be stripped off its critical infrastructure ranging from power plants down to cash dispensing ATMs and broadcasting stations all with the use of computers and programmed hacking tools.

Furthermore, with all the attacks we have seen so far it is safe to conclude that cyber warfare is not only here to stay but getting more and more sophisticated and easy to access such tools with their availability online and in the deep dark web. Lastly, it is no surprise the world powers are decommissioning nuclear warheads and instead building up their cybersecurity portfolio gearing up for what is to come.

Bibliography

- https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
- https://www.geeksforgeeks.org/what-is-wannacry-how-does-wannacry-ransomware-work/
- https://en.wikipedia.org/wiki/EternalBlue
- https://www.kaspersky.com/resource-center/threats/ransomware-wannacry
- https://www.avast.com/c-wannacry
- https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html
- https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html