**Outline**

· This is an individual assignment.

· You will be assigned one of the following virus topics.

· Research your topic to learn about computer malware and to prepare a presentation about your topic.

· Suggested Slide Topics and layout for your presentation is provided below.

· The presentation should be between 5-10 minutes and will be given in front of the class.

· Slides should be shared with Mr. Nestor (p0079141@pdsb.net) via. Google drive.

**Virus Topics**

1. CIH Virus – 1998

2. Melissa Worm – 1999

3. Code Red Worm – 2001

4. Slammer Worm – 2003

5. SoBig.F Worm – 2003

6. My Doom Worm – 2004

7. Stuxnet Worm – 2010

8. Cryptolocker Trojan – 2013

9. ZeroAccess Botnet – 2013

10. Superfish Adware – 2014

11. Locky Ransomware – 2016

12. WannaCry Ransomware - 2017

**Suggested Slide Layout**

1. Overview

· Summarize what is known about the malware

· Provide: Year / Creator / Origin

· Its classification: Virus / Worm / Trojan / DoS Attack / Email Phish, etc.

Wanna Cry was a ransomware worm that spread rapidly across a number of computer networks in May 2017. This malware is linked to the Lazarus Group, which is a cybercrime organization that may be connected to the North Korean government. After infecting a Windows computer, it encrypts files on the PC's hard drive, making them impossible for users to access. Then it demands a ransom payment in bitcoin in order to decrypt them. The WannaCry ransomware consisted of multiple different components. It initially arrived at the computer in the form of a dropper. Once launched, it tries to access a hard-coded URL but if it couldn't do that, it searched for and then encrypted files in order of important formats, leaving them inaccessible to the user. It then displayed a ransom notice, demanding $300 in Bitcoin to decrypt the files.

2. Any Other Interesting Facts

· This will be topic dependent

A number of factors made the initial spread of WannaCry very interesting. Firstly, it struck a number of important and high-profile systems, including many in Britain's National Health Service. Secondly, it exploited a Windows vulnerability that was suspected to have been first discovered by the United States National Security Agency. Lastly, it was linked by Symantec and other security researchers to the Lazarus Group, which is a cybercrime organization that may be connected to the North Korean government.

3. Its Targets

· Target Hardware Type: e.g. PC, Network, Smartphone, etc.

· Target Operating System: e.g. Windows, Mac, Android, etc.

· Target Software Applications

The vulnerability WannaCry exploits lies in the Windows implementation of the Server Message Block (SMB) protocol. The SMB protocol helps various nodes on a network communicate, and Microsoft's implementation could be tricked by specifically crafted packets into executing arbitrary code. And it is believed that the U.S. National Security Agency discovered this vulnerability and rather than reporting it, they developed code to exploit it, which is called EternalBlue. This exploit was in turn stolen by a hacking group known as the Shadow Brokers, who released it on April 8th, 2017. Microsoft itself had discovered the vulnerability a month prior and had released a patch, but many systems remained vulnerable, and WannaCry, which used EternalBlue to infect computers, began spreading rapidly on May 12. It spread through an organization’s network or it could have affected individual users as well. During the outbreak, Microsoft was really angry at the U.S. NSA for not reporting this exploit to them earlier.

4. What it Did

· What it did to Computer Hardware

· What it did to Computer Software

· What it did to Computer Data

The program code is not confusing and it was relatively easy for security pros to analyze. Once launched, WannaCry tries to access a hard-coded URL, which is the so-called kill switch and if it can't, it proceeds to search for and encrypt files in order of important formats, ranging from Microsoft Office files to MP3s and MKVs, leaving them inaccessible to the user. It then displays a ransom notice, demanding $300 in Bitcoin to decrypt the files.

5. How it Worked

· How did it get into a computer

· How did it spread between computers

It initially arrived at the computer in the form of a dropper. This is basically a self-contained program that extracts the application components embedded within itself. Some of these components are an application that encrypts and decrypts data. It has files which contain encryption keys. And it contains a copy of Tor. Once launched, it tries to access a hard-coded URL but if it can’t do that, and as I said before, it searches for and then encrypts files in order of important formats, ranging from Microsoft Office files to MP3s and MKVs, leaving them inaccessible to the user. This malicious worm was spread by an operation that hunts down vulnerable public facing SMB ports and then uses the alleged NSA-leaked EternalBlue exploit to get on the network and then also the NSA alleged DoublePulsar exploit to establish persistence and allow for the installation of the WannaCry Ransomware.

6. Its Effect

· Summarize its Financial impact

· Summarize its User Base impact

The ransomware campaign was unprecedented in scale according to Europol, which estimates that around 200,000 computers were infected across 150 countries. According to Kaspersky Lab, the five most affected countries were Russia, Ukraine, India, United Kingdom and Taiwan. As of 14 June 2017, after the attack had subsided, a total of 327 payments totalling $130,634.77 US dollars had been transferred. 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 cybersecurity checks. Nissan Motor Manufacturing UK in England halted production after the ransomware infected some of their systems. Renault also stopped production at several sites in an attempt to stop the spread of the ransomware. 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 if Marcus Hutchins had not discovered that a kill-switch had been built in by its creator. According to cyber-risk-modelling 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.

7. Its Control

· How was it discovered

· How was it stopped

· How can it be removed

The day after the initial attack in May, Microsoft released emergency security patches for Windows 7 and Windows 8.1, as well as security updates for the end of life products Windows XP, Windows Server 2003 and Windows 8. Organizations were advised to patch Windows and plug the vulnerability in order to protect themselves from the cyber attack. Researcher Marcus Hutchins accidentally discovered the kill switch domain hardcoded in the malware. Registering a domain name for a DNS sinkhole stopped the attack from spreading like 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. Separately, researchers from University College London and Boston University reported that their PayBreak system could defeat WannaCry and several other families of ransomware. A French researcher developed a tool known as WannaKey, which automates this process on Windows XP systems. This approach was followed by a second tool known as Wanakiwi, which was tested to work on Windows 7 and Server 2008 R2. Within four days of the initial outbreak, new infections had been slowed due to these responses.

Resources

<https://www.symantec.com/connect/blogs/bios-threat-showing-again>

<https://www.symantec.com/security-center/writeup/2000-122113-1425-99>

<https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/zeroaccess-indepth-13-en.pdf>