Activity 3 Guide

Ryan Coon

CST-407

Professor Ty Howard

December 24, 2023

Part 1: Malware Categories

Table 2: Malware Definitions

|  |  |
| --- | --- |
| **Malware** | **Description** |
| Virus | 1. Code with malicious behavior. Copies itself to other programs. |
| Trojan | 1. Code that contains unexpected, undocumented malicious features. Often hidden within a useful or legitimate looking program. |
| Worm | 1. Code that copies itself through a network. Usually degrades performance. |
| Rabbit | 1. Code that replicates itself without limit to exhaust resources. |
| Logic Bomb | 1. Code that triggers an action when a certain condition is met. |
| Time Bomb | 1. Code that triggers an action at a certain date. |
|  | 1. Code that intercepts communications or steals data from a user. |
| Botnet | 1. Program controlled remotely by a master "herder." |
| Zombie | 1. A program or entire computer unknowingly under control of a remote master program. |
| Hijack | 1. Code that changes settings in a browser to allow access to websites or redirect browsers to specific sites. |
| Rootkit | 1. Code installed in administrator privileged access mode in an operating system. |
| Backdoor | 1. Code that bypasses normal authentication methods. |
|  | 1. Code that causes advertisements to appear on the user's computer. |
| Ransomware | 1. Code that disables a computer system and requires payment to the perpetrator in order to be reversed. |
| Keylogger | 1. Code to record keystrokes. |
|  | 1. Malicious code written in a scripting language for application commands. |
| Adware | 1. Unwanted software that is installed as a default option during a legitimate installation process of another program. |
| Ddos | 1. Group of computers used to perform a coordinated attack on a targeted resource. Often results in a denial of service event. |
| Boot Sector Infection | 1. Code embedded in the startup process of an operating system that often re-distributes its code on each restart. |
| Polymorphic | 1. Code that can modify itself in order to make it less visible to antivirus software. |
| Zero Day Exploit | 1. Vulnerability of a program that has not yet been discovered by the maker. |
|  | 1. Code within a malware package that accomplishes the goal of the attacker. |
| Resident Process | 1. A program that remains resident in the RAM of a computer and is frequently used by the operating system. |
| Resident Process | 1. A program that has access to the core operations of an operating system which typically requires special credential rights above that of a user process. |
| cryptography | 1. The study of the behavior of a program such as observing the fact that a program modifies its own code or changes other files, or other actions that are common to viruses. |
| Cavity Virus | 1. Virus that can utilize empty or unused spaces within a host file to store itself. This prevents the file from changing size. |
| Kernel Process | 1. A process to compare the initial values of a set of data (or program file) to current values to ensure that the file has not been modified. |

**Table 3. Notorious Malware Programs**

|  |  |  |
| --- | --- | --- |
| 1. Creeper | Year(s) | 1971 |
| Type of Virus | Worm |
| Notorious For | Self replicating computer program |
| Vulnerability Exploited | n/a |
| Remedy | Using the reaper antivirus |
| 2. Melissa | Year(s) | 1999 |
| Type of Virus | Mass mailing macro virus - worm |
| Notorious For | Slowing down Microsoft Outlook and Exchange email servers |
| Vulnerability Exploited | Microsoft Outlook and Exchange servers |
| Remedy | Use Panda Antivirus to remove it |
| 3. ILOVEYOU | Year(s) | 2000 |
| Type of Virus | Worm |
| Notorious For | Overwriting files, copying itself to address book and mass emailing |
| Vulnerability Exploited | Making people think it is a normal text file |
| Remedy | Removal using a Symantec’s tool. |
| 4. Chernobyl | Year(s) | 1998 |
| Type of Virus | Worm |
| Notorious For | Overwrites critical information on systems and drives, destroying BIOS |
| Vulnerability Exploited | Windows 95 and windows 98 operating systems |
| Remedy | Antivirus released by Chernobyl creator |
| 5. Code Red | Year(s) | 2001 |
| Type of Virus | Worm |
| Notorious For | Defacing websites, Dos |
| Vulnerability Exploited | Software distributed with IIS, Buffer Overflow |
| Remedy | Implement effective internet security suite with antivirus |
| 6. WannaCry | Year(s) | 2007 |
| Type of Virus | Ransomware cryptoworm |
| Notorious For | Encrypting data and demanding ransom payment |
| Vulnerability Exploited | Computer with Microsoft Windows operating systems |
| Remedy | Install latest patches and validate security setup |
| 7. Slammer | Year(s) | 2003 |
| Type of Virus | Worm |
| Notorious For | Dos on internet hosts and slowing internet traffic |
| Vulnerability Exploited | Buffer overflow |
| Remedy | A quality antivirus program |
| 8. Jerusalem | Year(s) | 1987 |
| Type of Virus | Logic bomb Dos virus |
| Notorious For | Deletes programs running on a given day, stacking up exe files until computer slows down |
| Vulnerability Exploited | Dos computer systems |
| Remedy | Move infected file to quarantine |
| 9. Stuxnet | Year(s) | 2010 |
| Type of Virus | Worm |
| Notorious For | Targeting programmable logic controllers that control machinery |
| Vulnerability Exploited | Zero day flaws |
| Remedy | Anti virus tools |
| 10. Chameleon | Year(s) | 2013 |
| Type of Virus | Botnet |
| Notorious For | Infecting computers generating website traffic |
| Vulnerability Exploited | Windows pc |
| Remedy | ClamWin or Exterminate it! |

Part 2: Stuxnet, the World’s First Cyber Weapon

1. According to the interviews shown in "Stuxnet Virus Mystery," the U.S. and Israel were the major actors behind Stuxnet. What evidence was used in this cybercrime/cyberwar research to implicate the U.S.?

Reports and analyses from cybersecurity researchers, intelligence agencies, and government officials, which point to the sophisticated nature of the Stuxnet virus and its potential ties to state-sponsored cyber programs. The use of specific technical details and analysis of the Stuxnet code, which indicated the involvement of highly skilled and well-resourced actors, such as nation-states. Insights from whistleblowers and investigative journalists, shedding light on covert operations and collaborative efforts between the U.S. and Israel in targeting Iran's nuclear facilities. It's important to note that the evidence implicating the U.S. in the Stuxnet cyber-attack is based on a combination of technical analysis, insider accounts, and intelligence assessments, which have been widely reported and discussed in the cybersecurity community and the media.

1. Define the following terms and explain how they relate to Stuxnet.
   1. Worm – Stuxnet is a worm that was created and designed to target industrial control systems, specifically those used in the Iranian nuclear program.
   2. Air Gap – air gaps can be used to prevent the spread of malware or other malicious code. Stuxnet was designed to bypass air gaps by using infected USB drives to spread from one network to another.
   3. "Fire and Forget" – used to describe malware that is designed to self-propagate and spread without human intervention. Stuxnet is an example of this.
   4. Zero Day Exploit - A zero day exploit is a vulnerability in software that is unknown to the software vendor. Stuxnet used this exploit to infect systems.
   5. WinCC – is a program that is used to monitor and control industrial processes. Stuxnet was designed to infect WinCC systems and use them to control the centrifuges in the Iranian nuclear program.
   6. PLC – Programmable Logic Controller. These are used to control industrial processes. Stuxnet was designed to infect these via WinCC.
   7. Centrifuge – is a machine that is used to separate liquids or gasses by spinning them at high speeds. These are used in the Iranian nuclear program in which Stuxnet was designed to infect.

### A New Type of Warfare

1. If the United States is the designer and instigator of Stuxnet, there are at least two opinions. For each of the following statements, express the opposing viewpoints' likely counterarguments.

|  |  |
| --- | --- |
| **Viewpoint 1**  **The U.S. Was Reckless and Provocative** | **Viewpoint 2**  **The U.S. Was Precise and Restrained** |
| The United States was reckless in creating a new category of warfare by releasing Stuxnet. They have crossed the line. Since Stuxnet creates physical damage to its victim, it is similar to dropping a nuclear bomb in WWII. The world has changed for the worse and the US should be blamed for putting us all in greater danger. | Iran has declared the destruction of Israel a national priority and sponsored attacks to do so. The U.S. and Israel, in trying to prevent Iran from developing a nuclear weapon, choose to utilize a relatively nondestructive method to disrupt uranium purification. The alternatives to Stuxnet, such as air strikes and special forces or a ground invasion, which would kill people, cause economic damage and political chaos. The U.S. should be *credited,* not criticized, for utilizing a restrained approach in trying to stop a nuclear war. |
| **Contrary Response: What would a contrary opinion say about this charge?** | **Contrary Response: What would a contrary opinion say about this charge?** |
| While creating this work to attack Iran’s nuclear program could have turned out bad, no actual harm was accomplished and war was avoided. The only thing that went wrong with this was that the worm took too long to inflict more damage faster. It was a slow burn attack that allotted Iran time to recover and continue it’s nuclear program. | It was an ill advised attack and we were lucky that war was avoided. Minimal damage was made but it could have been worse. |

1. It has been said that the use of Stuxnet compares with the use of nuclear weapons. Are they the same? What truly makes them different? Justify your rationale.

If Stuxnet was more efficient and was able to accomplish what it was set to, I do feel that this could be the same. Altering centrifuges for nuclear materials could be catastrophic. This reminds me somewhat of what happened in Chernobyl.

1. Do you feel we can compare cyber warfare to traditional conflict? Are the consequences comparable? Justify your rationale.

It all depends if human life is affected at all. If the attacks are just on the government and does not harm civilians, than I believe it is fair.

### Malware Usage and Effectiveness

1. Summarize how Stuxnet works according to the interviews in "Stuxnet Virus Mystery."

Stuxnet works by targeting and infecting industrial control systems, specifically those used in the Iranian nuclear program. It spreads through infected USB drives and exploits zero-day vulnerabilities to gain access to these systems. Once inside, it takes control of the programmable logic controllers (PLCs) and manipulates the speed of the centrifuges used for uranium enrichment, causing physical damage and disrupting the nuclear program. Stuxnet was designed to spread autonomously and operate in a stealthy manner, making it difficult to detect and attribute its origins.

1. According to in "Stuxnet Virus Mystery," why wasn't the Stuxnet attack very effective?

It was not very effective because it was not able to completely destroy Iran’s nuclear program. Although it did cause some damage, but Iran was able to recover and continue their nuclear activities. The experts in the film believe that the attack was not as effective as it should have been because it was not designed as a one-and-done attack. It was instead designed to be a long term campaign of disruption to eventually wear down Iran’s nuclear program.

### Consequences and Conclusion

1. Near the end of "Stuxnet Virus Mystery," the experts comment on weapons treaties that were negotiated in the 20th century. How is it suggested we handle the use of cyber weapons in the future?

It is said that use of cyber weapons in the future should be handled through international agreements and treaties specifically tailored for the digital age. They recommended an International corporation, transparency and accountability, cyber arms controls, and international legal frameworks.

1. Estimate the effectiveness of future cyber weapons. What potential consequences could occur? Present at least 2 examples.

Comparing to how they are now, the effectiveness of future cyber weapons is likely to be significant. This includes potential consequences like widespread disruption of critical infrastructure, economic damage, and even loss of life.

Disruption of critical infrastructure – cyber weapons could be used to disrupt essential services like power grids, transportation systems, and communication networks.

Manipulation of financial systems – cyber weapons could be used to manipulate financial systems like stock markets, banking networks, and digital currencies.

### Malware Analysis

Read "W32.Stuxnet Dossier," located in the topic Resources.

*Intro and Executive Summary*

1. According to the Symantec report, what is the goal and target of Stuxnet?

According to the report, the goal of the Stuxnet worm was to damage Iran’s nuclear program. It also states that Stuxnet was designed to target the Supervisory Control and Data Acquisition systems that control the centrifuges used in Iran’s nuclear program.

1. Explain the techniques used in Stuxnet to accomplish the goals of copying itself, elevating its privileges to admin/root status, delivering its payload, and remaining hidden from view.

Self Propagation – Stuxnet used this to spread the virus around without human intervention. It also was spreadable via removeable media such as USB drives.

Elevating privileges – Once installed on a computer, Stuxnet uses a variety of techniques to elevate its privileges to admin or root status.

Delivering its Payload – it is delivered by modifying the firmware of PLC or industrial control systems.

Remaining hidden from view – Stuxnet uses stealth techniques to avoid detection by antivirus software and firewalls.

1. Summarize the process by which a PLC device, not connected to a network, is infected.

The introduction of the malware – initial step that involves introducing the malware onto the PLC device. This is done via infected USB drives or other removeable media, or even deliberate intrusion into the facility.

Propagation within the network – once the malware is introduces into the system, it propagates from one computer to another exploiting vulnerabilities in the operating systems or other software running on the computer.

Discovery of the PLC – once inside the network, the malware can scan and identify PLC devices.

Exploiting vulnerabilities – once the PLC device is discovered, the malware exploits vulnerabilities in the communication protocols or the device’s firmware to gain access and control the PLC

Execution of malicious commands - Once the malware gains control of the PLC, it can execute malicious commands, such as altering the logic or parameters of the PLC program, leading to disruptions or damage to the industrial processes controlled by the PLC.

References:

Connect the Dots on State-Sponsored Cyber Incidents - Stuxnet. (2010, July). Council on Foreign Relations. https://www.cfr.org/cyber-operations/stuxnet

Eugene Kaspersky discusses the Stuxnet virus on Cybercrimes with Ben Hammersley. (n.d.). Www.youtube.com. Retrieved August 5, 2022, from https://www.youtube.com/watch?v=4oNnSStrc38

Fruhlinger, J. (2022, August 31). Stuxnet explained: The first known cyberweapon. CSO Online. https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html

Login. (n.d.). Login.lopes.idm.oclc.org. https://fod-infobase-com.lopes.idm.oclc.org/p\_ViewVideo.aspx?xtid=109727&loid=400843

Security Response Contents. (n.d.). https://www.wired.com/images\_blogs/threatlevel/2010/11/w32\_stuxnet\_dossier.pdf

Zetter, K. (2014, November 3). An Unprecedented Look at Stuxnet, the World’s First Digital Weapon. Wired. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/