**CST-407 Activity 3 Guide**

Contents

[Activity 3: Malicious Software 2](#_Toc58829517)

[Part 1: Malware Categories 2](#_Toc58829518)

[Malware Vocabulary 2](#_Toc58829519)

[The Registry of Villains 3](#_Toc58829520)

[Part 2: Stuxnet, the World's First Cyber Weapon 5](#_Toc58829521)

[Discovery 5](#_Toc58829522)

[A New Type of Warfare 6](#_Toc58829523)

[Malware Usage and Effectiveness 6](#_Toc58829524)

[Consequences and Conclusion 7](#_Toc58829525)

[Malware Analysis 7](#_Toc58829526)

# Activity 3: Malicious Software

This activity has multiple parts/assignments. All assignments must be completed prior to documentation submission.

## Part 1: Malware Categories

**Overview**

In this activity, students will define malware according to how it behaves and how it is designed, as well as examine famous malware case studies.

**Execution**

Execute this activity according to the following guidelines:

### Malware Vocabulary

1. Review the associated resources located in the topic Resources.
2. Complete Table 2.

**Table 1. Word Bank Suggestions** (Items that might appear in the table of definitions)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Backdoor | Adware | Ransomware | Virus | Keyboard Attack |
| Hijack | Shark Bait | Cavity Virus | Keylogger | Virus Signature |
| Logic Bomb | Grayware | List Agent | Payload | Boot Sector Infection |
| Dungeon | Resident Process | Kernel Process | Bot | Cyclic Redundancy Check |
| Horse | Rabbit | Benign Wolf | Wipeout | Zero Day Exploit |
| Polymorphic | Time Bomb | Spyware | Worm |  |
| Zombie | Disk Dump | Macro Virus | Botnet |  |
| Heuristics | Slipknot | Rootkit | Trojan |  |

**Table 2. Malware Definitions**

|  |  |
| --- | --- |
| **Malware** | **Description** |
|  | 1. Code with malicious behavior. Copies itself to other programs. |
|  | 1. Code that contains unexpected, undocumented malicious features. Often hidden within a useful or legitimate looking program. |
|  | 1. Code that copies itself through a network. Usually degrades performance. |
|  | 1. Code that replicates itself without limit to exhaust resources. |
|  | 1. Code that triggers an action when a certain condition is met. |
|  | 1. Code that triggers an action at a certain date. |
|  | 1. Code that intercepts communications or steals data from a user. |
|  | 1. Program controlled remotely by a master "herder." |
|  | 1. A program or entire computer unknowingly under control of a remote master program. |
|  | 1. Code that changes settings in a browser to allow access to websites or redirect browsers to specific sites. |
|  | 1. Code installed in administrator privileged access mode in an operating system. |
|  | 1. Code that bypasses normal authentication methods. |
|  | 1. Code that causes advertisements to appear on the user's computer. |
|  | 1. Code that disables a computer system and requires payment to the perpetrator in order to be reversed. |
|  | 1. Code to record keystrokes. |
|  | 1. Malicious code written in a scripting language for application commands. |
|  | 1. Unwanted software that is installed as a default option during a legitimate installation process of another program. |
|  | 1. Group of computers used to perform a coordinated attack on a targeted resource. Often results in a denial of service event. |
|  | 1. Code embedded in the startup process of an operating system that often re-distributes its code on each restart. |
|  | 1. Code that can modify itself in order to make it less visible to antivirus software. |
|  | 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. |
|  | 1. A program that remains resident in the RAM of a computer and is frequently used by the operating system. |
|  | 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. |
|  | 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. |
|  | 1. Virus that can utilize empty or unused spaces within a host file to store itself. This prevents the file from changing size. |
|  | 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. |

### The Registry of Villains

Table 3 lists some of the most notorious malware programs in history. Several were first of their kind, others the worst of their kind. All of them are famous among cybersecurity professionals.

1. Complete Table 3. For each malware item, research its history, make a note of when the attack first occurred, what kind of virus it was (trojan, worm, macro, etc.), what kind of weakness (vulnerability) its maker discovered and exploited, and finally, how was the code infection stopped.

**Table 3. Notorious Malware Programs**

|  |  |  |
| --- | --- | --- |
| 1. Creeper | Year(s) |  |
| Type of Virus |  |
| Notorious For |  |
| Vulnerability Exploited |  |
| Remedy |  |
| 2. Melissa | Year(s) |  |
| Type of Virus |  |
| Notorious For |  |
| Vulnerability Exploited |  |
| Remedy |  |
| 3. ILOVEYOU | Year(s) |  |
| Type of Virus |  |
| Notorious For |  |
| Vulnerability Exploited |  |
| Remedy |  |
| 4. Chernobyl | Year(s) |  |
| Type of Virus |  |
| Notorious For |  |
| Vulnerability Exploited |  |
| Remedy |  |
| 5. Code Red | Year(s) |  |
| Type of Virus |  |
| Notorious For |  |
| Vulnerability Exploited |  |
| Remedy |  |
| 6. WannaCry | Year(s) |  |
| Type of Virus |  |
| Notorious For |  |
| Vulnerability Exploited |  |
| Remedy |  |
| 7. Slammer | Year(s) |  |
| Type of Virus |  |
| Notorious For |  |
| Vulnerability Exploited |  |
| Remedy |  |
| 8. Jerusalem | Year(s) |  |
| Type of Virus |  |
| Notorious For |  |
| Vulnerability Exploited |  |
| Remedy |  |
| 9. Stuxnet | Year(s) |  |
| Type of Virus |  |
| Notorious For |  |
| Vulnerability Exploited |  |
| Remedy |  |
| 10. Chameleon | Year(s) |  |
| Type of Virus |  |
| Notorious For |  |
| Vulnerability Exploited |  |
| Remedy |  |

**Documentation**

All documentation will be submitted at the end of the activity to the learning management system. Ensure documentation of the following:

1. A Word document containing completed Tables 2 and 3.

## Part 2: Stuxnet, the World's First Cyber Weapon

**Overview**

In this activity, students will examine how cyber weapons can compromise industrial control systems and the political and social consequences of cyberwarfare, as well as the process of static and dynamic malware analysis used by cybersecurity professionals.

**Execution**

Execute this assignment according to the following guidelines:

1. **Background:** Stuxnet was the world's first cyber weapon directed to harm physical targets and cause real-world damage. Some compare its development to the first use of nuclear weapons in WWII.
2. Review the associated resources located in the topic Resources.
3. Answer the following items. Use complete answers that show your understanding of the issues by providing details and well-reasoned arguments.
4. Make sure to properly reference and cite all examples and supporting evidence.
5. Make sure to utilize appropriate industry terminology.

### Discovery

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.?
2. Define the following terms and explain how they relate to Stuxnet.
   1. Worm
   2. Air Gap
   3. "Fire and Forget"
   4. Zero Day Exploit
   5. WinCC
   6. PLC
   7. Centrifuge

### 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?** |
|  |  |

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

### Malware Usage and Effectiveness

1. Summarize how Stuxnet works according to the interviews in "Stuxnet Virus Mystery."
2. According to in "Stuxnet Virus Mystery," why wasn't the Stuxnet attack very effective?

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

### 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?
2. 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.
3. Summarize the process by which a PLC device, not connected to a network, is infected.

# Submission

Submit the following to the learning management system:

**Part 1**

1. A Word document containing completed Tables 2 and 3.

**Part 2**

1. A Word document containing an analysis of the questions and proposed topics.