# **The Virus Hall of Shame**

Name Angel Velazquez Class ITT-305 Date 10-08-2023

**Objectives:** Identify the strategies and coding designs that viruses use to infect, propagate, avoid detection and cause damage to their victims.

## ***Part 1 – Malware Terminology***

In this section, you will use classroom resources and activities to define the strategies and designs used by malware programs.

## ***Part 2 – The Malware Hall of Fame***

In this section, you will identify several well-known virus attacks and explain which design and anti-detection strategies they employ.

# **Terms about Malicious Software**

Directions: Match the word suggestions below with the correct definition. Not all words are used.

Use the following resources to help define these terms:

* Chapter 3 of the course textbook.
* “MALWARE 101 – VIRUSES” by Aman Hardikar. <https://www.sans.org/reading-room/whitepapers/incident/paper/32848>

| Type of malware | Description |
| --- | --- |
| virus | Code with malicious behavior. Copies itself to other programs. |
| trojan horse | Code that contains unexpected, undocumented malicious features. Often hidden within a useful or legitimate looking program. |
| worm | Code that copies itself through a network. Usually degrades performance. |
| rabbit | Code that replicates itself without limit to exhaust resources. |
| logic bomb | Code that triggers an action when a certain condition is met. |
| time bomb | Code that triggers an action at a certain date. |
| spyware | Code that intercepts communications or steals data from a user. |
| bot | Program controlled remotely by a master “herder”. |
| zombie | A program or entire computer unknowingly under control of a remote master program. |
| browser hijacker | Code that changes settings in a browser to allow access to website or redirect browsers to specific sites. |
| kernel process | Code installed in administrator privileged access mode in an operating system. |
| backdoor | Code that bypasses normal authentication methods. |
| adware | Code that causes advertisements to appear on the user’s computer. |
| ransom ware | Code that disables a computer system and requires payment to the perpetrator in order to be reversed. |
| keylogger | Code to record keystrokes. |
| macro virus | Malicious code written in a scripting language for application commands. |
| grayware | Unwanted software that is installed as a default option during a legitimate installation process of another program. |
| Botnet | Group of computers used perform a coordinated attack on a targeted resource. Often results in a denial of service event. |
| boot sector virus | Code embedded in the startup process of an operating system that often re-distributes its code on each restart. |
| polymorphic | Code that can modify itself in order to make it less visible to antivirus software. |
| zero-day vulnerability | Vulnerability of a program that has not yet been discovered by the maker. |
| virus | Code within a malware package that accomplishes the goal of the attacker. |
| TSR | A program that remains resident in the RAM of a computer and is frequently used by the operating system. |
| rootkit | 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. |
| polymorphic virus | 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 | Virus that can utilize empty or unused spaces within a host file to store itself. This prevents the file from changing size. |
| cyclic redundancy check | 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. |
|  |  |

**Word bank suggestions**

| Keyboard attack  Virus Signature  List agent  Payload  Dungeon  Resident Process | Benign Wolf  Wipeout  Shark Bait  Disk dump  Heuristics  Slipknot |
| --- | --- |

# **Virus Hall of Shame**

The following chart shows some historically significant virus attacks. For each virus mentioned, research the technical aspects of the virus and complete the chart by providing details on its design, damage and remedy.

Here are some video stories about a few of the viruses



Samy Kamkar Takes Down Myspace

<https://www.youtube.com/watch?v=DtnuaHl378M>

Five of the Worst Computer Viruses Ever

<https://www.youtube.com/watch?v=DF8Ka8Jh0BQ>

Five More Viruses You Don’t Ever Want to Get

<https://www.youtube.com/watch?v=wopM3A3tyTw>

The World’s First PC Virus

<https://www.youtube.com/watch?v=AVVnhBDCFDs>

Reverse Engineer of WannaCry Virus

<https://www.youtube.com/watch?v=Sv8yu12y5zM>

For each column in the table, provide the following:

1. Year

Include the year(s) that this virus first was used or became widespread.

1. Type

Type of infections may include, among others, boot sector infection, zero-day exploits, document macro language, worm, self-encrypted or morphing. Some viruses have more than one type of technology to make them effective.

1. Notorious

While there are thousands (millions) of viruses, many of these examples were selected for being the first of their kind or for causing a large interruption.

1. Exploit

A virus often is known for finding a vulnerability in an operating system or human process. What was the key vulnerability that allowed this virus to succeed?

1. Remedy

What technology or change of behavior makes this virus a low threat today?

# **Virus Hall of Shame**

|  | Year(s) | What type of virus was this? | Notorious for | Exploited what vulnerability? | Remedy |
| --- | --- | --- | --- | --- | --- |
| Melissa | 1999 | maco virus | forcing Intel and Microsoft to shut down their email systems | sent a trojan horse in a Word document | having an antivirus software |
| ILOVEYOU | 2000 | worm virus | infecting 50 million systems | sent a trojan horse in a .txt document | deleting virus files on the system |
| Chernobyl | 1998 | stealth virus | being highly destructive with the ability to destroy the bios of a system completely | filled gaps in the hard drives of computers, making it hard to detect | run the kill exe file |
| Code Red | 2001 | worm virus | defacement of sites served by the web server it infected | buffer overflows in certain configs of Microsoft OS | Antivirus software |
| WannaCry | 2017 | ransomware | being a North Korean attack on the states | Windows servers to remotely control systems and spread to other systems | update systems and check all traffic in the network |
| Slammer | 2003 | worm virus | crashing routers globally through dos | targetted vulnerable systems throughout the internet | restart servers often, block udp port 1434 |
| Stuxnet | 2010 | worm virus | shutting down Iran’s nuclear program | having workers on the job by spreading the virus through USB drives | It is no longer a threat |

# **Deliverables**

Complete this document using complete sentences, fully-developed ideas and correct grammar and usage. Submit the entire document.Grading Rubric

| Criteria | % Value | 1: Unsatisfactory | 2: Less Than Satisfactory | 3: Satisfactory | 4: Good | 5: Excellent |
| --- | --- | --- | --- | --- | --- | --- |
| **% Scaling** |  | 0% | 65% | 75% | 85% | 100% |
| **Identify Terminology and Strategies in Malware** | 70% | Missing content or what is provided does not address the question. | Incompletely defines terminology. Does not elaborate fully | Somewhat defines terminology. Does not elaborate fully | Partially defines terminology used. Does not elaborate fully. | Fully and accurately defines terminology, design and case studies used in malware. |
| **Grammar, Style and Spelling** | 30% | Missing content or writing style and organization is very difficult to understand. | Major issues with any of the items of an Excellent rating. | Multiple issues with any of the items of an Excellent rating. | Minor issues with any of the items of an Excellent rating. | Includes fully formed ideas. Logically arranged. No grammar or spelling issues. |