**UNIVERSITY OF INFORMATION TECHNOLOGY, VNUHCM**

**FACULTY OF INFORMATION SYSTEMS**



**PRESENTATION REPORT**

TOPIC: SOLID WALL AGAINST CYBERCRIME

**Course:** SPCH2713.P12.CTTT - Introduction to Speech Communication

**Instructor:** Dr. Đặng Khánh Hưng

**Group 9:**

1. Phạm Vũ Gia Minh 23520948 Leader
2. Trần Đình Duy 23520390 Member
3. Trần Quốc Hải 23520424 Member
4. Phạm Mạnh Hùng 23520575 Member

**Presentation Date:** September 24th, 2024

# ABSTRACT

This presentation consists of two parts. Part 1 mentions viruses that our computers are highly likely to be infected with including file-infecting viruses, worms, and ransomware. In the second part, we aim to clarify how current antivirus software Works, compare the development of antivirus software from year to year, and give you some advice on using Windows Defender and third-party antivirus software.

# Chapter I. Common Computer’s virus.

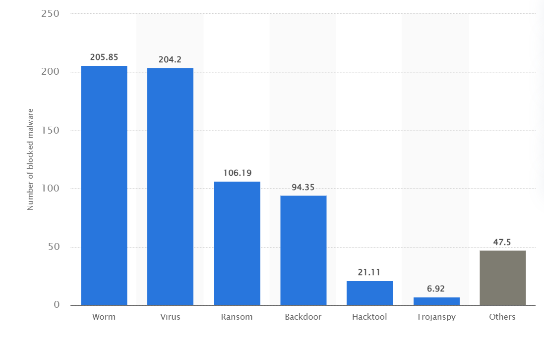


Figure 1. Global most commonly blocked malware 2022

## 1. File-infecting Virus

### 1.1. Key Characteristics

* **Attachment to Executables:** The virus inserts its code into executable files. This makes detection difficult since the virus may be hidden within legitimate software.
* **Execution upon File Access:** When the infected file is executed, the virus activates, allowing it to perform malicious activities such as deleting files, corrupting data, or spreading to other files.
* **Self-Replication:** A file-infecting virus replicates by inserting copies of its code into other executable files, which allows it to spread within the system or to other systems through shared files.
* **Destructive Potential:** Depending on its design, it can modify, delete, or corrupt files and data on the infected system.

### 1.2.  Symptoms

* Slow computer performance
* Unexpected crashes
* Files that become inaccessible or corrupted
* Unusual error messages.

## 2. Worm

### 2.1. Key Characteristics

* **Automatic Spreading Independently:** Worms can replicate themselves and spread without requiring a host file or user interaction. Once inside a system, they copy themselves to other machines, networks, or systems autonomously.
* **Exploits Vulnerabilities:** Worms spread primarily through network connections by exploiting vulnerabilities in software, operating systems, or network protocols with high speed.
* **Consumes System Resources:** As worms replicate, they consume significant amounts of bandwidth, memory, and processing power, often slowing down networks or crashing systems.
* **Command and Control:** Some worms allow hackers to control infected machines remotely, using them to carry out attacks like spamming, data theft, or further spreading of malware.

### 2.2.  Symptoms

* High Memory or CPU Usage
* Unexplained Network Activity
* Appearance of Strange Files or Processes
* Unauthorized Remote Access

## 3. Ransomware

### 3.1. Key Characteristics

* **Encryption**: Ransomware encrypts files on the infected system, rendering them inaccessible without a decryption key, which is often held by the attacker.
* **Ransom Demand**: Victims typically receive a ransom note, detailing how to pay, usually in cryptocurrencies like Bitcoin, to obtain the decryption key.
* **Widespread Impact**: Ransomware can target individuals, businesses, and government entities, causing widespread disruption.
* **Delivery Methods**: It spreads through phishing emails, malicious downloads, or vulnerabilities in software.

### 3.2.  Symptoms

* High Memory or CPU Usage
* Unexplained Network Activity
* Automatic opening and running of programs
* Unauthorized Remote Access

# Chapter II. How antivirus software works.

# Virus definition

Ảnh có chứa văn bản, biểu đồ, Phông chữ, Kế hoạch

Mô tả được tạo tự độngTraditional virus detection methods, like signature detection, rely on comparing program code to known malware signatures stored in a database. While effective, this approach has limitations, especially as new threats continue to emerge.

# Heuristic-based detection

To address the limitations of signature detection, heuristic models were developed to identify suspicious characteristics in both new and modified viruses. Heuristic analysis employs various techniques, including:

1. Ảnh có chứa văn bản, biểu đồ, ảnh chụp màn hình, hàng

   Mô tả được tạo tự động**Static Heuristic Analysis**: This involves decompiling a suspect program and comparing its source code to known malware in a heuristic database. If a certain percentage of the code matches, it is flagged as a potential threat.
2. **Dynamic Heuristic Analysis**: This method tests suspicious programs in a controlled virtual environment or sandbox. The antivirus program simulates running the code and monitors for behaviors typical of viruses, such as self-replication or file overwriting.

However, a significant drawback of heuristic analysis is the potential for false positives, where legitimate files are mistakenly identified as malicious.

# Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ Mô tả được tạo tự độngBehavior-based detection

Threat actors often conceal malicious code to evade static detection methods, using techniques like custom packers with anti-emulation features. This allows newly created ransomware to avoid detection by scans until execution, effectively completing the attack.

To counter such advanced threats, behavior-based detection focuses on analyzing the actions of programs rather than their code. This technique identifies malware by detecting suspicious patterns, such as modifying system files, creating new processes, or unusual resource usage (e.g., CPU, memory, disk, and network activity). By monitoring these behaviors, it can effectively identify malware, including fileless threats, ransomware, and zero-day exploits.

# Real-time Protection

Real-time protection does just what the name suggests: it offers protection in real-time.

Think of real-time antivirus protection as a security guard who never leaves his post, evaluating every person who attempts to pass through and raising the alarm when the unwelcome are detected.

# 5. The development of Windows Defender over the years.

The evolution of Windows Defender has been notable over the years. In December 2014, when many users were still on Windows 7, it performed poorly in AV-TEST evaluations compared to third-party antivirus solutions. However, by December 2015, with the release of Windows 8, Windows Defender showed significant improvements.

Microsoft has consistently enhanced Windows Defender, and by February 2024, it was recognized as one of the best free antivirus options available. Further advancements were noted in June 2024, solidifying its reputation in the cybersecurity landscape.

# 6. Advice on using Windows Defender and third-party antivirus software.

For the most part, yes. The actual security features are effective at what they set out to do. Regarding detecting malware and prompting you with warnings when suspicious things happen, Windows 11 works and you probably don’t need a standalone antivirus solution.

But Windows Security still puts the onus of safety in your hands. Certain features need to be properly configured ahead of time, and the overall protection offered by Windows Security is baseline. You still need to be smart, careful, and aware by:

* Not visiting suspicious websites
* Not downloading unsolicited files
* Not clicking links in emails or social media messages

However, The best free antivirus utilities still give you even more protection with addition features, and they also earn great scores from the independent testing labs.

# REFERENCE

1. <https://www.geeksforgeeks.org/>
2. <https://www.kaspersky.com/resource-center/definitions/heuristic-analysis>
3. <https://www.kaspersky.com/enterprise-security/wiki-section/products/behavior-based-protection>
4. <https://www.av-test.org/en/>
5. <https://www.av-comparatives.org/latest-tests/>
6. <https://www.statista.com/>
7. <https://www.pcworld.com/article/2379676/is-windows-11s-built-in-antivirus-enough-for-normal-everyday-users.html>
8. <https://www.pcmag.com/reviews/microsoft-windows-defender-security-center>
9. <https://www.researchgate.net/>