EVASION TECHNIQUES OF MODERN

COMPUTER VIRUSES

PRESENTED BY:

Ashish Basnet
Pallav Timalsina
Prajwal Shah
Pratik Sharma
Sakshyam Shrestha
Sandesh Pandit Chhetri

INTRODUCTION

Modern computer viruses are malicious programs designed to spread, disrupt, and exploit systems. Over time, they've grown more sophisticated, leveraging stealth and adaptability to evade even advanced cybersecurity defenses. These evolving threats endanger the confidentiality, integrity, and availability of digital information across industries.

TYPES OF COMPUTER VIRUSES

- **File Infectors:** Attach to executables; activate and spread when the host program runs.
- **Macro Viruses:** Hide in document macros (Word/Excel); propagate when a user opens or shares the file.
- **Boot-Sector Viruses:** Infect the MBR/VBR; load at startup to bypass file scanners.
- **Polymorphic Viruses:** Encrypt and mutate their decryption code each time, defeating signature checks.
- **Metamorphic Viruses:** Fully rewrite their own code each generation, evading both signatures and heuristics.

Evolution of Computer Viruses and Antivirus

Theoretical Foundations

John von Neumann's theory laid groundwork

First Experiments

Creeper and Reaper programs emerged

PC Virus Emergence

Elk Cloner and Brain viruses appeared

Commercial Antivirus

Rise of antivirus companies like McAfee

Network-Spread Viruses

Morris Worm and macro viruses spread

Global Outbreaks

ILOVEYOU and Code Red caused damage

Ransomware & Cyberwarfare

CryptoLocker and Stuxnet emerged

EVASION TECHNIQUES OVERVIEW

Code Obfuscation:

1

- **String Obfuscation:** Base64 encoding, XOR, substitution ciphers hide literals.
- **Control-Flow Obfuscation:** Opaque predicates, virtualization-based obfuscators; break straightforward analysis with convoluted branches .
- **Instruction Substitution:** Replace operations with equivalent sequences (e.g., sub rax, imm ↔ add rax, -imm).

EVASION TECHNIQUES OVERVIEW

Packing & Encryption:

2

- **Packers:** Compress/encrypt binaries; runtime unpackers load payload into memory, evading on-disk scanning.
- **Crypting:** Crypter tools wrap payloads in custom encryption layers; polymorphic variants change keys per infection.

EVASION TECHNIQUES OVERVIEW

Polymorphism & Metamorphism:

3

- **Polymorphism:** Mutation engine alters decryptor stubs and keys. Effective against static signatures but detectable by decryptor patterns.

- **Metamorphism:** Complete code rewriting—no fixed decryptor; each iteration appears novel, forcing behavior-focused detection.

EVASION TECHNIQUES OVERVIEW

Advanced Fileless Malware Techniques

4

- Operates entirely in system memory, not on disk.
- Uses legitimate tools like PowerShell and WMI to execute code.
- Leaves no traditional files, making it harder to detect with antivirus.
- Evades signature-based detection since there's no file to scan.

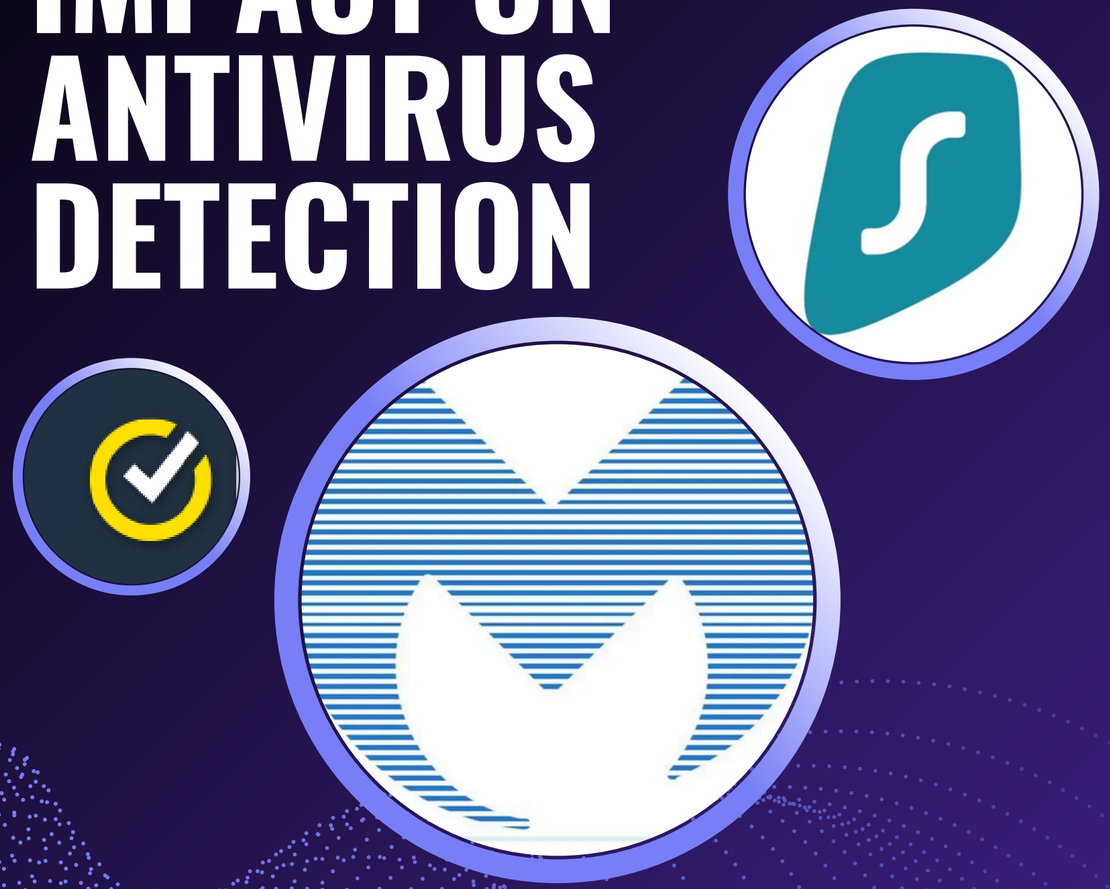
IMPACT ON ANTIVIRUS DETECTION

1. **Signature Bypass**
   Evasive malware alters its code to avoid detection by fixed virus signatures used in traditional antivirus software.

2. **Heuristic Evasion**
   Mimics normal behavior or delays execution, tricking heuristic engines into classifying it as safe.

3. **Sandbox Awareness**
   Detects virtual or sandbox environments and remains dormant to avoid triggering alerts during analysis.

IMPACT ON ANTIVIRUS DETECTION



4 **Memory-Only Execution**

Fileless malware operates in memory, leaving no trace on disk for antivirus to scan.

5 **Antivirus Disruption**

Some malware disables or corrupts antivirus processes, stopping them from detecting or responding.

6 **Overwhelms Detection Systems**

Rapidly mutating variants and obfuscation techniques overwhelm antivirus update and response capabilities.

ADVANCEMENTS IN COUNTERMEASURES

Next-Generation Antivirus (NGAV)

Uses cloud-powered AI and ML to analyze real-time threat data, detect novel malware patterns, and block exploits based on behavioral indicators.

Enhanced Sandboxing

Employs VM randomization and simulates user interactions like mouse movements to detect evasive malware that waits for human behavior.

EDR & XDR Platforms

Provide constant endpoint monitoring, telemetry collection, and threat hunting capabilities, enabling early detection and automated quarantine of infected assets.

ADVANCEMENTS IN COUNTERMEASURES

AI & ML Integration

Incorporates advanced models that can withstand adversarial manipulation and recognize subtle similarities among malware variants using clustering techniques.

Threat Intelligence

Centralizes and enriches Indicators of Compromise (IoCs) and integrates deception mechanisms like honeypots to trap and study evasion tactics.

Cloud-Native Detection

Utilizes scalable infrastructure and collective intelligence to monitor, correlate, and mitigate threats across distributed environments in real-time.

RESEARCH DIRECTIONS & BEST PRACTICES

1. Code semantics and logic flow analysis focuses on what the malware does rather than how it looks, making it effective against obfuscated or metamorphic threats.

2. Hybrid detection frameworks combine static, dynamic, and network-level analysis to improve resilience against complex, evasive malware.

3. Deception technologies use decoys like honeypots and fake credentials to attract and expose stealthy malware in a controlled environment.

CONCLUSION

In today's rapidly evolving threat landscape, virus evasion techniques are becoming increasingly advanced, leveraging stealth, adaptability, and deception to bypass traditional defenses. While signature-based antivirus solutions alone are no longer sufficient, modern layered approaches—combining behavior analysis, memory inspection, AI-driven detection, and proactive threat intelligence—offer a more resilient defense. Continued research, collaboration, and the adoption of intelligent, adaptive tools are essential to outpace attackers. Ultimately, the goal is not just to detect malware, but to anticipate, understand, and neutralize it before damage is done.

REFERENCES

- A. Author et al., “Evasion Techniques Used by Modern Computer Viruses and Their Impact on Antivirus Detection Systems,” Journal of Advanced Information Technology, vol. 15, no. 5, pp. 649–672, May 2025.
- Infosec Institute, Cyfirma, and VMRay, “Comprehensive Guides on Obfuscation and Sandbox Evasion,” accessed May 8, 2025.
- SentinelOne and CrowdStrike, “Threat Intelligence on Polymorphic and Fileless Malware,” White Paper, 2024.

Zscaler and VirtualGuardian, “AI-Driven Malware Research,” Tech. Rep., Jan. 2025.

MITRE ATT&CK, “Process Injection Techniques (T1055) and Impair Defenses (T1562) Frameworks,” MITRE Corporation, 2025.

THANK YOU