CS-011 · Malware

Computer Viruses

Malicious code that attaches to a host file and spreads when that file is run.

Executive Summary

A computer virus is malicious code that inserts itself into a legitimate host file or program and runs when that host is executed. Unlike a worm, a virus needs a user or process to launch the infected file before it can spread. Once active, it can copy itself into other files and deliver a payload that ranges from harmless to destructive.

What It Is

A computer virus is a type of malware that cannot exist on its own. It embeds its code inside a host, such as an executable program, a document with macros, or a boot sector, and it activates only when that host is opened or run. This dependence on a host and on user action is what distinguishes a virus from other malware families. Viruses are usually organized around three parts: an infection mechanism that finds and attaches to new hosts, a trigger that decides when the payload fires, and the payload itself, which is the action the virus performs. Common historical types include file infectors that attach to programs, macro viruses that live inside office documents, and boot sector viruses that load before the operating system.

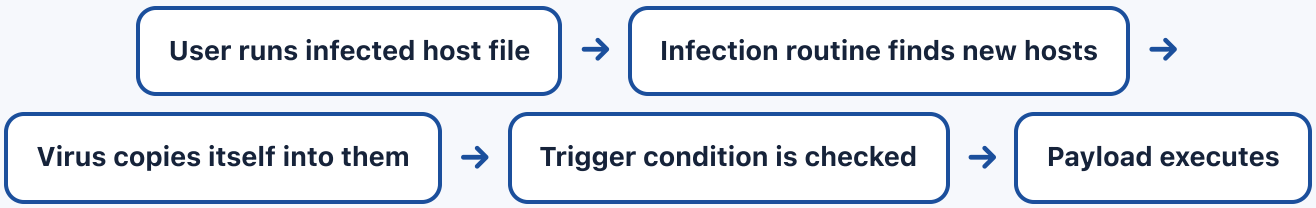
Why It Matters

Even though pure self-replicating viruses are less common today than blended threats, the concept remains central to how professionals think about malware. Understanding infection, triggering, and payload delivery is the foundation for analyzing modern threats, most of which reuse these ideas. A single infected file shared across a network can disrupt operations, corrupt data, and open a path for further compromise. For anyone building a security career, being able to explain how a virus attaches to a host and why user execution matters is a baseline expectation in interviews and on the job.

How It Works

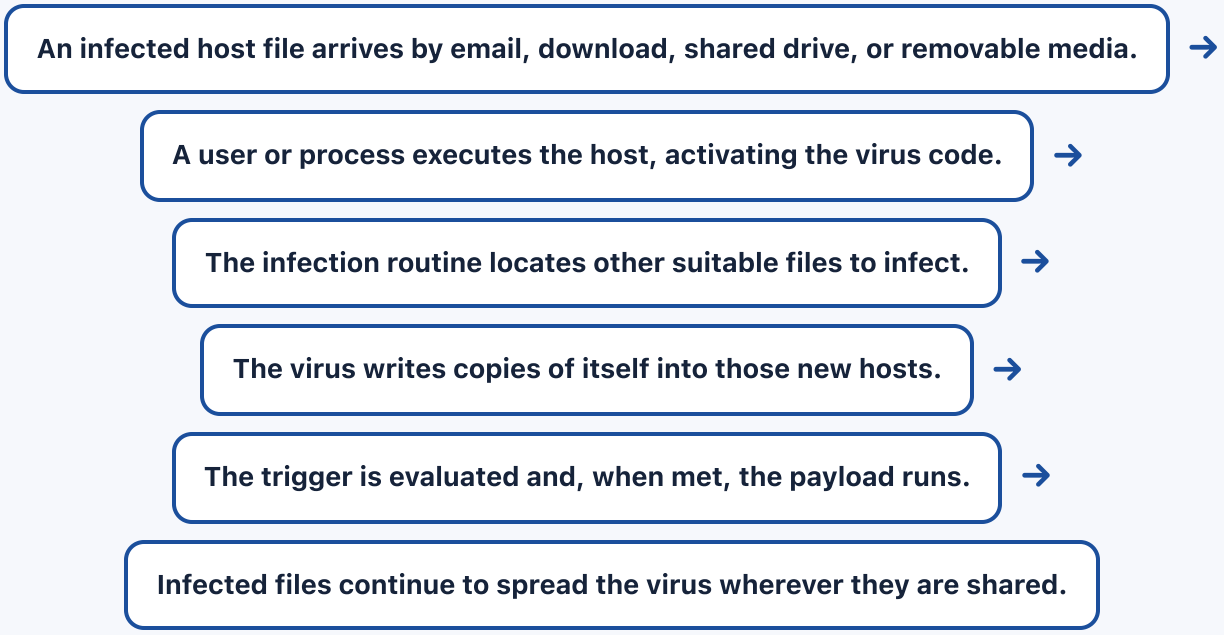
A virus begins when a user runs or opens an infected host, such as launching a program or enabling macros in a document. The infection routine then searches for other suitable hosts and writes copies of the virus into them, so the infection can spread each time one of those files is used. Many viruses try to avoid detection by encrypting or rearranging their own code, a technique broadly described as polymorphism or metamorphism, so that each copy looks different to simple signature scanners. The payload may fire immediately or wait for a trigger such as a specific date, a number of executions, or a particular condition. Because the virus rides inside legitimate files, it can travel through email attachments, shared drives, and removable media wherever those files go.

Architecture Diagram



A virus spreads only after an infected host is executed, then attaches copies to new hosts before or after firing its payload.

Visual Workflow



Common Attacks

- Macro viruses hidden in office documents that run when macros are enabled
- File infectors that attach to executable programs and spread on launch
- Boot sector infection that loads malicious code before the operating system
- Infected files spread through email attachments and shared network drives
- Removable media such as USB drives carrying infected files between systems

Common Mistakes

- Enabling macros on documents from unknown or unexpected senders
- Running executables downloaded from untrusted sources without scanning
- Disabling antivirus or letting its signatures fall out of date
- Assuming a single antivirus product catches every variant
- Ignoring how easily infected files travel on USB drives and shared folders

Best Practices

- Keep endpoint protection installed, running, and automatically updated
- Disable office macros by default and allow them only when verified
- Patch operating systems and applications so known flaws cannot be abused
- Apply least privilege so infected code cannot easily reach system files
- Scan removable media and downloads before opening them
- Keep tested backups so infected or corrupted files can be restored cleanly

Quick Checklist

- [x] Endpoint protection deployed on all devices with current signatures
- [x] Macro execution disabled by policy and controlled through trusted locations
- [x] Operating systems and applications patched on a defined schedule
- [x] Users run without local administrator rights for daily work

- [x] Removable media scanning enforced or removable media restricted
- [x] Tested backups available to restore infected or damaged files

Recommended Tools

Endpoint protection or antivirus
Detects and blocks known and suspicious file-based malware

Endpoint Detection and Response (EDR)
Watches for malicious behavior and enables containment and response

Sandbox or detonation service
Runs a suspicious file safely to observe what it does

File hashing and reputation lookup
Checks whether a file is known good or known malicious

Industry Standards

NIST SP 800-83
Guidance on preventing and handling malware incidents on endpoints

NIST SP 800-61
Computer security incident handling, including malware containment and recovery

CIS Critical Security Controls
Malware defenses and secure configuration as practical safeguards

Career Relevance

Understanding viruses is foundational for SOC analysts, incident responders, and malware analysts who must recognize infection, triggering, and payload behavior. Security engineers apply this knowledge when configuring endpoint defenses and hardening systems, and GRC and audit professionals rely on it to assess whether malware controls are in place. For the AI-Governance-Jobs.com audience, malware literacy is a common expectation across security and technology roles.

Interview Questions

- What is the difference between a virus and a worm?
- What are the three main parts of a virus, and what does each one do?
- Why does a virus typically require user action to spread?
- What is a macro virus, and why are documents a common carrier?
- How does polymorphism help a virus evade signature-based detection?

Related Certifications

CompTIA Security+ | ISC2 Certified in Cybersecurity (CC) | GIAC Reverse Engineering Malware (GREM)

Further Reading

- NIST SP 800-83: Guide to Malware Incident Prevention and Handling
- CISA: Cybersecurity Best Practices
- MITRE ATT&CK

Key Takeaways

- A virus attaches to a host file and needs that host to be executed to spread.
- Viruses have an infection mechanism, a trigger, and a payload.
- They travel inside legitimate files through email, shares, and removable media.
- Layered defenses of endpoint protection, patching, least privilege, and backups work best.
- Malware fundamentals are career-relevant across SOC, incident response, and analysis roles.

FAQ

▶ **Is a virus the same as malware?**

▶ **Why do viruses need a host file?**

▶ **Does antivirus stop every virus?**

Related Careers

RELATED ROLES

Soc Analyst | Incident Responder | Malware Analyst

RELATED CERTIFICATIONS

CompTIA Security+

ISC2 Certified in Cybersecurity (CC)

GIAC Reverse Engineering Malware (GREM)

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides | Role roadmaps | Salary data | Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **Computer Viruses**
3. Go deeper: Trojans
4. Go deeper: Worms
5. Validate it: work toward **CompTIA Security+**
6. Find the role: browse current openings

RELATED SHEETS

CS-012 Trojans | CS-013 Worms | CS-014 Ransomware | CS-001 Cybersecurity | CS-010 Cyber Hygiene