CS-012 · Malware

Trojans

Malware disguised as something useful that runs harmful code once a user installs it.

Executive Summary

A Trojan is malware that disguises itself as legitimate or desirable software to trick a user into installing and running it. Named after the Trojan horse, it relies on deception rather than self-replication. Once executed it can open a backdoor, steal data, download more malware, or give an attacker remote control of the device.

What It Is

A Trojan, sometimes called a Trojan horse, is malicious software that pretends to be something the user wants, such as a free tool, a game, a cracked application, a software update, or an email attachment. The user is deceived into installing it, which is the whole point of the technique. Unlike a virus or a worm, a Trojan does not spread by itself. It depends entirely on social engineering to get onto a system. Trojans are often described by what they do rather than how they spread, which is why professionals talk about categories such as remote access Trojans that give an attacker control, banking Trojans that steal financial credentials, downloaders that pull in additional malware, and droppers that install other payloads.

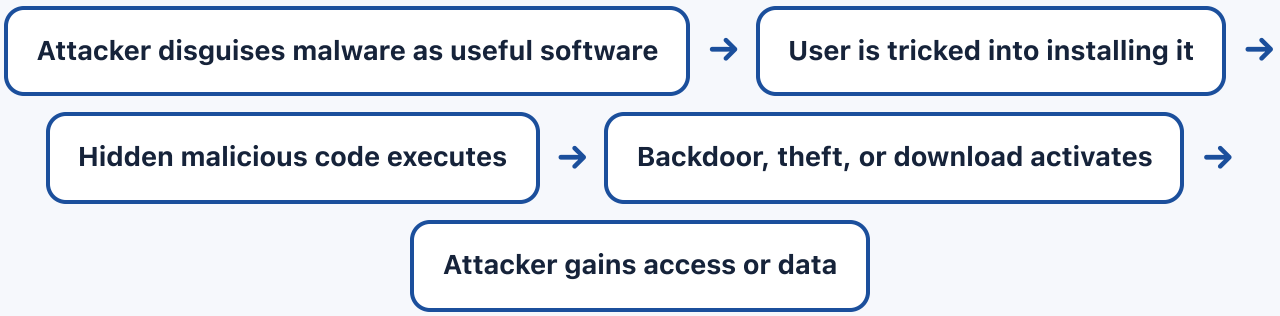
Why It Matters

Trojans are one of the most common ways attackers gain their initial foothold on a system, precisely because they exploit human trust rather than a technical flaw. A convincing disguise can bypass a cautious user and lead to stolen credentials, drained accounts, ransomware deployment, or long-term hidden access. Because the delivery relies on deception, no patch alone fixes the problem, which makes user awareness and layered controls essential. For security professionals, recognizing Trojan tactics is central to understanding how intrusions begin and how to shut them down early.

How It Works

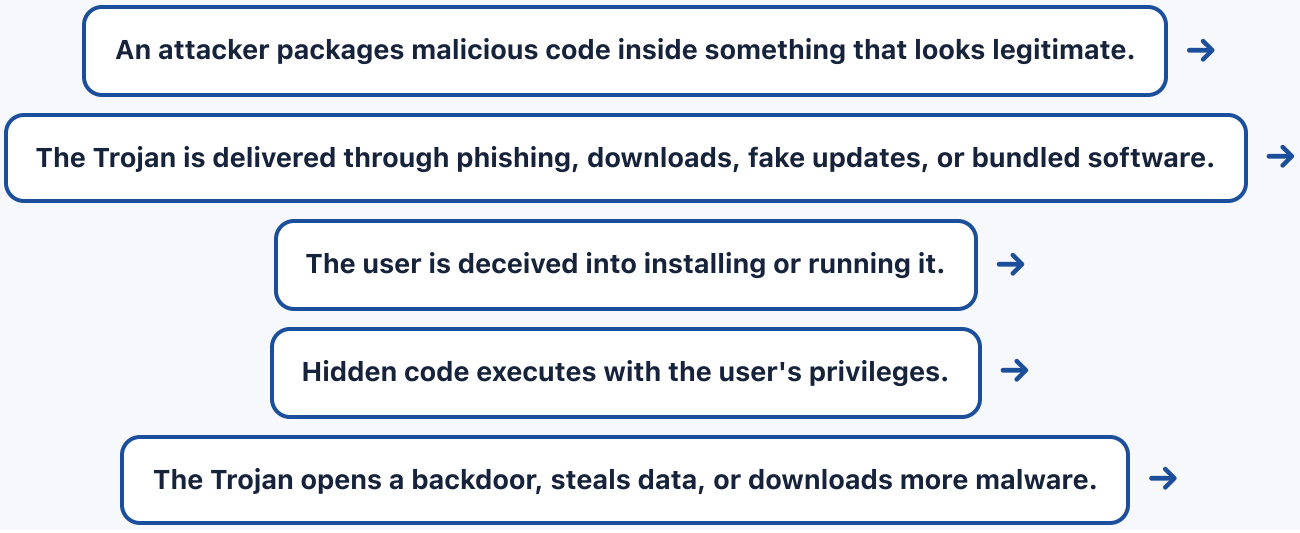
A Trojan reaches a victim through a channel that looks trustworthy, such as a download site, a phishing email attachment, a fake update prompt, or bundled software. The user installs or runs it, believing it is legitimate. At that point the hidden malicious code executes with whatever privileges the user has. Depending on its type, the Trojan may open a backdoor for remote control, log keystrokes, exfiltrate files, or download and install additional malware. Many Trojans work to remain hidden by disguising their processes, establishing persistence so they survive a reboot, and communicating quietly with an attacker-controlled server for instructions. Because a Trojan cannot replicate on its own, attackers often distribute it at scale through spam campaigns, malicious ads, and compromised websites.

Architecture Diagram



A Trojan relies on deception: the user installs seemingly useful software, and hidden code then runs to serve the attacker.

Visual Workflow



It establishes persistence and communicates with the attacker for instructions.

Common Attacks

- Remote access Trojans that give an attacker hidden control of a device
- Banking Trojans that steal login and financial credentials
- Downloaders and droppers that install ransomware or other malware
- Fake software updates and cracked applications carrying hidden payloads
- Malicious email attachments disguised as invoices, resumes, or documents

Common Mistakes

- Installing software from unofficial or untrusted download sources
- Trusting fake update prompts that appear while browsing
- Opening email attachments from unexpected senders without verification
- Running everyday tasks with local administrator rights
- Assuming a program is safe because it appears to work as advertised

Best Practices

- Install software only from official vendors and trusted app stores
- Keep endpoint protection running with current signatures and behavior detection
- Apply least privilege so installed code has limited reach
- Use application allow-listing to block unapproved executables where practical
- Train users to recognize fake updates, lures, and suspicious attachments
- Monitor outbound connections for unexpected communication to unknown servers

Quick Checklist

- [ ] Software sourced only from official or approved locations
- [ ] Endpoint protection with behavior-based detection enabled

- [x] Users work without local administrator rights by default
- [x] Application allow-listing or control enforced where feasible
- [x] Outbound network activity monitored for suspicious connections
- [x] Security awareness training covers fake updates and malicious attachments

Recommended Tools

Endpoint Detection and Response (EDR)
Detects malicious behavior after execution and enables containment

Application allow-listing
Prevents unapproved programs, including Trojans, from running

Sandbox or detonation service
Safely runs a suspicious installer to reveal hidden behavior

Network monitoring
Flags unexpected outbound connections used for command and control

Industry Standards

NIST SP 800-83
Guidance on preventing and handling malware, including deceptive installers

NIST SP 800-61
Incident handling framework for containing and recovering from compromise

MITRE ATT&CK
Catalogs adversary techniques such as command and control and persistence

Career Relevance

Trojans are a core topic for SOC analysts and incident responders who investigate how an intrusion started and what the malware did after execution. Malware analysts reverse engineer Trojans to understand their capabilities, and security engineers design allow-listing and least-privilege controls to block them. GRC professionals use this understanding to evaluate malware

and awareness controls. The AI-Governance-Jobs.com audience benefits from recognizing how deception drives real intrusions.

Interview Questions

- How does a Trojan differ from a virus and a worm?
- What is a remote access Trojan, and why is it dangerous?
- Why is user awareness so important in defending against Trojans?
- How can least privilege and application allow-listing reduce Trojan impact?
- What signs might indicate a Trojan is communicating with an attacker?

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 Trojan disguises itself as useful software to trick users into installing it.
- It does not self-replicate and depends entirely on deception.
- Once run, it can open backdoors, steal data, or install more malware.
- Defenses combine trusted sources, least privilege, allow-listing, and awareness.
- Trojans are a leading cause of initial access in real intrusions.

FAQ

▶ **Why is it called a Trojan?**

▶ **Can a Trojan spread on its own?**

▶ **What is a remote access Trojan?**

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: **Trojans**
3. Go deeper: Computer Viruses
4. Go deeper: Worms
5. Validate it: work toward **CompTIA Security+**
6. Find the role: browse current openings

RELATED SHEETS

CS-011 Computer Viruses | CS-013 Worms | CS-014 Ransomware | CS-001 Cybersecurity | CS-032 Phishing