Trojan horse

In computing, a Trojan horse is a program downloaded and installed on a computer that appears harmless, but is, in fact, malicious. Unexpected changes to computer settings and unusual activity, even when the computer should be idle, are strong indications that a Trojan is residing on a computer.

Typically, the Trojan horse is hidden in an innocent-looking email attachment or free download. When the user clicks on the email attachment or downloads the free program, the malware that is hidden inside is transferred to the user's computing device. Once inside, the malicious code can execute whatever task the attacker designed it to carry out.

Common types of Trojan malware

Backdoor Trojan

This Trojan can create a “backdoor” on your computer. It lets an attacker access your computer and control it. Your data can be downloaded by a third party and stolen. Or more malware can be uploaded to your device.

Distributed Denial of Service (DDoS) attack Trojan

This Trojan performs DDoS attacks. The idea is to take down a network by flooding it with traffic. That traffic comes from your infected computer and others.

Downloader Trojan

This Trojan targets your already-infected computer. It downloads and installs new versions of malicious programs. These can include Trojans and adware.

Fake AV Trojan

This Trojan behaves like antivirus software, but demands money from you to detect and remove threats, whether they’re real or fake.

Game-thief Trojan

The losers here may be online gamers. This Trojan seeks to steal their account information.

Infostealer Trojan

As it sounds, this Trojan is after data on your infected computer.

Mailfinder Trojan

This Trojan seeks to steal the email addresses you've accumulated on your device.

Remote Access Trojan

This Trojan can give an attacker full control over your computer via a remote network connection. Its uses include stealing your information or spying on you.

Rootkit Trojan

A rootkit aims to hide or obscure an object on your infected computer. The idea To extend the time a malicious program runs on your device.

SMS Trojan

This type of Trojan infects your mobile device and can send and intercept text messages. Texts to premium-rate numbers can drive up your phone costs.

Trojan banker

This Trojan takes aim at your financial accounts. It's designed to steal your account information for all the things you do online. That includes banking, credit card, and bill pay data.

Trojan IM

This Trojan targets instant messaging. It steals your logins and passwords on IM platforms.

Worms

A **worm virus** is a malicious, self-replicating program that can spread throughout a network without human assistance.

Worms cause damage similar to viruses, exploiting holes in security software and potentially stealing sensitive information, corrupting files and installing a back door for remote access to the system, among other issues.

Worms often utilize large amounts of memory and bandwidth, so affected servers, networks and individual systems are often overloaded and stop responding.

But worms are not viruses. Viruses need a host computer or operating system. The worm program operates alone.

The worm is often transmitted via file-sharing networks, information-transport features, email attachments or by clicking links to malicious websites. Once downloaded, the worm takes advantage of a weakness in its target system or tricks a user into executing it. Some worms have a phishing component that entices users to run the malicious code.

Internet worms are often designed to exploit new security issues, and search for systems that haven't installed current software or operating system security updates.

Classifications and names of worms include:

- Email-Worm
- IM(Instant Messaging)-Worm
- IRC(Internet Relay Chat)-Worm
- Net-Worm
- P2P(Peer2Peer)-Worm