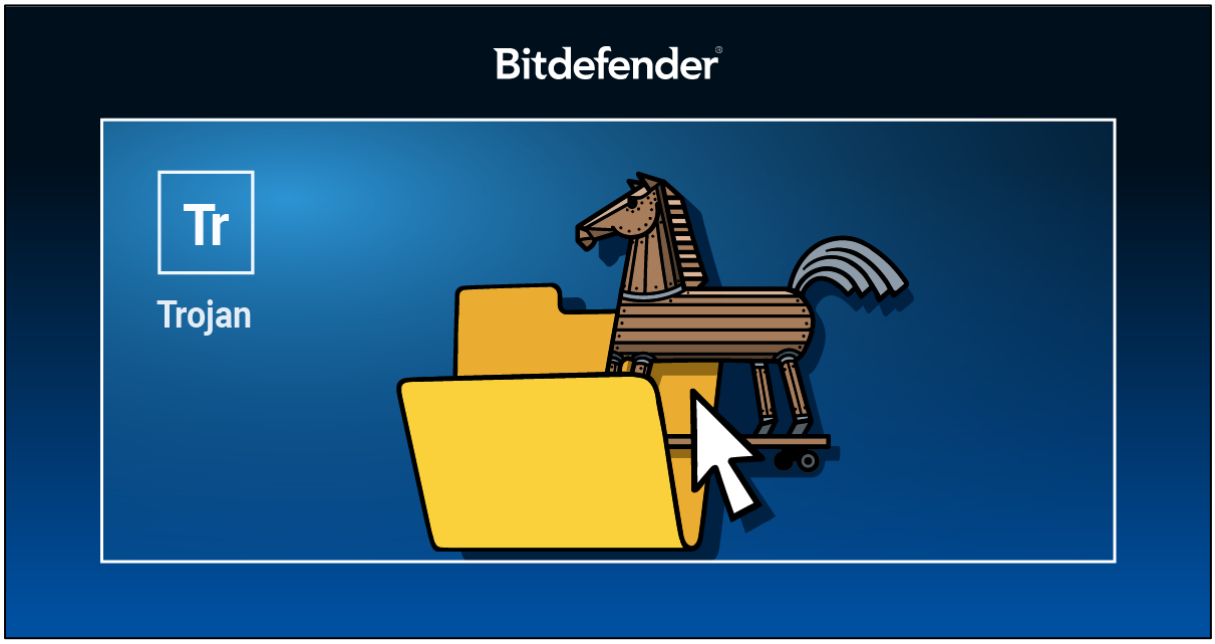
What is a Trojan? Prevention & Removal

The Trojan horse was a sly trick the ancient Greeks used to infiltrate their troops in Troy to ultimately conquer the city. Following the same analogy, a Trojan is a malicious program a hacker will use to break into a computer. Just as the original Trojan horse deceived the people of Troy, so does the computer Trojan deceive the user by posing as legitimate software.

What is a Trojan?

A Trojan is a specific breed of malware that impersonates an application, utility, or software product to deceive the user into running it. For instance, a Trojan operator would attempt to trick the user trying to watch video content (usually downloaded via P2P networks) to install a “special codec”, that ultimately proves to be a backdoor or a piece of ransomware.



Trojans account for the bulk of currently existing malware, and, unlike viruses or worms, they can neither infect files nor propagate across a network without user intervention. These malicious applications are highly specialized: they can provide remote access to a computer or smartphone, can be used to launch denial-of-service attacks, download other Trojans for other cyber-criminals or send spam e-mails from the infected devices.

Remote Access Trojans (RATs) are usually popular on Android, as they enable attackers to leverage seemingly legitimate applications to exploit vulnerabilities within the mobile operating system and take control of it.

As of late 2014, a new family of Trojans made headlines in the media: ransomware. Ransomware is a species of malware specialized in encrypting user data and asking for ransom in exchange for the decryption key.

How does a Trojan get into my device?

Trojans are the most common type of malware on both Mac and Windows. The delivery method for Trojans on any given platform typically involves social engineering techniques like spam and phishing, infected websites, or scams leveraging the victim's favourite social networks.

Trojans are used extensively against high-profile **Windows** targets and remain on the map of the top threats to Windows computers globally. In 2021, despite international efforts to dismantle big-name Trojans like Trickbot, Emotet, Dridex and AgentTesla, cybercriminals continued to leverage this infamous malware family.

On **Macs**, a fair number of Trojan infections also occur through warez sites – hotbeds for pirated downloads. Whatever the vector, Trojans are the biggest single threat to Macs, and most of those attempted attacks were picked up in the US, which registered 36% of Trojan activity targeting macOS globally in 2021 – unsurprisingly so, considering the US has the biggest macOS install base in the world.

Android is no stranger to Trojans. If threats were traditionally targeting Windows and macOS, with more than 3 billion active Android devices in the world in 2022, it makes sense for cybercriminals to develop threats for Android smartphones. While SMS-sending Trojans are usually quite popular, especially since they present an easy way of making money, rooting Trojans are among the most devious threats. Rooting Trojans are designed to take full remote control over a device, enabling the attacker to access any type of stored information, as if holding the device.

While some users might want to root their devices to either delete pre-installed applications that normally cannot be removed or even change the Android version the device is running, rooting Trojans are usually installed without a user's" knowledge. For example, there have even been rooting Trojans that managed to slip into Google Play. The application was submitted as a perfectly legitimate colour block game, following which attackers would update it with malicious code. After the malicious update reached the device and gained system privileges, it had the ability to covertly install applications from third-party marketplaces potentially malicious without the user's knowledge. After successfully doing that, the application was once again updated with a benign version so as not to stir suspicion.

How to identify and wipe out a Trojan

Because the concept behind a Trojan is to trick users in an undetectable manner, they're not always easy to catch, and Trojan infections are on the rise. It's better to be sceptical and double-check that you know what you are downloading or clicking on, so you don't risk downloading a counterfeit program. Stay informed and pay close attention to the language used in emails or on the websites you visit, especially if they ask you to download software.

How to stay safe

If you still have doubts about detecting Trojans by yourself, the best protection to keep your system clean is to install a software security solution that protects all your devices. However, do your part as well and refrain from visiting suspicious sites, following unknown links, or downloading bootleg games, music, or movies from questionable sources.

By installing applications from trusted marketplaces, you reduce the chances of accidentally installing rooting Trojans or any type of threat. But even Google Play is not immune to Trojans, as some have managed to infiltrate.

Regularly updating the operating system with its latest security patches is highly recommended, as attackers cannot use known vulnerabilities to their own advantage. Since smartphones hold just as much personal data, if not more, than traditional PCs, everyone is encouraged to always have a mobile security solution installed, as they're usually highly capable of identifying malicious apps from official marketplaces and third-party ones.

A security solution can timely identify any malicious application that's packing routing capabilities as it's not exactly legitimate behavior, keeping users safe from attackers trying to remotely control their device. Whether the app is downloaded via third-party marketplaces or simply delivered via a malicious URL, a security solution will be capable of blocking both the malware-serving URL and the actual application before installing, securing your device and data from a wide range of attack vectors.