

Security Utility Abuses Supply Chain for a Malware Attack

 securityintelligence.com/news/security-utility-abuses-supply-chain-for-a-malware-attack/



Security Intelligence

Over 2 million users have installed infected versions of a security application owned by software firm Avast.

According to [Cisco Talos](#), CCleaner version 5.33, which was available as a legitimate download from Aug. 15 to Sept. 12, was found to contain a multistage malware attack hidden inside of it. CCleaner Cloud v1.07.3191 was also infected by the malware.

Characteristics of the Malware Attack

FloXif is a downloader that gathers information about infected systems and then sends it back to the command-and-control (C&C) server associated with it, reported [Bleeping Computer](#). The malware gleans the computer name, a list of software installed, a list of running processes, MAC addresses for the first three network interfaces and unique IDs that identify each computer. It only runs on 32-bit systems, which have to be administrator accounts.

If the primary C&C server does not return a response to the HTTP POST request made by the malware, it uses a domain generation algorithm (DGA) to generate a new location. The DGA is time-based and can be calculated using the values of year and month. Cisco evaluated the DGA and sinkholed the domains it produced to prevent them from being used in an attack.

FloXif can run other binaries, but there is not yet any evidence that another payload was downloaded and run on the infected systems.

Supply Chain Problem

Cisco Talos believed that the threat actors compromised Avast's supply chain. Avast bought Piriform, the utility's actual developer, in July, which was one month before the poisoned version made its appearance. [Piriform](#) confirmed the problem in a blog post.

Since the malware binary was digitally signed using a valid certificate issued to the software developer, the attacker was able to breach somewhere in the development process and switch out the production version for the malware version. It's possible that the change in company ownership facilitated this supply chain attack.

"2.27 million is certainly a large number, so we're not downplaying in any way," Avast chief technology officer (CTO) Ondrej Vlcek told [Forbes](#). "It's a serious incident. But based on all the knowledge, we don't think there's any reason for users to panic."

While the cloud-based version of CCleaner will accept an update pushed out by Avast, the app version will not. Anyone who downloaded the [antivirus software](#) during the infection period must update the app manually to undo this infection.

[Antivirus](#) | [Cyberattack](#) | [Malware](#) | [Supply Chain](#) | [Supply Chain Security](#)

[Larry Loeb](#)

Principal, PBC Enterprises

POPULAR

[Data Protection](#) January 3, 2025

Router reality check: 86% of default passwords have never been changed

[4 min read - Misconfigurations remain a popular compromise point — and routers are leading the way. According to recent survey data, 86% of respondents have never changed their router admin password, and 52% have never adjusted any factory settings. This puts attackers in the...](#)

[Risk Management](#) November 6, 2024

What Telegram's recent policy shift means for cyber crime

4 min read - [Since its launch in August 2013, Telegram has become the go-to messaging app for privacy-focused users. To start using the app, users can sign up using either their real phone number or an anonymous number purchased from the Fragment blockchain...](#)

[Risk Management](#) December 31, 2024

The 5 most impactful cybersecurity guidelines (and 3 that fell flat)

4 min read - [The best cybersecurity guidelines have made a huge difference in protecting data from theft and compromise, both in the United States and around the world. These guidelines are comprehensive sets of recommended practices, procedures and principles designed to help organizations...](#)

Topic updates

Get email updates and stay ahead of the latest threats to the security landscape, thought leadership and research.

Subscribe today