Piriform admits legitimate downloads of its CCleaner software carry a "multi-stage malware payload"-- essentially a backdoor allowing hackers to install ransomware or keyloggers to further infect PCs.

According to the company around 2.27 million users ran the affected software (specifically CCleaner version 5.33.6162 and CCleaner Cloud version 1.07.3191) following download from a hacked server. The company says the situation could have been a lot worse, since CCleaner gets around 5 million new users per month, for a total of over 2 billion downloads.

It also says the affected version is already updated, and it was "able to disarm the threat before it was able to do any harm" following initial warnings from security researchers at Cisco and Morphisec. According to the Cisco Talos research unit the affected CCleaner infects computers through the inclusion of remote administration tools that, once installed, connect to several unregistered websites in order to download more unauthorised programs.

CCleaner is a "crap cleaner" able to remove rogue programs and tracking cookies from Windows PCs. It is developed by Piriform, a British company owned by security vendor Avast. The name is something of an established brand, making it a target to attackers wanting to take advantage of the trust relationship between users and vendors. Previously attackers would create fake alternatives to popular applications, but now they have taken to directly attacking the source.

"This is a prime example of the extent that attackers are willing to go through in their attempt to distribute malware to organizations and individuals around the world," Cisco Talos adds. "Attackers have shown that they are willing to leverage this trust to distribute malware while remaining undetected."

Customers with potentially infected versions of CCleaner should restore their PCs to a state before 15 August 2017, as well as update to the latest version of CCleaner. Such updates need to be done manually, since the free version does not do so automatically.

Go Security Notification for CCleaner v5.33.6162 and CCleaner Cloud v1.07.3191 for 32-bit Windows users

Go CCleanup: A Vast Number of Machines at Risk