CCleaner has been hacked, attached malware, things to know and how to fix it

An unknown hacker group attacked CCleaner's infrastructure and added malware to the 32bit versions of CCleaner 5.33.6162 and CCleaner Cloud 1.07.3191.

An unknown hacker group attacked CCleaner's infrastructure and added malware to the 32bit versions of CCleaner 5.33.6162 and CCleaner Cloud 1.07.3191. These files are available for download from August 15 to September 12. Users who have installed CCleaner during this time are likely to have become victims of the attack.

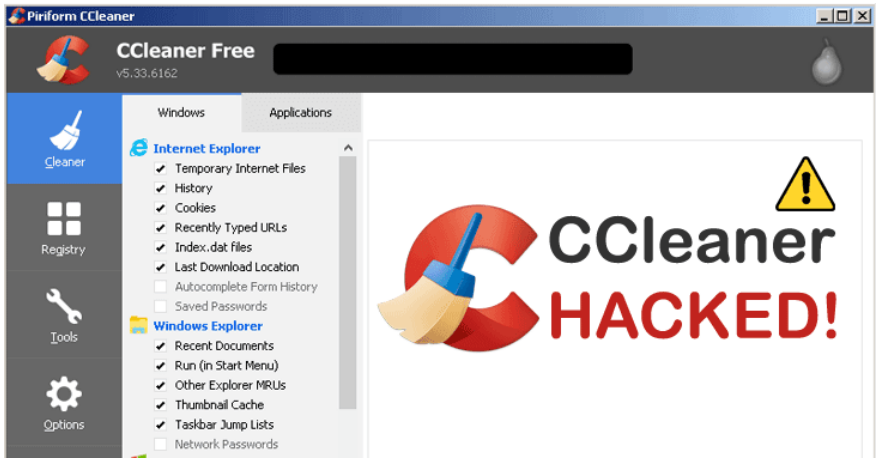
Who is affected?

Those who have downloaded and installed CCleaner 5.33.6162 and CCleaner Cloud 1.07.3191 during the above period. Avast estimates the number of affected machines up to 2.27 million.

What does CCleaner malware do?

This malware is called Floxif, collecting data from infected computers, such as computer name, list of installed software on the computer, list of running processes on the computer, MAC address for 3 networks. The first interface and unique IDs to identify each computer.

The malware also downloads and executes another malware, but Avast said it found no evidence that hackers used it.



How to delete malware on CCleaner?

Malware is embedded directly into CCleaner's executable file. Updating CCleaner to version 5.34 will remove old executables and malware. CCleaner does not have an automatic update system, so users must download and install CCleaner 5.34 manually.

Avast said it has released an update for CCleaner Cloud users, and there is no problem with malware being detected. The clean version is CCleaner Cloud 1.07.3214.

Anything else?

Malware is only executed if the user is using the Administrator account. If you are using a low-powered account and installing CCleaner 5.33, you are not affected much. However, updating to version 5.34 is necessary,

Why does antivirus software not detect this malware?

CCleaner binaries include malware signed by a valid digital certificate issued by Symantec to Piriform, so antivirus software does not notice the difference and therefore does not detect malware. Furthermore, the hacker used the Domain Generation Algorithm (DGA) so that if their server crashed, the DGA could create new domain names and send stolen information.

Users also do not notice anything unusual because every installation operation is done automatically like normal. In summary, download CCleaner 5.34 here and reinstall immediately if you are using the affected CCleaner 5.33 version.

1. 9 most effective antivirus software for Windows today

Avast got the malware when it just bought CCleaner not long ago, a security company, released software bundled with malware, didn't know which haker group "scratched" so .

Latest update: Avast blocked the server connected to malware.