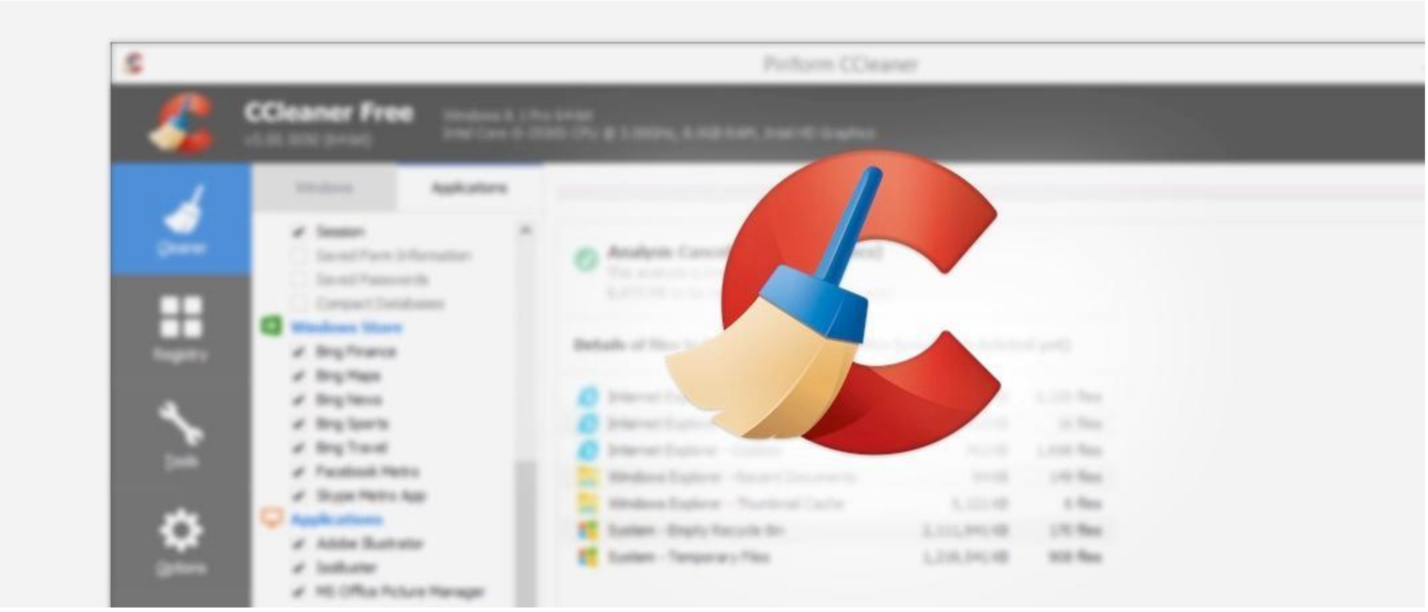
CCleaner Malware Incident - What You Need to Know and How to Remove



This is a small guide and FAQ on the malware installed by the 32-bit version of CCleaner 5.33.6162. For a full recap of what happened, you can read our complete CCleaner coverage.

What happened?

An unknown threat group compromised the CCleaner infrastructure.

The attacker added malware to the 32-bit versions of CCleaner 5.33.6162 and CCleaner Cloud 1.07.3191.

The files were available for download between August 15 and September 12.

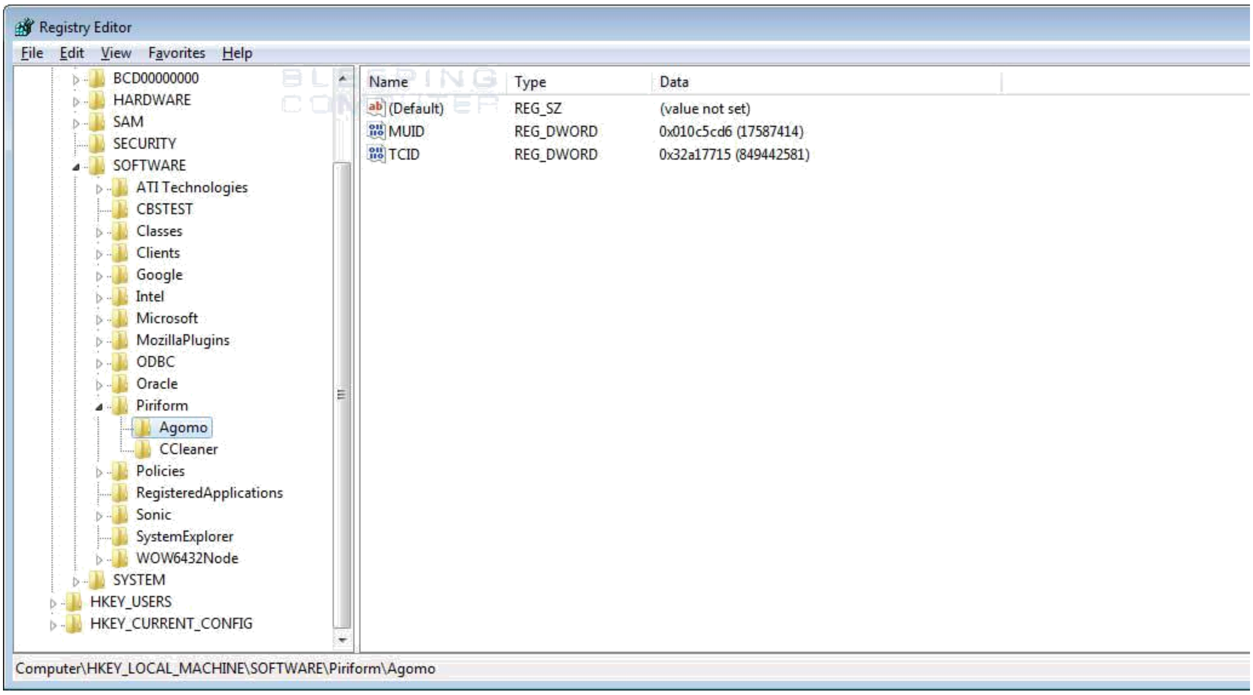
Who is affected?

Everybody who downloaded and installed the affected versions in that timespan.

Avast estimates the number of affected machines at 2.27 million.

How can I tell if I was infected?

When an infected version of CCleaner was installed it would have created a Windows Registry key located at HKEY_LOCAL_MACHINE\SOFTWARE\Piriform\Agomo. Under this key will be two data values named MUID and TCID, which are used by the installed Floxif infection.



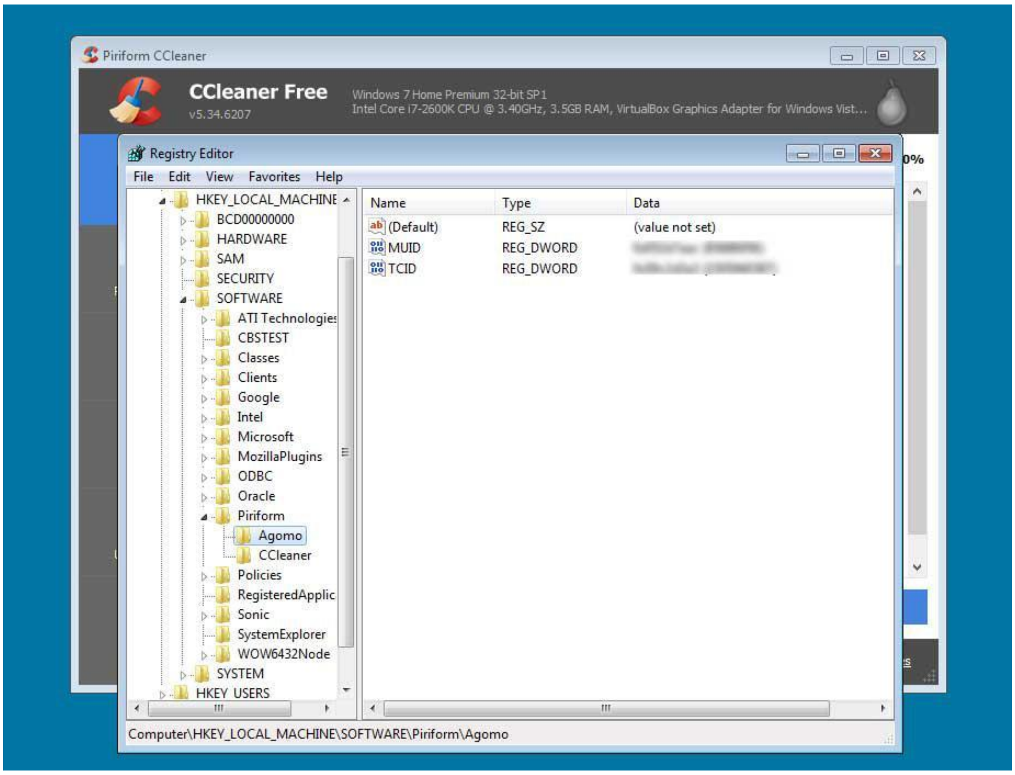
Name	Type	Data
(Default)	REG_SZ	(value not set)
MUID	REG_DWORD	0x010c5cd6 (17587414)
TCID	REG_DWORD	0x32a17715 (849442581)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Piriform\Agomo

Registry key created by Compromised CCLeaner

You can use Registry Editor to navigate to the Agomo key and see if it exists. If it does, then you are infected with this malware.

Please note. as seen below, upgrading to version 5.34 will not remove the Agomo key from the Windows registry. It will only replace the malicious executables with legitimate ones so that the malware is no longer present.



Name	Type	Data
(Default)	REG_SZ	(value not set)
MUID	REG_DWORD	[redacted]
TCID	REG_DWORD	[redacted]

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Piriform\Agomo

Registry Key Present After Ugprade

What does the Floxif malware do?

The malware — named Floxif — collects data from infected computers, such as computer name, a list of installed software, a list of running processes, MAC addresses for the first three network interfaces, and unique IDs to identify each computer in part.

The malware could also download and execute other malware, but Avast said it did not find evidence that attackers ever used this function.

How do I remove the Floxif or CCleaner Malware?

The malware was embedded in the CCleaner executable itself. Updating CCleaner to v5.34 removes the old executable and the malware.
CCleaner does not have an auto-update system, so users must download and install CCleaner 5.34 manually.

Avast said it already pushed an update to CCleaner Cloud users, and they should be fine. The clean version is CCleaner Cloud 1.07.3214.

Should I do anything else after the malware has been removed?

As the installed Floxif infection was sending information about your computer and had the ability to download and install other programs, victims should change their passwords and perform security scans on the computer.

It is suggested that victims stop using the infected computer and then change their passwords from a computer or cell phone that did not have this version of CCleaner installed on it. This is because it is not known if other malware was installed by the Floxif infection and is currently running that may steal passwords and other information.

Once you have changed your passwords, you should perform scans using a antivirus application, if not multiple applications, to make sure that there are no other infections present on the computer. After this has been finished, and anything that may have been detected has been removed, you can begin using your computer again.

For those who want to be truly safe, the best course of action is to always reinstall Windows to be 100% safe. It goes without saying that this is not always feasible, so at a minimum, the suggested actions should be completed before you use the computer again.

Anything else?

The malware executed only if the user was using an admin account. If you use a low-privileged account and installed CCleaner 5.33, you more not affected. If you are running Windows 7 Home Premium, then your main account is most likely an administrative account and you should assume you are infected if you had installed this version of CCleaner.

Nonetheless, it is recommended that you update to version 5.34.

Why didn't antivirus software catch the infection?

The CCleaner binary that included the malware was signed using a valid digital certificate.