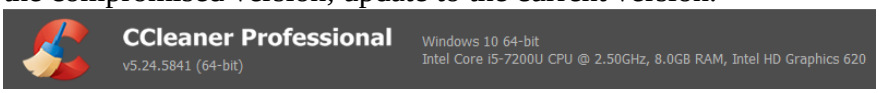
APCUG Sept. 18-17 - CCleaner app "Version 5.33 compromised with malware.

From: Judy Taylour [mailto:jtaylour@apcug.org]
Sent: September 18, 2017 12:42 PM
To: Judy Taylour <jtaylour@apcug.org>
Subject: APCUG - CCleaner Important Information - Please read

Thanks to APCUG Director Jim Evans for alerting us that CCleaner has been compromised with malware. He posted information to APCUG's Facebook page early this morning and I uploaded the info to the website (Tech Tips and Apple Tips). Judy

CCleaner version 5.33 was compromised with malware. Please check to see which version of CCleaner you have on your computer.

Open CCleaner and you will find the version number in the upper left corner on the title bar. If you have the compromised version, update to the current version.



From Bleeping Computer: "Version 5.33 of the CCleaner app offered for download between August 15 and September 12 was modified to include the Floxif malware, according to a report published by Cisco Talos a few minutes ago. Updating to recent versions removes malware.

Floxif is a malware downloader that gathers information about infected systems and sends it back to its C&C server. The malware also had the ability to download and run other binaries, but at the time of writing (9/18), there is no evidence that Floxif downloaded additional second-stage payloads on infected hosts.

The malware collected information 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. Researchers noted that the malware only ran on 32-bit systems. The malware also quit execution if the user was not using an administrator account."

Avast recently bought Piriform – below from Avast CTO:

"In an email to Bleeping Computer, Avast CTO Ondrej Vlcek said that updating CCleaner to the most recent recent versions fixes any issues, as "the only malware to remove is the one embedded in the CCleaner binary itself.

The affected software (CCleaner v5.33.6162 and CCleaner Cloud v1.07.3191) has been installed on 2.27M machines from its inception up until now," Vlcek also added. "We believe that these users are safe now as our investigation indicates we were able to disarm the threat before it was able to do any harm."

"There is no indication or evidence that any additional "malware" has been delivered through the backdoor," Vlcek added.

Read the complete article at: http://bit.ly/2f5XmGX