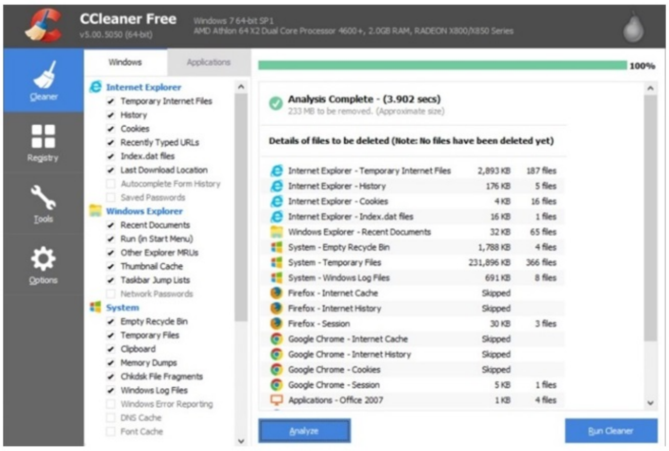
CCleaner

Threat: **Supply-Chain Attack**

Author: **Jeffrey Farnan** Date Originally Published: **May 31th, 2021**

1. SUMMARY

- CCleaner is a popular file clean-up and performance optimization utility for the windows operating system. It removes unused files, allowing windows to run faster and free up valuable hard disk space. It cleans traces of your online history and also features a registry cleaner, cleans temporary files to optimize and speed up your computer. It is available in 32bit and 64bit with the option of a free or a professional version.



Internet Explorer
- ☑ Temporary Internet Files
- ☑ History
- ☑ Cookies
- ☑ Recently Typed URLs
- ☑ Index.dat files
- ☑ Last Download Location
- ☐ Autocomplete Form History
- ☐ Saved Passwords

Windows Explorer
- ☑ Recent Documents
- ☑ Run (in Start Menu)
- ☑ Other Explorer MRUs
- ☑ Thumbnail Cache
- ☑ Taskbar Jump Lists
- ☐ Network Passwords

System
- ☑ Empty Recycle Bin
- ☑ Temporary Files
- ☑ Clipboard
- ☑ Memory Dumps
- ☑ Chkdsk File Fragments
- ☑ Windows Log Files
- ☐ Windows Error Reporting
- ☐ DNS Cache
- ☐ Font Cache

Analysis Complete - (3.902 secs)
233 MB to be removed. (Approximate size)

Details of files to be deleted (Note: No files have been deleted yet)

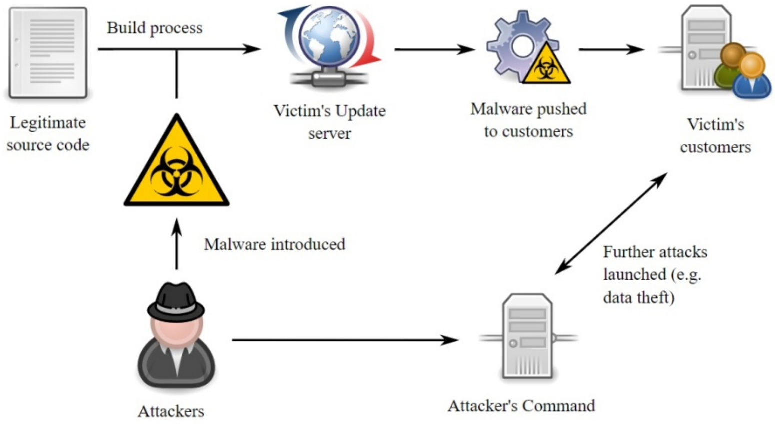
Internet Explorer - Temporary Internet Files	2,893 KB	187 files
Internet Explorer - History	176 KB	5 files
Internet Explorer - Cookies	4 KB	16 files
Internet Explorer - Index.dat files	16 KB	1 files
Windows Explorer - Recent Documents	32 KB	65 files
System - Empty Recycle Bin	1,788 KB	4 files
System - Temporary Files	231,896 KB	366 files
System - Windows Log Files	691 KB	8 files
Firefox - Internet Cache	Skipped	
Firefox - Internet History	Skipped	
Firefox - Session	30 KB	3 files
Google Chrome - Internet Cache	Skipped	
Google Chrome - Internet History	Skipped	
Google Chrome - Cookies	Skipped	
Google Chrome - Session	5 KB	1 files
Applications - Office 2007	1 KB	4 files

- Avast who owns CCleaner discovered its download servers had been hacked into and malicious code had been injected to two versions of its CCleaner application installers. This allowed the legitimate signed version of CCleaner 5.33 and cloud version 1.07 installers to contain a multi-stage malware payload that rode on top of the installation of CCleaner. These versions of CCleaner were available to the general public between August 15 and September 12, 2017. Avast believes it was able to prevent the breach harming customers, and users are now safe as its investigation indicates it was able to disarm the threat before it was able to do any harm.

2. MALWARE FAMILY

- **Type** = Supply Chain Attack.
- **Sub-type** = Spyware.

- The attack on CCleaner is known as a supply-chain malware attack, it's a cyber-attack that seeks to damage an organization by targeting less-secure elements in the supply chain of the company.



- This type of attack is a well thought out attack, the hackers would have been monitoring the organization for a period of time, looking for weak points, and leveraging its systems to gain maximum advantage. Spyware was downloaded as well as the legitimate CCleaner application, sending back user information to the cybercriminals C&C servers. The hackers were looking for high profile targets, large tech organizations, such as Google or Microsoft, which they could steal source code, software applications, or any data they may deem useful.

3. MALWARE CHARATERISTICS

- **Suspected country of origin** = China.
- **First seen date/period** = 13 / 6 / 2017.
- **Still active** = No. This supply chain attack was detected and stopped. The malicious binaries linked with this attack are still active in other campaigns.

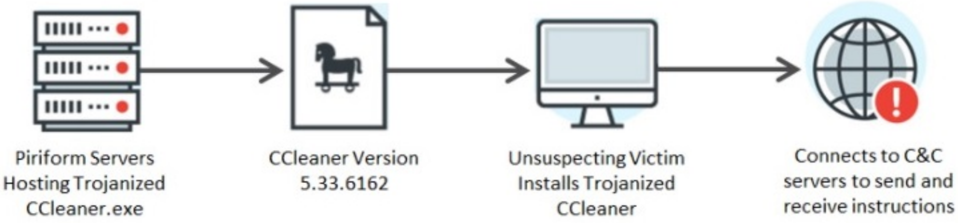
4. APPLACATION HISTORY

- CCleaner, originally named Crap Cleaner when the small company Piriform released it in 2004. The app started life as a registry cleaner, which removed old Windows Registry entries after users have uninstalled old apps, which would improve Windows OS speed. Over the years the app evolved and now supports a trove of other features. It can remove temporary or old files left by removed apps, perform automatic updates for other apps and block ad trackers, etc. CCleaner is now owned by Czech cybersecurity firm Avast, who acquired Piriform in 2017 and had to deal with the PR fallout throughout 2017 and 2018.

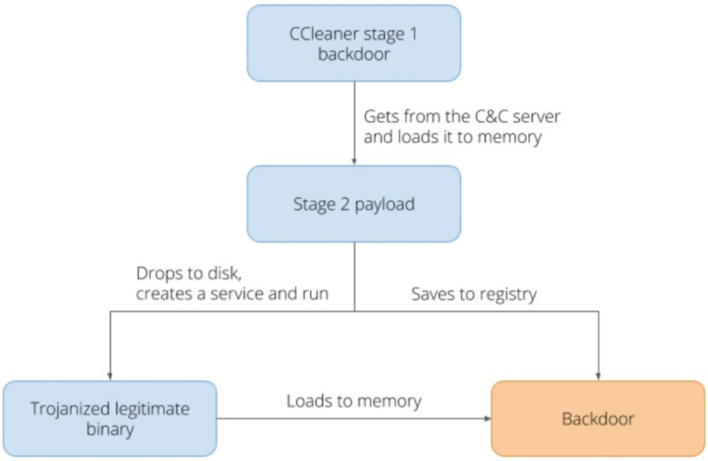
5. MALWARE DESCRIPTION

CCleaner is a legitimate system clean-up software solution which fell victim to hackers who inserted rouge code into the program’s free version, sometime between March 11th and July 4th 2017. It is believed a group of Chinese state-sponsored hackers breached Piriform's network via a TeamViewer account, searched for CCleaner distribution servers, and then released a CCleaner update tainted with malware. Avast says about 2.27 million people ran the infected software. This happened prior to Avast's acquisition of Piriform on July 18, 2017.

- **Arrival and Installation:** The distribution of the compromised CCleaner came from the actual website of Piriform. Hackers were able to compromise the CClenaner installer binaries hosted in the website which resulted to the distribution of the malicious software to the unsuspecting users. Since it came from a legitimate source and digitally signed, it would be almost impossible for users to identify that software has been modified to perform malicious activity.


Piriform Servers Hosting Trojanized CCleaner.exe
CCleaner Version 5.33.6162
Unsuspecting Victim Installs Trojanized CCleaner
Connects to C&C servers to send and receive instructions

- **Two stage Malware**: The malware came in two stages, the first stage was designed to collect non-sensitive information from CCleaners users and was also used as a downloader for the second stage. The second stage was used to download a binary, only if the hackers deemed the user a high value target.


CCleaner stage 1 backdoor
Gets from the C&C server and loads it to memory
Stage 2 payload
Drops to disk, creates a service and run
Saves to registry
Trojanized legitimate binary
Loads to memory
Backdoor

  - **Stage 1:** The malware creates a backdoor and uses a hardcoded C2 server to send information about the affected system and fetch the second payload. The first payload when executed installed a piece of spyware called Foxif. This program builds a complete picture of the infected device and a complete picture of the local network. The malware gathers information of the running processes, installed software, mac addresses and network interfaces. This information is useful for targeting vulnerable system, running outdated versions of programs containing known vulnerabilities. The payload included download capabilities for the second stage.
  - **Stage 2:** The second payload was a malicious binary called Trojan.Nyetya, when dropped is automatically loaded, created a service and ran on the system. This payload includes patched legitimate software products, used to unzipping files and uninstall antivirus software. Creates a backdoor to get commands from its C&C servers, it uses a completely different control network than the first stage. Some of the user information passed to the cybercriminals is:
    - The users keystrokes.
    - Saved passwords used in browsers.
    - Financial information.
    - Any frequently used MS Word documents.

The complex code is heavily obfuscated and uses anti-debugging tricks to conceal its inner workings. Only 40 PC's were ever affected by this second payload, a possible reason was Hackers were looking for computers installed on the networks of one the several major tech companies, such as Google or Microsoft.

- **The Third stage:** After further investigations of the 2017 attack, Avast found a possible third stage of the attack in 2018. This stage would install ShadowPad malware on compromised computers. ShadowPad is a cyberattack platform that cybercriminals deploy in victims networks to gain remote access capabilities. There is no evidence that this stage actually affected any computers. The possible reason this stage never took place, could be because of the fast detection and speedy clean-up of the attack by Avast.
- In 2019 several attempts by Hackers to gain access to CCleaner servers once again, this time compromising its main internal network in the process and yet again, seeking to tamper with CCleaner releases.
- A product by a security vender is the last place people will expect to find comprised software, we expect such companies to maintain and have security check on their own products. Accidents like this demonstrate that no one, not even a security vendor can escape such attacks.

6. POTENTIAL CUSTOMER DEFENSE

- When the breach was discovered Avast took steps to correct the situation, removing the malicious installers and moving to new clean upgraded versions. Users using 5.33 version had to uninstall and reinstall the new version and cloud version 1.07 installers were updated automatically. Avast said on their blog "To the best of our knowledge, we were able to disarm the threat before it was able to do any harm". Here are some defenses you can take:

    - The Malware was embedded in the CCleaner executable itself. A simple uninstall or upgrading to the new version 5.34 would remove the old CCeaner executable plus the malware.
    - As Floxif infection was used to gather information and send it the hackers, it would be advised to change all browser passwords. Floxif also had the ability to download and install other programs, so running security scans would be beneficial.
    - For those who want to be truly safe a complete Windows reinstall would be the best course of action.

- Many antivirus products, such as Windows Defender are now marking CCleaner as PUA – Potentially Unwanted Application, and may automatically remove the app from your system.
- Older versions of CCleaner are still considered safe, and are still available online. CCleaner is not the only option for cleaning your computer, there are recommended alternative options:

    - Download Cleaning Applications with a good track record.
    - Create simple Batch scripts.
    - You can use the manual method, as the admin of your system you can, remove apps, remove registry keys, etc.

Research Sources:

- https://www.bleepingcomputer.com/how-to/security/ccleaner-malware-incident-what-you-need-to-know-and-how-to-remove/
- https://www.kaspersky.com/resource-center/threats/ccleaner-malware
- https://www.safetydetectives.com/blog/remove-ccleaner-malware/
- https://threatpost.com/avast-network-breached-as-hackers-target-ccleaner-again/149358/

Disclaimer: All opinions expressed in this article are the opinions solely of the author.