New investigations into the CCleaner incident point to a possible third stage that had keylogger capacities

By Threat Intelligence Team 8 Mar 2018

Activity was found in Piriform network although not on any of the CCleaner customers' PCs

Following the CCleaner incident last year, we have continued to investigate what happened and have shared our latest insights at the Security Security Analyst Summit today.

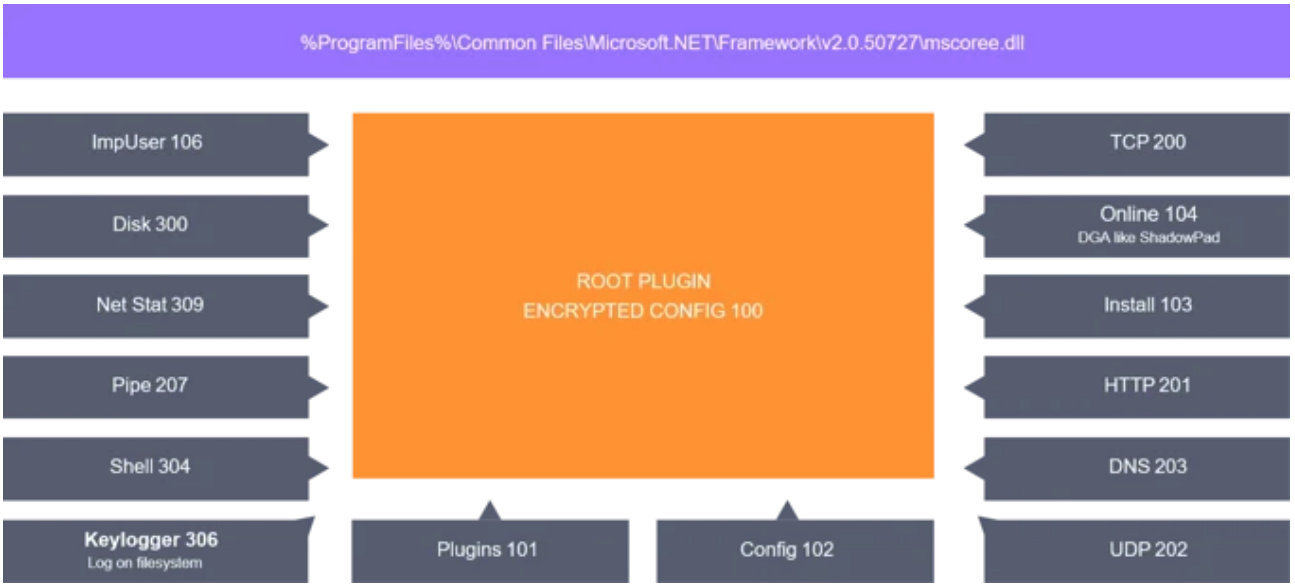
To recap, on September 18, 2017, we disclosed that CCleaner had been targeted by cybercriminals, in order to distribute malware via the CCleaner installation file. The altered installation file was downloaded by 2.27 million CCleaner customers worldwide. The malware was introduced to the build server of Piriform, the company developing CCleaner, some time between March 11 and July 4, 2017, prior to Avast's acquisition of Piriform on July 18, 2017.

The first stage of the malware was designed to collect non-sensitive information from CCleaner users, including, for example, name of the computer, list of installed software, and a list of running processes. The first stage included downloader capabilities, which were used to download a second stage binary onto just 40 PCs out of the millions of devices infected with stage one, making it a highly targeted attack. Up until now, we don't have any evidence that a third stage binary has been downloaded onto the affected computers. However, we have found evidence of activity that could indicate what the intended third stage of the attack could have looked like.

To eliminate the threat from the Piriform network, we migrated the Piriform build environment to the Avast infrastructure, replaced all hardware and moved the entire Piriform staff onto the Avast-internal IT system. We consolidated and inspected the Piriform infrastructure and computers, and found preliminary versions of the stage one and stage two binaries on these, and we found evidence of a specialized tool, ShadowPad, which is used by a specific group of cybercriminals, installed on four Piriform computers.

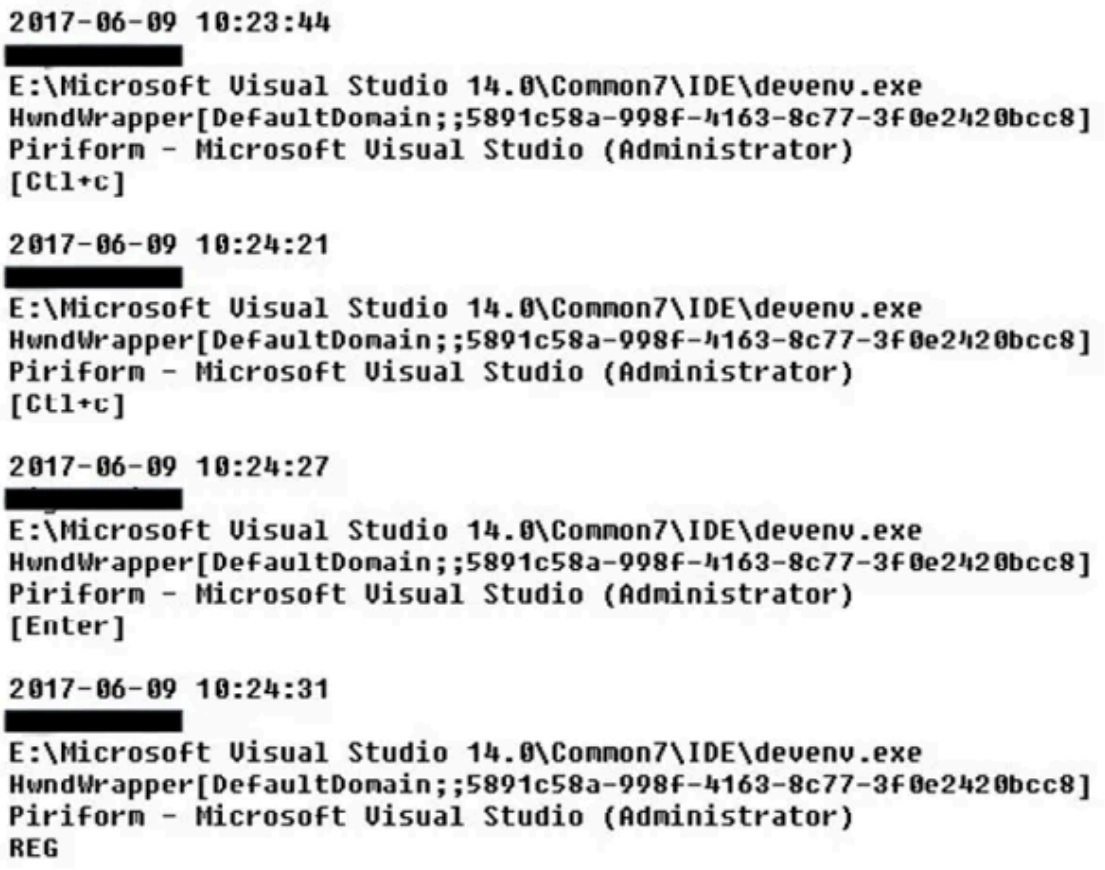
ShadowPad is a cyber attack platform that cybercriminals deploy in victims' networks to gain remote control capabilities, and has been analyzed in the past. The tool was installed on the four Piriform computers on April 12th, 2017, while the preliminary version of stage two had been installed on the computers on March 12th, 2017.

The older version of the stage two downloader was contacting CnC servers, but the servers were no longer functioning by the time we got our hands on the computers, so we cannot say with 100% certainty what they were supposed to download. However, given the timeline of the events, we assume that the preliminary stage two downloader installed ShadowPad on the four Piriform computers. Another clue that lead us to this assumption is that ShadowPad is believed to be a product of the Chinese hacker group, Axiom, the group likely behind the CCleaner attack. The connection between Axiom and the CCleaner attack was first discovered by security researcher Constin Raiu.



ShadowPad plugins found on Piriform PCs

We also found ShadowPad log files that contained encrypted keystrokes from a keylogger installed on the computers. We discovered that the keylogger's log was encrypted with the volume ID of the hard drive and consequently were able to decrypt the key strokes. Looking into the log, we found out that the keylogger had been active since April 12th, 2017, recording keystrokes on these computers, including keylogs from Visual Studio and other programs. The logged data showed us that the keylogger was functional at that time. The version of the ShadowPad tool is custom-built, which makes us think it was explicitly built for Piriform.



Logged keystrokes found on the Piriform computers

By installing a tool like ShadowPad, the cybercriminals were able to fully control the system remotely while collecting credentials and insights into the operations on the targeted computer. Besides the keylogger tool, other tools were installed on the four computers, including a password stealer, and tools with the capacity to install further software and plugins on the targeted computer remotely.

ShadowPad was installed on the Piriform network and, as far as we can tell from our investigations up until today, it was not installed on any of the CCleaner customers' computers, however we believe it was the intended third stage for the CCleaner customers. While up to 2.27 million CCleaner consumers and businesses had downloaded the infected CCleaner product, the attackers installed the malicious second stage on just 40 PCs operated by high-tech and telecommunications companies. We don't have a sample of a possible third stage that might have been distributed via the CCleaner attack, and it is not clear if it was the attacker's intention to attack all 40 PCs or just a few or none. We continue investigating the data dumps from the computers, and will post an update as soon as we learn more.
