Progress on CCleaner Investigation

blog.avast.com/progress-on-ccleaner-investigation

Vince Steckler & Ondrej Vlcek 21 Sep 2017

Large technology and telecommunications companies were targeted

Following the take-down of the CnC server and getting access to its data, the Avast Security Threat Labs team has been working around the clock to investigate the source and other details of the recent Piriform CCleaner attack. To recap, the attack affected a total of 2.27M computers between August 15, 2017 and September 15, 2017 and used the popular PC cleaning software CCleaner version 5.33.6162 as a distribution vehicle. Today, we would like to report on the progress so far.

First of all, analysis of the data from the CnC server has proven that this was an APT (Advanced Persistent Threat) programmed to deliver the 2nd stage payload to select users. Specifically, the server logs indicated 20 machines in a total of 8 organizations to which the 2nd stage payload was sent, but given that the logs were only collected for little over three days, the actual number of computers that received the 2nd stage payload was likely at least in the order of hundreds. This is a change from our previous statement, in which we said that to the best of our knowledge, the 2nd stage payload never delivered.

At the time the server was taken down, the attack was targeting select large technology and telecommunication companies in Japan, Taiwan, UK, Germany and the US. Given that CCleaner is a consumer-oriented product, this was a typical watering hole attack where the vast majority of users were uninteresting for the attacker, but select ones were. For privacy reasons, we're not disclosing the list of targeted companies publicly; instead, we have been reaching out individually to those companies who we know have been impacted, and providing them with additional technical information to assist them.

The 2nd stage payload is a relatively complex piece of code that uses two components (DLLs). The first component contains the main business logic. As with the first payload, it is heavily obfuscated and uses a number of anti-debugging and anti-emulation tricks. Much of the logic is related to the finding of, and connecting to, yet another CnC server, whose address can be determined using three different mechanisms: 1) an account on GitHub, 2) an account on Wordpress, and 3) a DNS record of a domain get.ad*xxxxxx*.net (name modified here). Subsequently, the address of the CnC server can also be arbitrarily modified in the future by sending a special command, recognized by the code as a signal to use the DNS protocol (udp/53) to get the address of the new server. Together with law enforcement, we're continuing the analysis by getting access to the data from these additional CnC servers and tracing further to the attacker.

The second part of the payload is responsible for persistence. Here, a different mechanism is used on Windows 7+ than on Windows XP. On Windows 7+, the binary is dumped to a file called "C:\Windows\system32\ITSMSISrv.dll" and automatic loading of the library is ensured by autorunning the NT service "SessionEnv" (the RDP service). On XP, the binary is saved as "C:\Windows\system32\spool\prtprocs\w32x86\localspl.dll" and the code uses the "Spooler" service to load.

Structurally, the DLLs are quite interesting because they piggyback on other vendors' code by injecting the malicious functionality into legitimate DLLs. The 32-bit code is activated through a patched version of VirtCDRDrv32.dll (part of Corel's WinZip package), while the 64-bit uses EFACli64.dll – part of a Symantec product. Most of the malicious code is delivered from registry (the binary code is saved directly in registry in keys "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WbemPerf\00[1-4]"). Again, all of these techniques demonstrate the attacker's high level of sophistication.

In parallel to the technical analysis, we have continued working with law enforcement units to trace back the source of the attack. We are committed to getting to the bottom of who is behind this attack. While providing routine periodic updates, our energies are focused on catching the perpetrators. Our approach is to do all of this in the background, to increase our chances of identifying the perpetrator. We believe nothing is served by being too noisy, e.g. stating who was targeted and/or compromised and it is up to the target to choose when to disclose.

Finally, it is extremely important to us to resolve the issue on customer machines. For consumers, we stand by the recommendation to upgrade CCleaner to the latest version (now 5.35, after we have revoked the signing certificate used to sign the impacted version 5.33) and use a quality antivirus product, such as Avast Antivirus. For corporate users, the decision may be different and will likely depend on corporate IT policies. At this stage, we cannot state that the corporate machines could not be compromised, even though the attack was highly targeted.

We will provide additional updates as we progress.

Vince Steckler, CEO
Ondrej Vlcek, CTO and EVP Consumer Business