The CCleaner Malware Fiasco Targeted at Least 18 Specific Tech Firms

wired.com/story/ccleaner-malware-targeted-tech-firms

Andy Greenberg September 21, 2017

Update: On September 25, Avast confirmed that of the 18 companies targeted, a total of 40 computers were successfully infected with a secondary malware installation at the following companies: Samsung, Sony, Asus, Intel, VMWare, O2, Singtel, Gauselmann, Dyn, Chunghwa and Fujitsu.

Hundreds of thousands of computers getting penetrated by a corrupted version of an ultra-common piece of security software was never going to end well. But now it's becoming clear exactly how bad the results of the recent CCleaner malware outbreak may be. Researchers now believe that the hackers behind it were bent not only on mass infections, but on targeted espionage that tried to gain access to the networks of at least 18 tech firms.

Earlier this week, security firms Morphisec and Cisco revealed that CCleaner, a piece of security software distributed by Czech company Avast, had been hijacked by hackers and loaded with a backdoor that evaded the company's security checks. It wound up installed on more than 700,000 computers. On Wednesday, researchers at Cisco's Talos security division revealed that they've now analyzed the hackers' "command-and-control" server to which those malicious versions of CCleaner connected.

On that server, they found evidence that the hackers had attempted to filter their collection of backdoored victim machines to find computers inside the networks of 18 tech firms, including Intel, Google, Microsoft, Akamai, Samsung, Sony, VMware, HTC, Linksys, D-Link and Cisco itself. In about half of those cases, says Talos research manager Craig Williams, the hackers successfully found a machine they'd compromised within the company's network, and used their backdoor to infect it with another piece of malware intended to serve as a deeper foothold, one that Cisco now believes was likely intended for industrial espionage.[2]

"When we found this initially, we knew it had infected a lot of companies," says Williams. "Now we know this was being used as a dragnet to target these [companies] worldwide...to get footholds in companies that have valuable things to steal, including Cisco unfortunately."

A Wide Net

Cisco says it obtained a digital copy of the hackers' command-and-control server from an unnamed source involved in the CCleaner investigation. The server contained a database of every backdoored computer that had "phoned home" to the hackers' machine between September 12 and 16. That included over 700,000 PCs, just as Avast has said in the days since it first revealed its CCleaner debacle. (Initially the company put the number much higher, at 2.27 million.) But the database also showed a list of specific domains onto which the hackers sought to install their secondary malware payload, as well as which ones received that second infection.

The secondary payload targeted 18 companies in all, but Williams notes that some companies had more than one computer compromised, and some had none. He declined to say which of the targets had in fact been breached, but Cisco says it's alerted all the affected companies to the attack.

Williams also notes the target list Cisco found likely isn't comprehensive; it appears to have been "trimmed," he says. It may have included evidence of other targets, successfully breached or not, that the hackers had sought to infect with their secondary payload earlier in the month-long period when the corrupted version of CCleaner was being distributed. "It’s very likely they modified this through the monthlong campaign, and it’s almost certain that they changed the list around as they progressed and probably targeted even more companies," says Williams.

In an update post Thursday morning, Avast backed Cisco's findings, and confirmed that eight of the 18 known target companies had been breached by the hackers. But it also wrote that the total number of victim firms "was likely at least in the order of hundreds."[1]

That target list presents a new wrinkle in the unfolding analysis of the CCleaner attack, one that shifts it from what might have otherwise been a run-of-the-mill mass cybercrime scheme to a potentially state-sponsored spying operation that cast a wide net, and then filtered it for specific tech-industry victims. Cisco and security firm Kaspersky have both pointed out that

the malware element in the tainted version of CCleaner shares some code with a sophisticated hacking group known as Group 72, or Axiom, which security firm Novetta named a Chinese government operation in 2015.

Cisco concedes that code reuse alone doesn't represent a definitive link between the CCleaner attack and Axiom, not to mention China. But it also notes that one configuration file on the attackers' server was set for China's time zone—while still acknowledging that's not enough for attribution.

Supply Chain Woes

For any company that may have had computers running the corrupted version of CCleaner on their network, Cisco warns that its findings mean merely deleting that application is no guarantee the CCleaner backdoor wasn't used to plant a secondary piece of malware on their network, one with its own, still-active command and control server. Instead, the researchers recommend that anyone affected fully restore their machines from backup versions prior to the installation of Avast's tainted security program. "If you didn't restore your system from backup, you're at high risk of not having cleaned this up," Williams says.

The exact dimensions of the CCleaner attack will likely continue to be redrawn, as analysis continues. But it already represents another serious example in the string of software supply-chain attacks that have recently rocked the internet. Two months earlier, hackers hijacked the update mechanism of the Ukrainian accounting software MeDoc to deliver a destructive piece of software known as NotPetya, causing massive damage to companies in Ukraine as well as in Europe and the United States. In that case, as in the CCleaner attack, victims installed seemingly legitimate software from a small but trusted company, only to find that it had been silently corrupted, deeply infecting their IT systems.

In the days following the NotPetya attack, many in the security research community shifted their assessment of the attack from a criminal ransomware outbreak to something more insidious, targeted, and created by nation-state hackers. Now, it seems that the mystery surrounding the CCleaner attack may be moving in that same, disturbing direction.

[1]*Updated 9/21/2017 11:15am with a comment from Avast.*[2]*Correction 9/21/2017 1:08pm to change the number of total companies targeted to 18. While Cisco had initially reported 20, that number had counted some different domains of companies separately.*[3]*Updated 9/25/2017 4:20PM EST with additional information from Avast.*