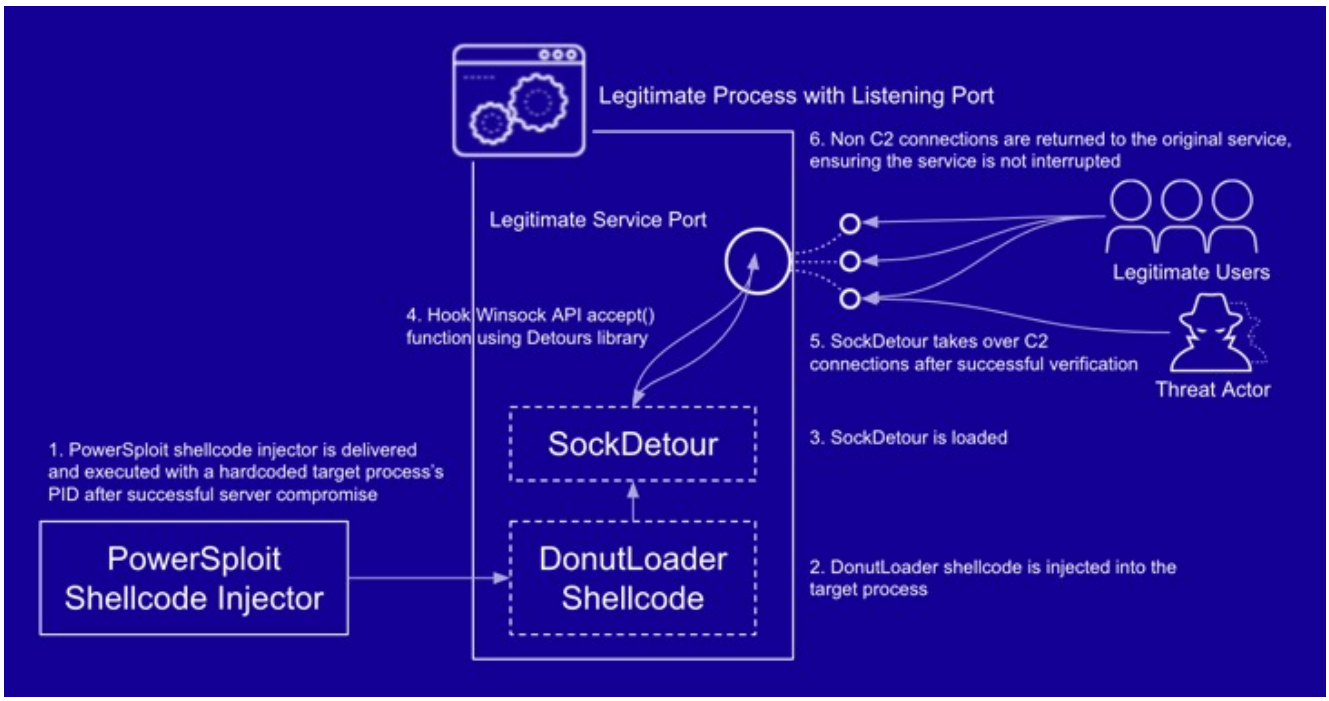
New "SockDetour" Fileless, Socketless Backdoor Targets U.S. Defense Contractors

thehackernews.com/2022/02/new-sockdetour-fileless-socketless.html

February 25, 2022



Cybersecurity researchers have taken the wraps off a previously undocumented and stealthy custom malware called **SockDetour** that targeted U.S.-based defense contractors with the goal of being used as a secondary implant on compromised Windows hosts.

"SockDetour is a backdoor that is designed to remain stealthily on compromised Windows servers so that it can serve as a backup backdoor in case the primary one fails," Palo Alto Networks' Unit 42 threat intelligence said in a report published Thursday. "It is difficult to detect, since it operates filelessly and socketlessly on compromised Windows servers."

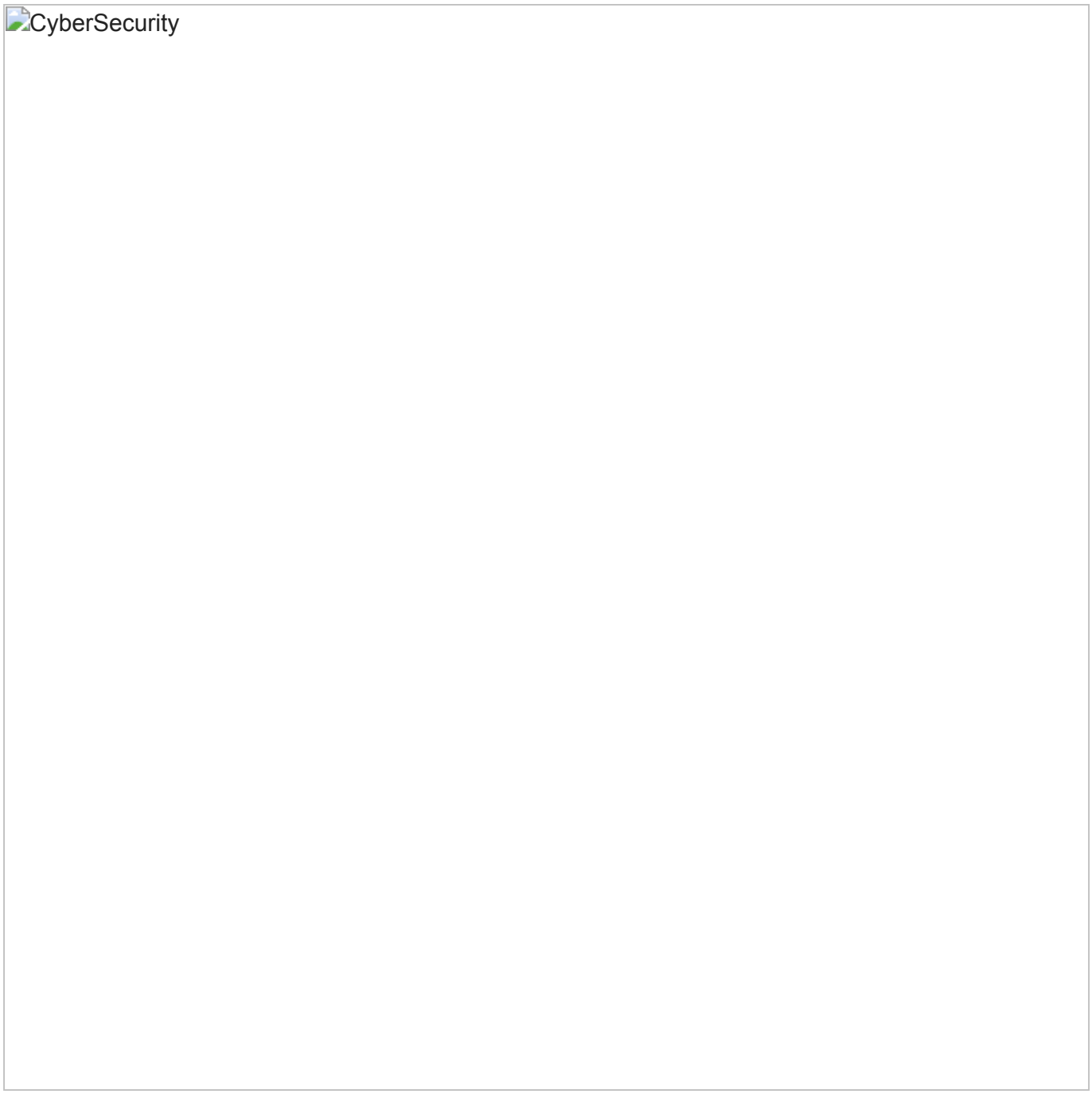
Even more concerningly, SockDetour is believed to have been used in attacks since at least July 2019, based on a compilation timestamp on the sample, implying that the backdoor successfully managed to slip past detection for over two-and-a-half years.

The attacks have been attributed to a threat cluster it tracks as TiltedTemple (aka DEV-0322 by Microsoft), which is the designated moniker for a hacking group operating out of China and was instrumental in exploiting zero-day flaws in Zoho ManageEngine ADSelfService Plus and ServiceDesk Plus deployments as a launchpad for malware attacks last year.

The ties to TiltedTemple come from overlaps in the attack infrastructure, with one of the command-and-control (C2) servers that was used to facilitate the distribution of malware for the late 2021 campaigns also hosting the SockDetour backdoor, alongside a memory dumping utility and numerous web shells for remote access.

Unit 42 said it unearthed evidence of at least four defense contractors targeted by the new wave of attacks, resulting in the compromise of one of them.

The intrusions also predate the attacks that occurred through compromised Zoho ManageEngine servers in August 2021 by a month. Analysis of the campaign has revealed that SockDetour was delivered from an external FTP server to a U.S.-based defense contractor's internet-facing Windows server on July 27, 2021.



"The FTP server that hosted SockDetour was a compromised Quality Network Appliance Provider (QNAP) small office and home office (SOHO) network-attached storage (NAS) server," the researchers pointed out. "The NAS server is known to have multiple vulnerabilities, including a remote code execution vulnerability, CVE-2021-28799."

What's more, the same server is said to have been already infected with the QLocker ransomware, raising the possibility the TiltedTemple actor leveraged the aforementioned flaw to gain unauthorized initial access.

SockDetour, for its part, is fashioned as a stand-in backdoor that hijacks legitimate processes' network sockets to establish its own encrypted C2 channel, followed by loading an unidentified plugin DLL file retrieved from the server.

"Thus, SockDetour requires neither opening a listening port from which to receive a connection nor calling out to an external network to establish a remote C2 channel," the researchers said. "This makes the backdoor more difficult to detect from both host and network level."

SHARE □ □ □ □ □
SHARE □