US defense contractors hit by stealthy SockDetour Windows backdoor

bleepingcomputer.com/news/security/defense-contractors-hit-by-stealthy-sockdetour-windows-backdoor/

Sergiu Gatlan

By
Sergiu Gatlan

- February 24, 2022
- 11:43 AM
- 0

Image: Milo Bauman

A new custom malware dubbed SockDetour found on systems belonging to US defense contractors has been used as a backup backdoor to maintain access to compromised networks.

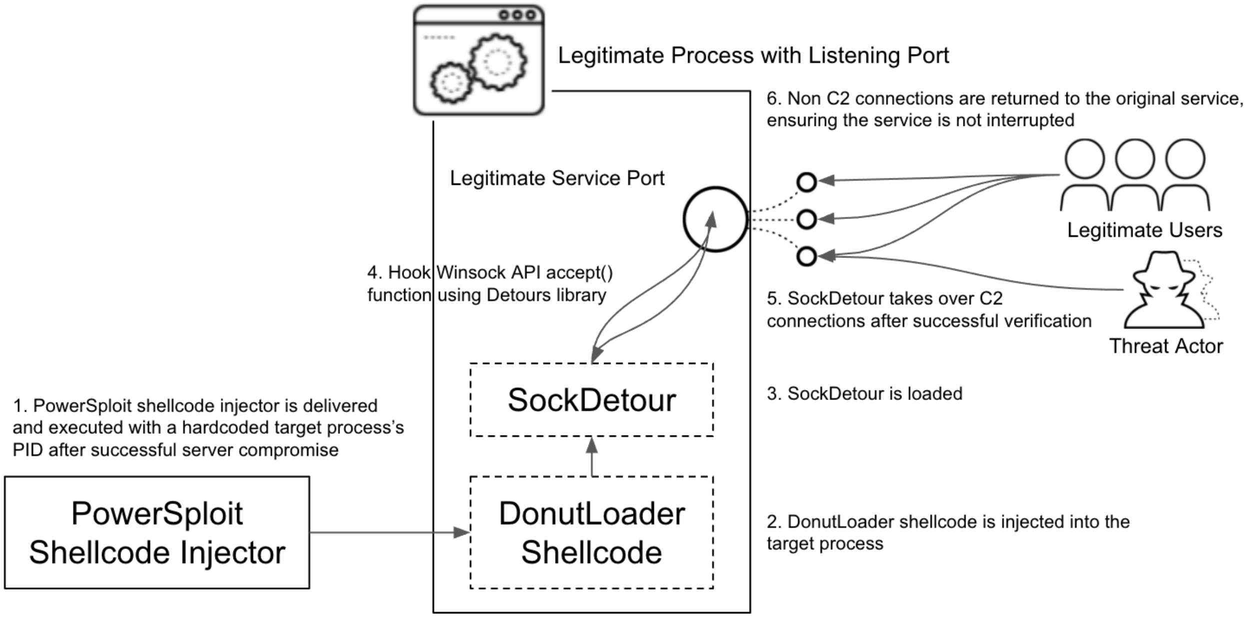
The malicious payload was spotted by Unit 42 security researchers, who believe that its operators kept the backdoor under the radar for a long time as it has been used in the wild since at least July 2019.

SockDetour's stealthiness can be explained by the fact that it "operates filelessly and socketlessly" on infected Windows servers by hijacking network connections, making it a lot harder to detect at the host and network levels.

The connection hijacking is done using the legitimate Microsoft Detours library package used for Windows API call monitoring and instrumentation.

"With such implementation, SockDetour [..] serves as a backup backdoor in case the primary backdoor is detected and removed by defenders," Unit 42 explained.

In one of the attacks, the threat actors also used a very specific delivery server, a QNAP network-attached storage (NAS) device typically used by small businesses and previously infected with QLocker ransomware — they likely exploited the same security flaw (the CVE-2021-28799 remote code execution bug) to gain access to the server.


Legitimate Process with Listening Port
6. Non C2 connections are returned to the original service, ensuring the service is not interrupted
Legitimate Service Port
Legitimate Users
4. Hook Winsock API accept() function using Detours library
5. SockDetour takes over C2 connections after successful verification
Threat Actor
SockDetour
3. SockDetour is loaded
1. PowerSploit shellcode injector is delivered and executed with a hardcoded target process's PID after successful server compromise
PowerSploit Shellcode Injector
DonutLoader Shellcode
2. DonutLoader shellcode is injected into the target process

SockDetour backdoor workflow (Unit 42)

The researchers first spotted the malware being deployed onto the Windows server of at least one US defense contractor on July 27, 2021, which led to the discovery of three other defense orgs being targeted by the same group with the same backdoor.

"Based on Unit 42's telemetry data and the analysis of the collected samples, we believe the threat actor behind SockDetour has been focused on targeting U.S.-based defense contractors using the tools," the researchers revealed.

"Unit 42 has evidence of at least four defense contractors being targeted by this campaign, with a compromise of at least one contractor."

The Chinese connection

The SockDetour backdoor is used in attacks by an APT activity cluster tracked by Unit 42 as TiltedTemple and previously linked to attacks exploiting several vulnerabilities in Zoho products, including ManageEngine ADSelfService Plus (CVE-2021-40539) and ServiceDesk Plus (CVE-2021-44077).

While the company did not attribute the SockDetour malware to a specific hacking group, Unit 42 researchers suspected in November that the TiltedTemple campaign is the work of a Chinese-sponsored threat group tracked as APT27.

The partial attribution is based on tactics and malicious tools matching APT27's previous activity and similar targeting of the same range of industry sectors (e.g., defense, technology, energy, aerospace, government, and manufacturing) for cyber espionage.

TiltedTemple attacks focused on Zoho vulnerabilities led to the breach of networks belonging to critical infrastructure orgs organizations worldwide in three different campaigns throughout 2021, using:

- an ADSelfService zero-day exploit between early-August and mid-September,
- an n-day AdSelfService exploit until late October,
- and a ServiceDesk one starting with October 25.

Related Articles:

US, UK link new Cyclops Blink malware to Russian state hackers

New ChromeLoader malware surge threatens browsers worldwide

FTC fines Twitter $150M for using 2FA info for targeted advertising

New ERMAC 2.0 Android malware steals accounts, wallets from 467 apps

BPFDoor malware uses Solaris vulnerability to get root privileges