

Unidentified RAT pushes NetSupport RAT

 isc.sans.edu/diary/Unidentified+RAT+pushes+NetSupport+RAT/33034

Published: 2026-06-01. **Last Updated:** 2026-06-01 00:02:30 UTC

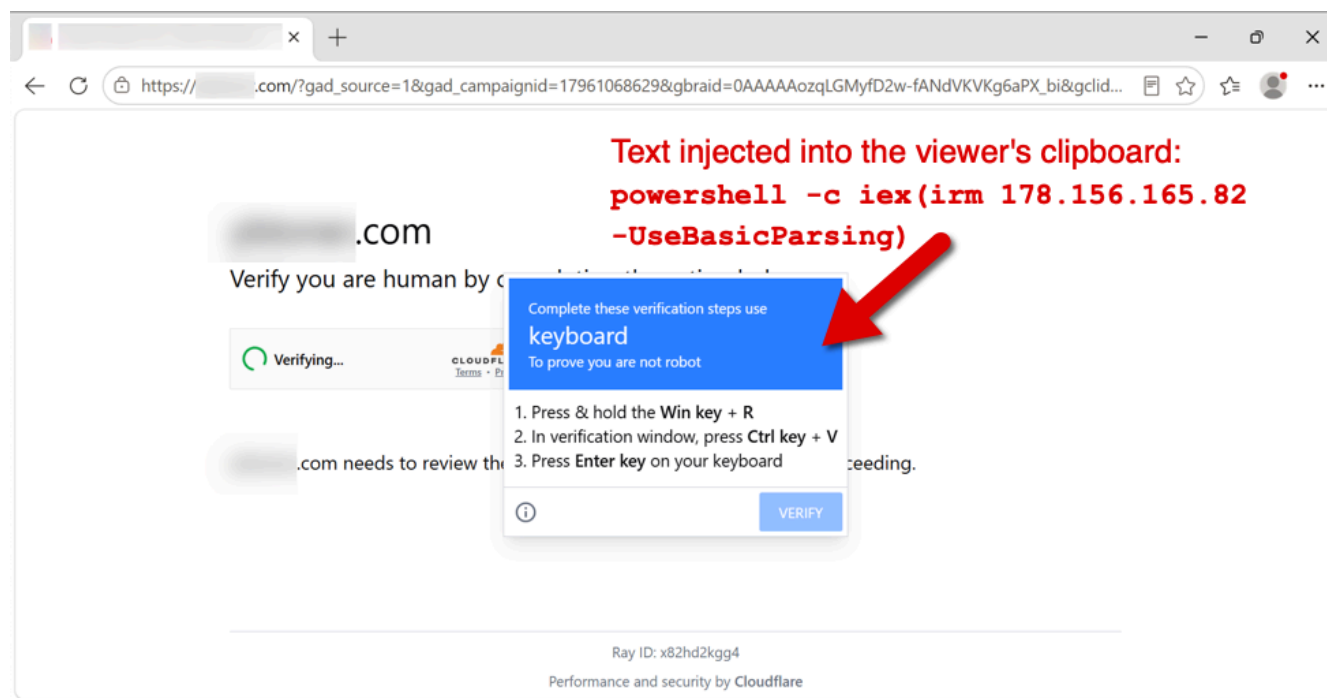
by [Brad Duncan](#) (Version: 1)

[0 comment\(s\)](#)

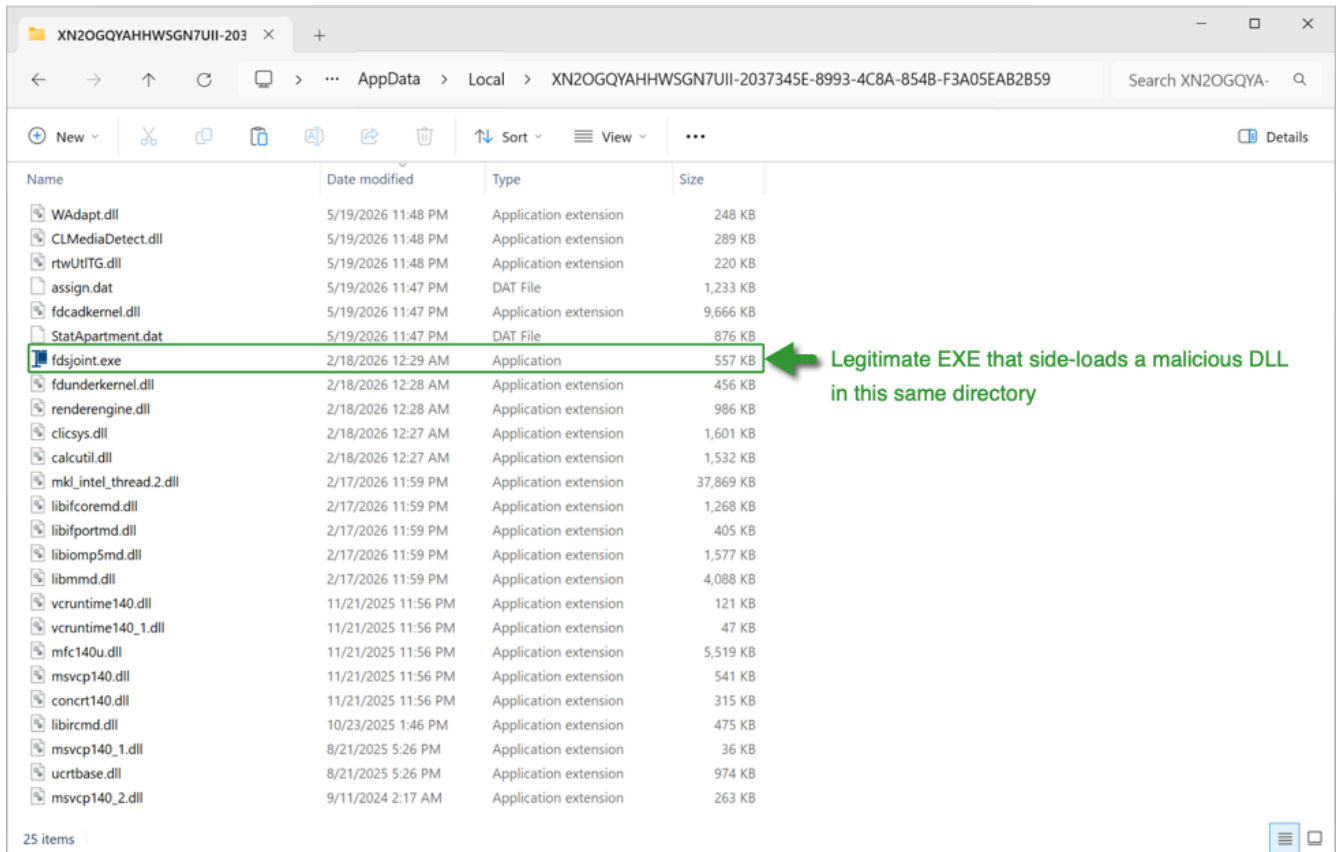
Introduction

This diary provides indicators from an unidentified RAT infection on Wednesday 2026-05-27 that was followed by a malicious NetSupport Manager RAT package. This originated from the SmartApeSG ClickFix campaign. I still don't know the name of the initial RAT, but it has consistently been generating encoded (not HTTPS/SSL/TLS) traffic to a command and control (C2) server at 89.110.110[.]119 over TCP port 443 since I first noticed it sometime in April 2026.

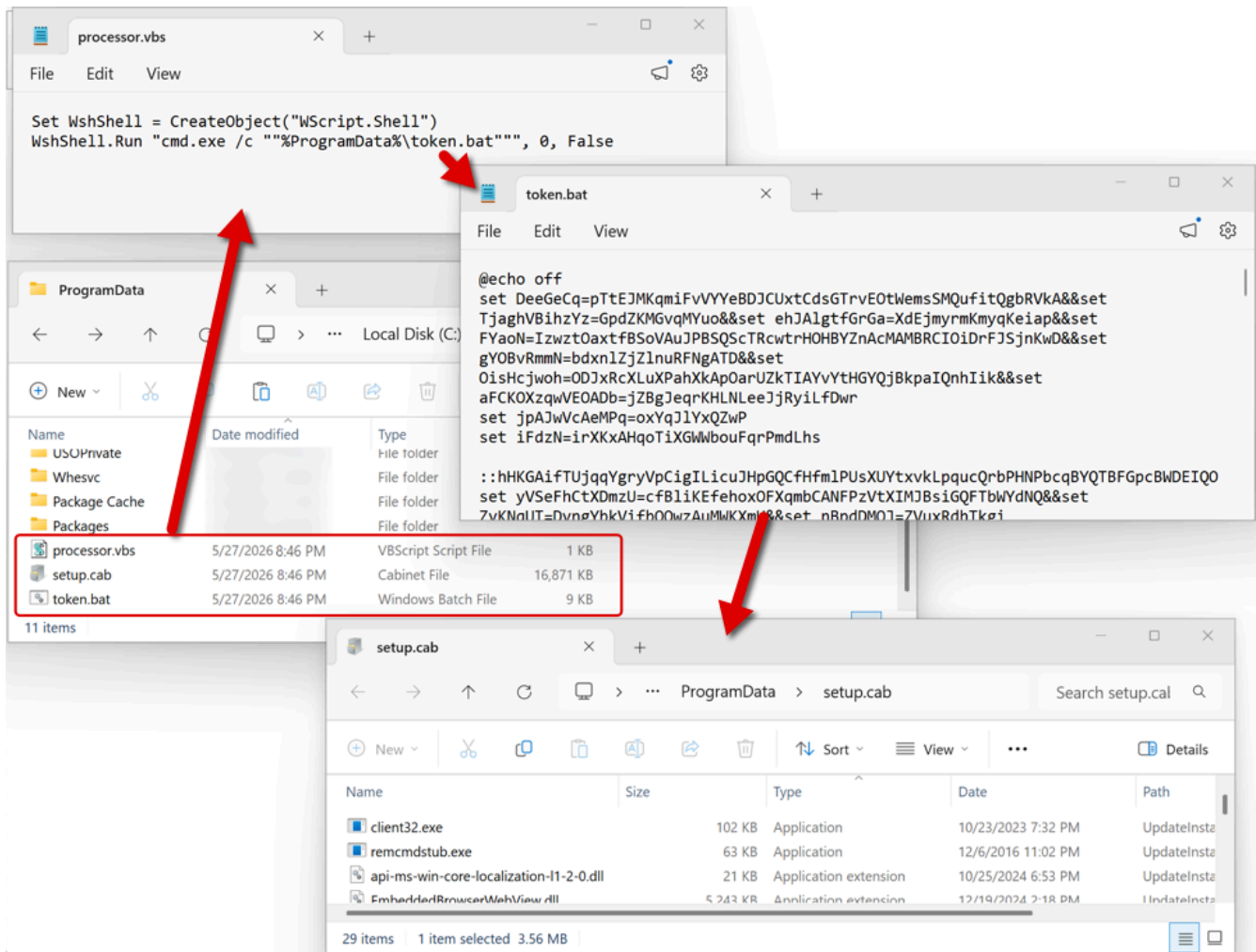
Images from the infection



Shown above: Fake verification page with ClickFix instructions from the SmartApeSG campaign.



Shown above: Initial RAT malware on an infected Windows host.



Shown above: Follow-up files for NetSupport RAT sent through the initial RAT C2 traffic.

Time	Dst	Port	Host	Info
2026-05-27 20:47:25	172.67.68.212	80	geo.netsupportsoftware.com	GET /location/loca.asp HTTP/1.1
2026-05-27 20:47:25	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 20:47:25	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 20:47:26	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 20:47:26	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 20:48:26	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 20:49:26	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 20:50:26	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 20:51:26	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 20:52:26	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 20:53:27	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 20:54:27	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 20:55:27	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 20:56:27	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 20:57:27	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 20:58:27	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 20:59:27	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 21:00:27	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 21:01:27	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 21:02:27	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 21:03:28	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 21:04:28	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 21:05:28	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 21:06:28	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 21:07:28	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 21:08:28	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 21:09:28	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 21:10:28	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 21:11:28	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/
2026-05-27 21:12:28	185.163.47.217	443	185.163.47.217	POST http://185.163.47.217/fakeurl.htm HTTP/

Shown above: NetSupport RAT C2 traffic.

Indicators of Compromise

Example of SmartApeSG URLs seen on Wednesday 2026-05-27:

- hxxps[:]//hiddenplanetlab[.]top/signin/secure-util.js
- hxxps[:]//hiddenplanetlab[.]top/signin/private-template?c66kjD5i
- hxxps[:]//hiddenplanetlab[.]top/signin/legacy-worker.js?18b3825af007e53d

Example of traffic generated by running the associated ClickFix script:

- hxxp[:]//178.156.165[.]82/
- hxxp[:]//178.156.173[.]194/
- hxxps[:]//silverharvestnetwork[.]com/check

Initial RAT C2 traffic:

tcp[:]//89.110.110[.]119:443/

IP address for NetSupport RAT C2 server:

hxxp[:]//185.163.47[.]217:443

Files from the infection:

SHA256 hash: [1514b1268e9dc6d2f37137aa38c756cb4bf8186ac9235d6863b78e7f8bbbe976](#)

- File size: 26,555,757 bytes
- File type: Zip archive data, at least v2.0 to extract
- File location: hxxps[:]//silverharvestnetwork[.]com/check
- File description: Zip archive containing software package for the initial RAT.

SHA256 hash: [469bac8e10f50263e8ff0806e6ba126bb4cc660799129a8653eab3f8ec7201e5](#)

- File size: 109 bytes
- File type: ASCII text
- File location: C:\ProgramData\processor.vbs
- File description: Initial script that runs token.bat

SHA256 hash: [9c7eda2c4d3aaa8746495741bef57a07de180f0409409faf0f91658e88ba33f5](#)

- File size: 8,262 bytes
- File type: DOS batch file text, ASCII text, with very long lines
- File location: C:\ProgramData\token.bat
- File description: Batch scrip that extracts, runs, and makes persistent NetSupport RAT from setub.cab

SHA256 hash: [7ba5481c873bb3081442561f749f590badd72ef249fddfe993e30b28dc0c2112](#)

- File size: 17,275,805 bytes
- File type: Microsoft Cabinet archive data
- File location: C:\ProgramData\setup.cab
- File description: CAB file containing malicious NetSupport RAT package
- Contents of this CAB file extracted to: C:\ProgramData\UpdateInstaller\

Note 1: The files processor.vbs, token.bat, and setup.cab are all deleted by the token.bat script after it installs the malicious NetSupport RAT package and makes it persistent on the infected Windows host.

Note 2: The indicators for this activity (domains, file hashes, etc.) change on a daily basis. For more up-to-date indicators on SmartApeSG and similar campaigns, see the [@monitorsg feed](#) on Mastodon.

Bradley Duncan

brad [at] malware-traffic-analysis.net

Keywords: [SmartApeSG](#) [RAT](#) [NetSupportRAT](#) [NetSupport](#) [ClickFix](#)
[0 comment\(s\)](#)