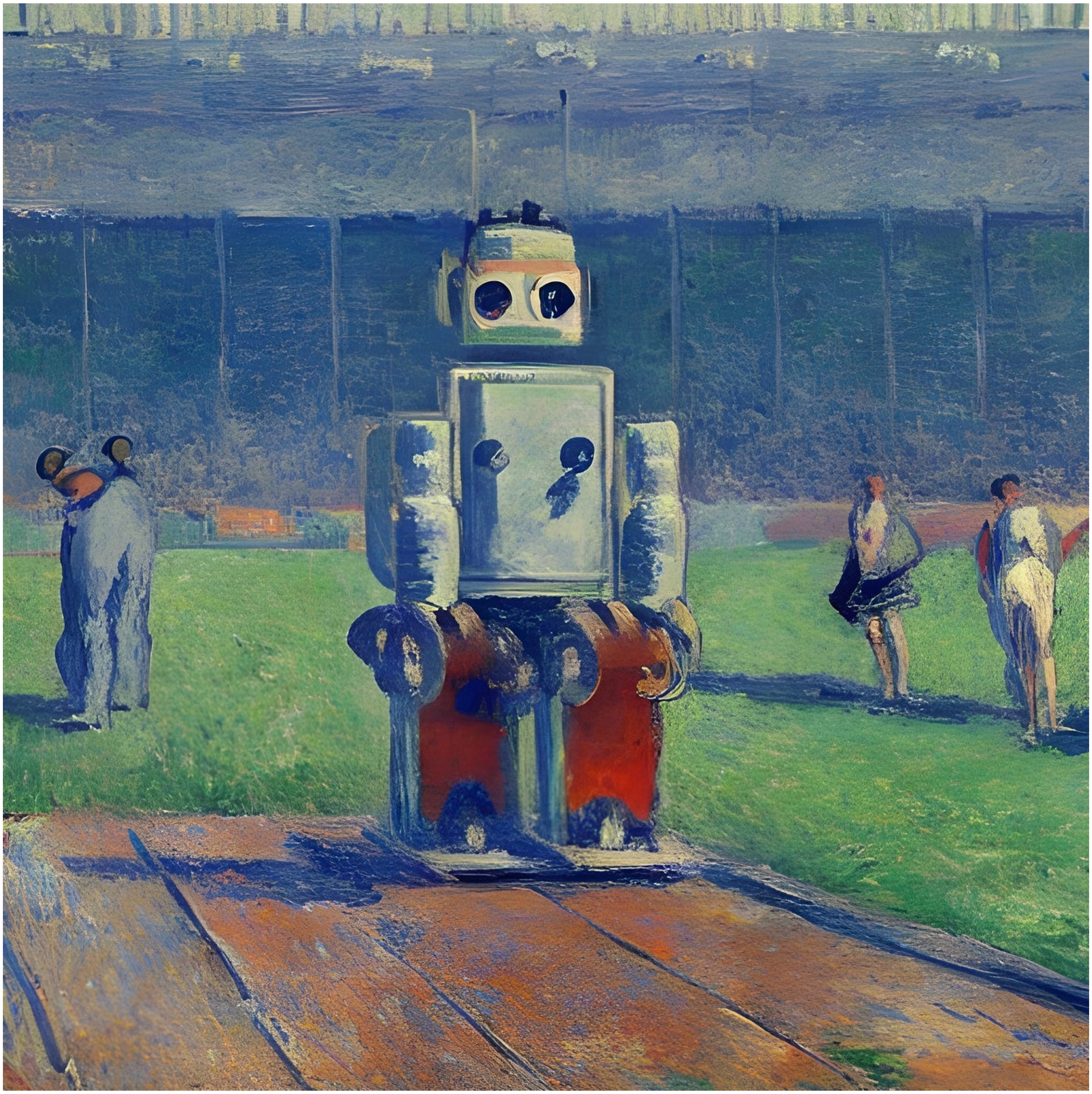
SmartApeSG | by Jonathan Mccay | Walmart Global Tech Blog | Oct, 2023

medium.com/walmartglobaltech/smartapesg-4605157a5b80

Jonathan Mccay　　　　October 26, 2023



SmartApeSG

--

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.

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

Compromised Site Inject

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.

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.

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

Older javascript payload

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

Obfuscated javascript payload

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

Base64 encoded .zip

SmartApeSG — Fake Update

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

Extracted .zip
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.

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.

Powershell — Download & Execute

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

Netsupport:

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/
bin.js
```

HKCU — Run Key

```
DIVXDIVXX
```

SmartApeSG:

```
cdespto[.]orgseyishalom[.]combaroksmig[.]onlinecheetahsnv[.]comclubcamporico[.]comalti
cex-io[.]comnilselsholz[.]comcredit-
volta[.]comaflomusic[.]comwebull[.]artzahrajoulaei[.]techdomaintestss[.]xyzpixelbase[.
posh[.]compolyfieldgallery[.]comseosuccesslab[.]comoffshorechain[.]orglucyflix[.]commy
rem[.]commansaentertainment[.]comloloalexander[.]comgnavigatio[.]comarauas[.]comgamefl
```

SmartApeSG — Netsupport:

```
94.158.244[.]11894.158.247[.]23185.163.46[.]935.252.178[.]485.252.177[.]2145.252.177[.
```

References

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