The Seamless Campaign Isn’t Losing Any Steam

malwarebreakdown.com/2017/08/23/the-seamless-campaign-isnt-losing-any-steam/

August 23, 2017

Some security researchers on Tuesday had noted that their requests for the Seamless gates were failing. However, if there was any noticeable stoppage, it certainly didn’t last very long. Shortly after hearing about this I started checking my logs for any exploit kit activity and, as usual, I found a detection for RIG EK from one of our Palo Alto firewalls. Checking the traffic before the RIG EK detection showed the culprit to be the Seamless campaign.

Here is an example of the infection chain that I found:

```
Ad -> 193.124.xxx.xxx/vnc-seller -> 193.124.xxx.xxx/vnc-seller/ -> paremated-
conproxy[.]com -> 15cen.redirectvoluum[.]com -> 194.58.xxx.xxx/signu1.php
```

The redirection chain that I found hasn’t changed much, however, this is the first time I’ve seen requests for /vnc-seller and /vnc-seller/. This could have had something to do with the geo-location of the host or the HTTP referer.

Other notable changes include the addition of the domain paremated-conproxy[.]com and the subdomain 15cen.redirectvoluum[.]com. They had been using the subdomains tqbeu.voluumtrk[.]com and tqbeu.redirectvoluum[.]com to redirect hosts to the Seamless gate.

The domain paremated-conproxy[.]com was first seen on 8/18/17. The Whois information is private. The subdomain 15cen.redirectvoluum[.]com was registered by CodeWise and was first seen on 08/21/17. They’re using CodeWise’s marketing suite called “Voluum“.

Furthermore, the Seamless .php file that returns the iframe pointing to the RIG EK landing page is now called signu[1-4].php rather than signup[1-4].php.

It was at this point that I decided to go hunting for my own infection.

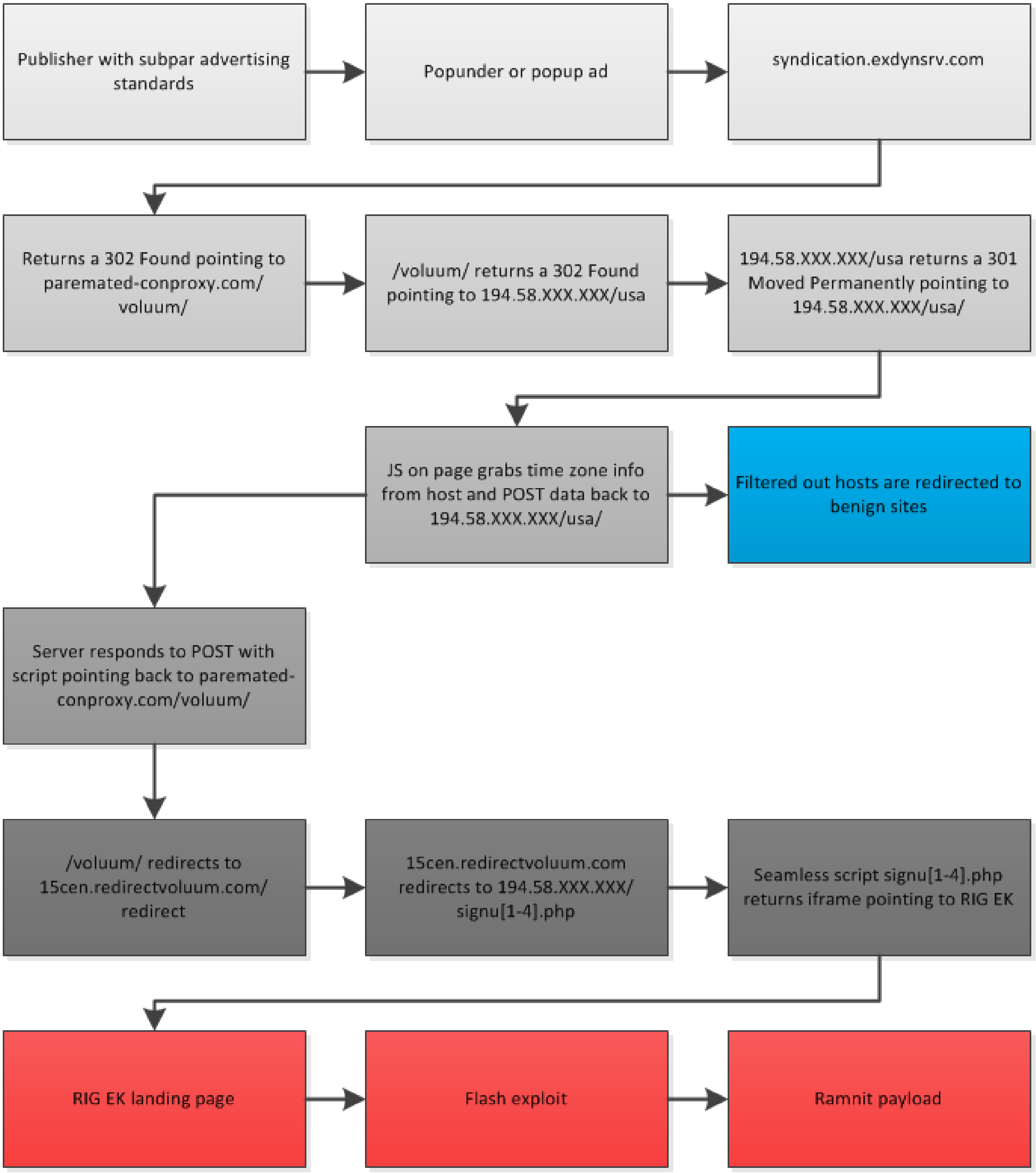
The publisher that I used for my infection chain was another video streaming site. According to Alexa it is currently ranked in the top 69,000 globally and top 36,000 in the United States. Below is Alexa’s statistics on the site’s visitors by country:

Country	Percent of Visitors	Rank in Country
United States	27.20%	35,100
United Kingdom	14.60%	13,900
India	12.50%	23,900

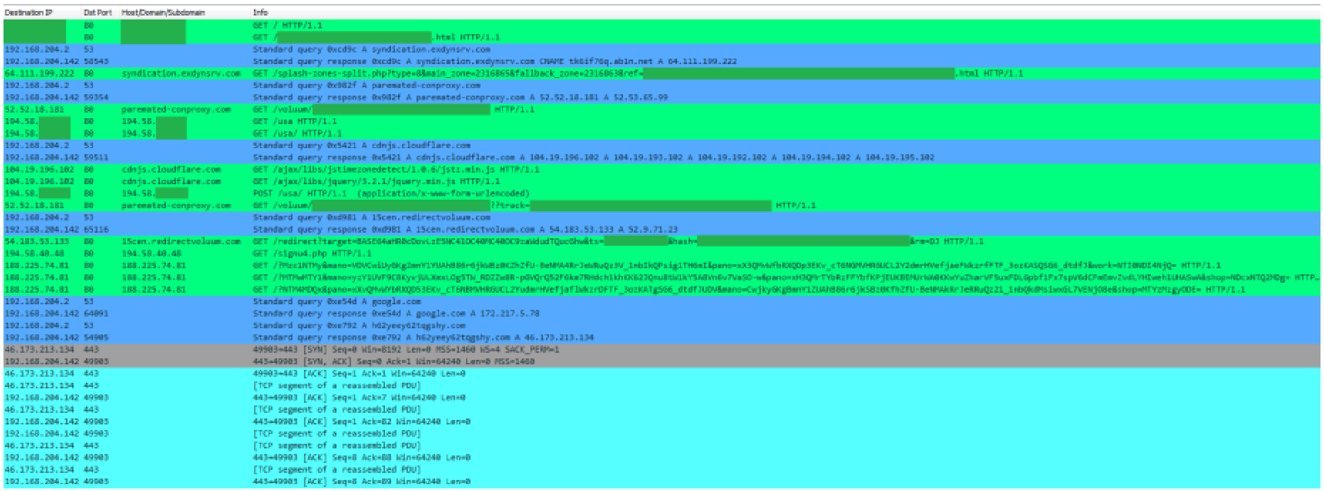
South Africa	4.60%	7,500
Australia	3.80%	19,100

Overall the site received roughly 340,000 visitors in the last 30 days.

Below is a flowchart from my infection:

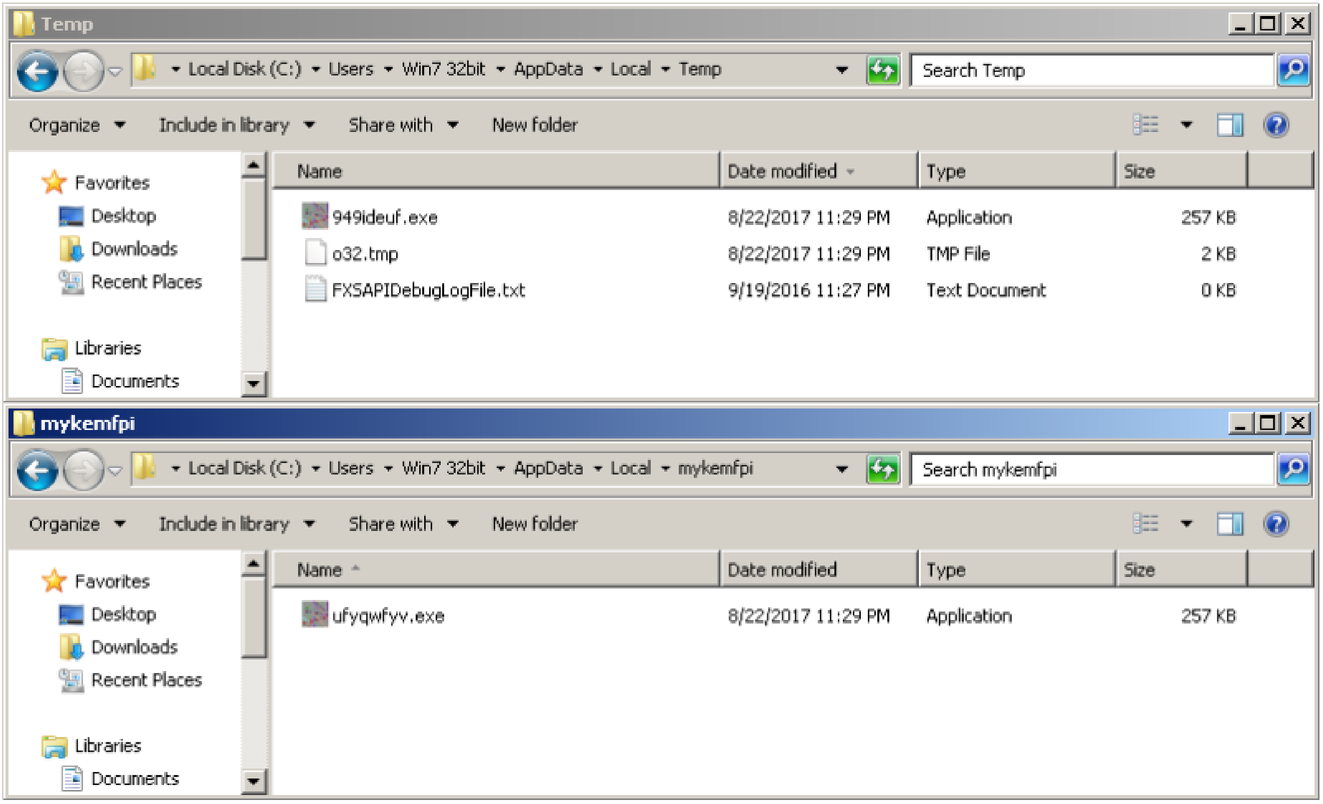

Publisher with subpar advertising standards
Popunder or popup ad
syndication.exdynsrv.com
Returns a 302 Found pointing to paremated-conproxy.com/voluum/
/voluum/ returns a 302 Found pointing to 194.58.XXX.XXX/usa
194.58.XXX.XXX/usa returns a 301 Moved Permanently pointing to 194.58.XXX.XXX/usa/
JS on page grabs time zone info from host and POST data back to 194.58.XXX.XXX/usa/
Filtered out hosts are redirected to benign sites
Server responds to POST with script pointing back to paremated-conproxy.com/voluum/
/voluum/ redirects to 15cen.redirectvoluum.com/redirect
15cen.redirectvoluum.com redirects to 194.58.XXX.XXX/signu[1-4].php
Seamless script signu[1-4].php returns iframe pointing to RIG EK
RIG EK landing page
Flash exploit
Ramnit payload

Below is an image of the HTTP, DNS, and C2 traffic filtered in Wireshark:



```
Destination IP    Dst Port Host/Domain/Subdomain      Info
[redacted]        80       [redacted]                 GET / HTTP/1.1
                  80                                  GET /[redacted].html HTTP/1.1
192.168.204.2     53                                  Standard query 0xcd9c A syndication.exdynsrv.com
192.168.204.142   58543                               Standard query response 0xcd9c A syndication.exdynsrv.com CNAME tk6if76q.ab1n.net A 64.111.199.222
64.111.199.222    80       syndication.exdynsrv.com   GET /splash-zones-split.php?type=8&main_zone=2316865&fallback_zone=2316863&ref=[redacted].html HTTP/1.1
192.168.204.2     53                                  Standard query 0x982f A paremated-conproxy.com
192.168.204.142   59354                               Standard query response 0x982f A paremated-conproxy.com A 52.52.18.181 A 52.53.65.99
52.52.18.181      80       paremated-conproxy.com     GET /voluum/[redacted] HTTP/1.1
194.58.[redacted] 80       194.58.[redacted]          GET /usa HTTP/1.1
194.58.[redacted] 80       194.58.[redacted]          GET /usa/ HTTP/1.1
192.168.204.2     53                                  Standard query 0x5421 A cdnjs.cloudflare.com
192.168.204.142   59511                               Standard query response 0x5421 A cdnjs.cloudflare.com A 104.19.196.102 A 104.19.193.102 A 104.19.192.102 A 104.19.194.102 A 104.19.195.102
104.19.196.102    80       cdnjs.cloudflare.com       GET /ajax/libs/jstimezonedetect/1.0.6/jstz.min.js HTTP/1.1
104.19.196.102    80       cdnjs.cloudflare.com       GET /ajax/libs/jquery/3.2.1/jquery.min.js HTTP/1.1
194.58.[redacted] 80       194.58.[redacted]          POST /usa/ HTTP/1.1  (application/x-www-form-urlencoded)
52.52.18.181      80       paremated-conproxy.com     GET /voluum/[redacted]??track=[redacted] HTTP/1.1
192.168.204.2     53                                  Standard query 0xd981 A 15cen.redirectvoluum.com
192.168.204.142   65116                               Standard query response 0xd981 A 15cen.redirectvoluum.com A 54.183.53.133 A 52.9.71.23
54.183.53.133     80       15cen.redirectvoluum.com   GET /redirect?target=BASE64aHR0cDovLzE5NC41OC40MC40OC9zaWdudTQucGhw&ts=[redacted]&hash=[redacted]&rm=DJ HTTP/1.1
194.58.40.48      80       194.58.40.48               GET /signu4.php HTTP/1.1
188.225.74.81     80       188.225.74.81              GET /?Mzc1NTMy&mano=VDVCwiUy6Kg2mnY1YUAhB86r6jkWBz0K2hZfU-BeNMA4RrJeWRuQz3V_1nb1kQPsig1TH6mI&pano=xX3QMvWfbRXQDp3EKv_cT6NQMVHR8UCL2Y2dmrHVefjaeFWkzrfFTF_3ozKASQSG6_dtdfJ&work=NTI0NDI4NjQ= HTTP/1.1
188.225.74.81     80       188.225.74.81              GET /?MTMwMTY1&mano=yzY1UVF9C8KyvjULXmxLOg5TW_RDZZw8R-pGVQrQ52F6km7RMdch1khKK62JQnu8tW1KY5A8Vn6v7VaSO-w&pano=xH3QMrTYbRzFFYbfKPjEUKBEMUrkWAKKwYuZharVF5uxFDL6pbf1Fx7spV6dCFmEmvZvdLYHEweh1UHASwA&shop=NDcxNTQ2MDg= HTTP…
188.225.74.81     80       188.225.74.81              GET /?NTM4MDQx&pano=xXvQMvWYbRXQD53EKv_cT6NBMVHRGUCL2YudmrHVefjafIWkzrOFTF_3ozKATgSG6_dtdfJUDV&mano=CwjkyGKgBmnY1ZUAhB86r6jkSB20KfhZfU-BeNMAkRrJeRRuQz21_1nbQkdMs1wxGL7VENjO8e&shop=MTY2MzgyODE= HTTP/1.1
192.168.204.2     53                                  Standard query 0xe54d A google.com
192.168.204.142   64091                               Standard query response 0xe54d A google.com A 172.217.5.78
192.168.204.2     53                                  Standard query 0xe792 A h62yeey62tqgshy.com
192.168.204.142   54905                               Standard query response 0xe792 A h62yeey62tqgshy.com A 46.173.213.134
46.173.213.134    443                                 49903→443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
192.168.204.142   49903                               443→49903 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
46.173.213.134    443                                 49903→443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
46.173.213.134    443                                 [TCP segment of a reassembled PDU]
192.168.204.142   49903                               443→49903 [ACK] Seq=1 Ack=7 Win=64240 Len=0
46.173.213.134    443                                 [TCP segment of a reassembled PDU]
192.168.204.142   49903                               443→49903 [ACK] Seq=1 Ack=82 Win=64240 Len=0
192.168.204.142   49903                               [TCP segment of a reassembled PDU]
46.173.213.134    443                                 [TCP segment of a reassembled PDU]
192.168.204.142   49903                               443→49903 [ACK] Seq=8 Ack=88 Win=64240 Len=0
46.173.213.134    443                                 [TCP segment of a reassembled PDU]
192.168.204.142   49903                               443→49903 [ACK] Seq=8 Ack=89 Win=64240 Len=0
```

The Ramnit payload was dropped and detonated in %Temp%. We then see the malware copy itself to a new folder in %LocalAppData% where it was then executed.

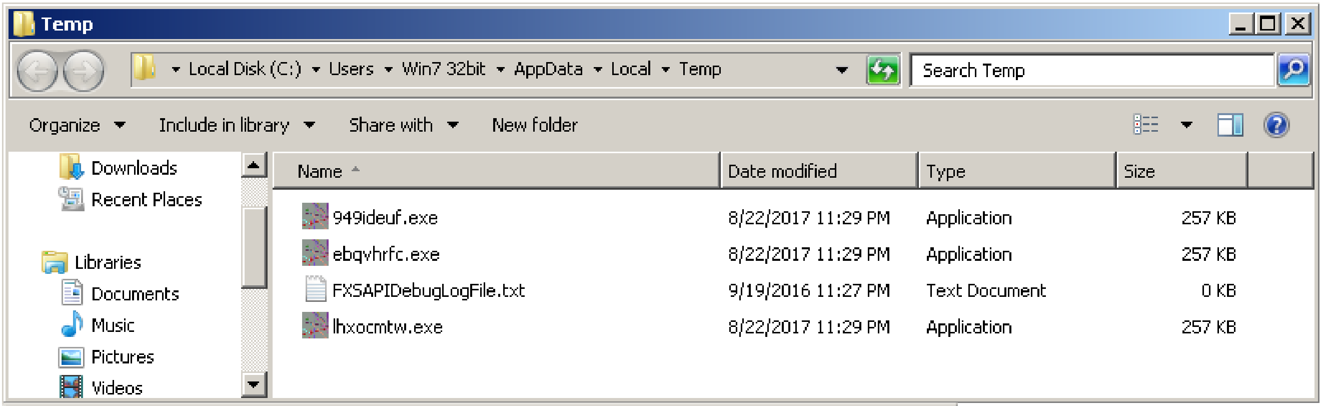


Name	Date modified	Type	Size
949ideuf.exe	8/22/2017 11:29 PM	Application	257 KB
o32.tmp	8/22/2017 11:29 PM	TMP File	2 KB
FXSAPIDebugLogFile.txt	9/19/2016 11:27 PM	Text Document	0 KB

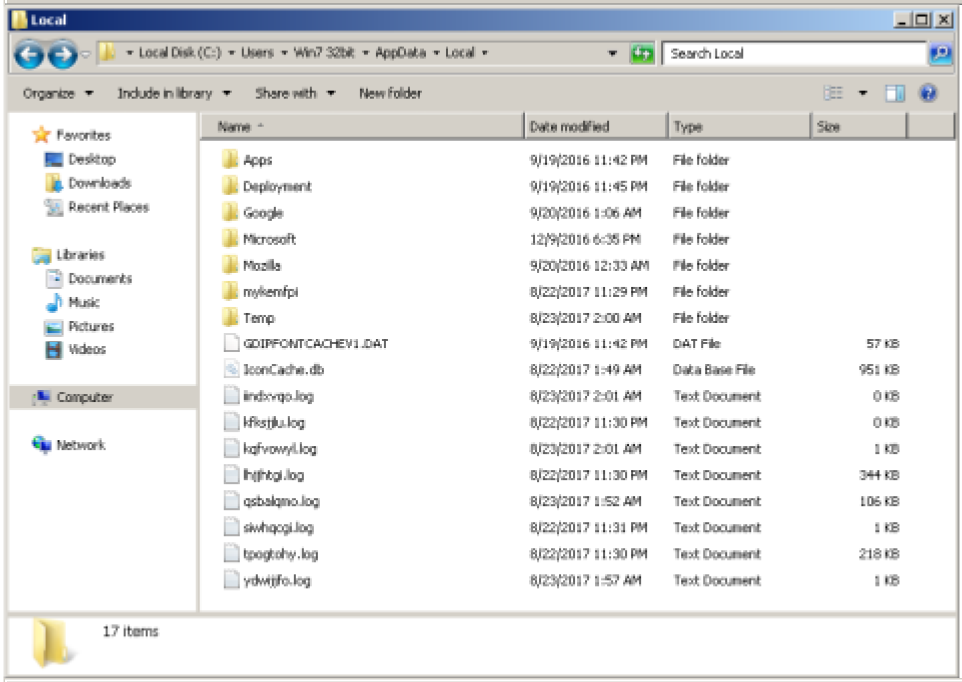
Name	Date modified	Type	Size
ufyqwfyv.exe	8/22/2017 11:29 PM	Application	257 KB

Once the file is run from %LocalAppData% we see the first DNS query for Google.com. After successfully resolving Google.com comes the DNS query for the C2 domain h62yeey62tqgshy.com (resolves to 46.173.213.134). The infected host then initiated connections to the C2 server via TCP port 443.

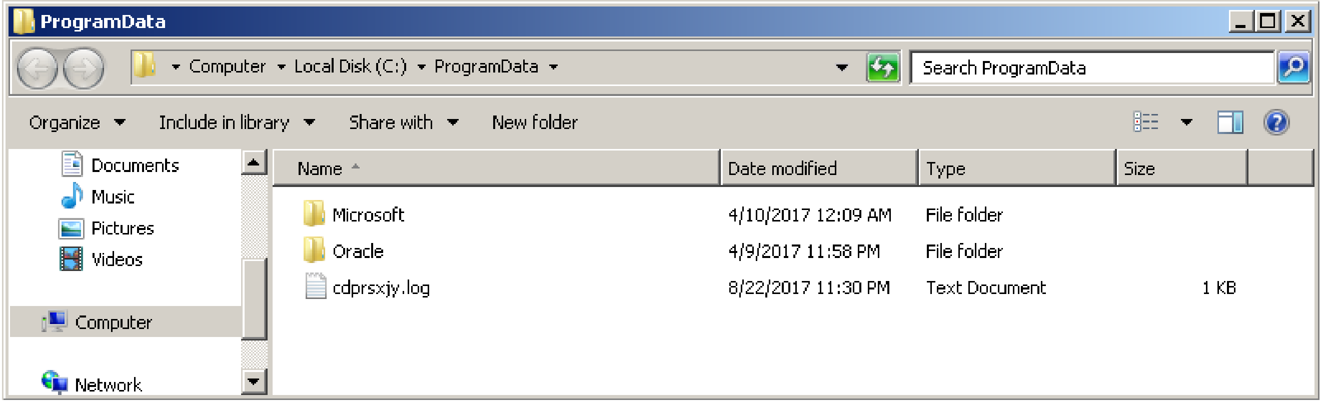
During this same time, you see two more copies of the malware being dropped back into %Temp% as well as Ramnit's .log files being created in various locations like %LocalAppData% and %ProgramData%:



Name	Date modified	Type	Size
949ideuf.exe	8/22/2017 11:29 PM	Application	257 KB
ebqvhrfc.exe	8/22/2017 11:29 PM	Application	257 KB
FXSAPIDebugLogFile.txt	9/19/2016 11:27 PM	Text Document	0 KB
lhxocmtw.exe	8/22/2017 11:29 PM	Application	257 KB

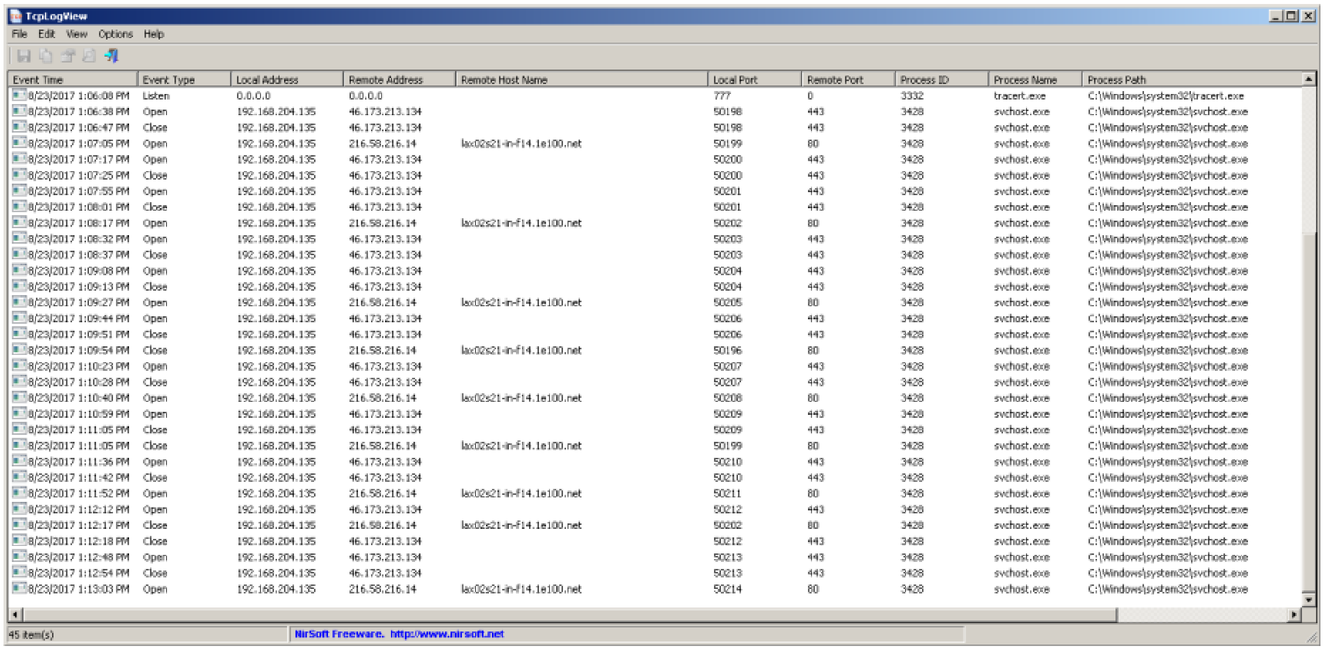


Name	Date modified	Type	Size
Apps	9/19/2016 11:42 PM	File folder	
Deployment	9/19/2016 11:45 PM	File folder	
Google	9/20/2016 1:06 AM	File folder	
Microsoft	12/9/2016 6:35 PM	File folder	
Mozilla	9/20/2016 12:33 AM	File folder	
mykemfpi	8/22/2017 11:29 PM	File folder	
Temp	8/23/2017 2:00 AM	File folder	
GDIPFONTCACHEV1.DAT	9/19/2016 11:42 PM	DAT File	57 KB
IconCache.db	8/22/2017 1:49 AM	Data Base File	951 KB
iindxvqo.log	8/23/2017 2:01 AM	Text Document	0 KB
kfksjjlu.log	8/22/2017 11:30 PM	Text Document	0 KB
kqfvowyl.log	8/23/2017 2:01 AM	Text Document	1 KB
lhjjhtgi.log	8/22/2017 11:30 PM	Text Document	344 KB
qsbalqno.log	8/23/2017 1:52 AM	Text Document	106 KB
siwhqcgi.log	8/22/2017 11:31 PM	Text Document	1 KB
tpogtohy.log	8/22/2017 11:30 PM	Text Document	218 KB
ydwijjfo.log	8/23/2017 1:57 AM	Text Document	1 KB



Name	Date modified	Type	Size
Microsoft	4/10/2017 12:09 AM	File folder	
Oracle	4/9/2017 11:58 PM	File folder	
cdprsxjy.log	8/22/2017 11:30 PM	Text Document	1 KB

This same beaconing pattern with Google.com and the C2 repeats itself over and over again:



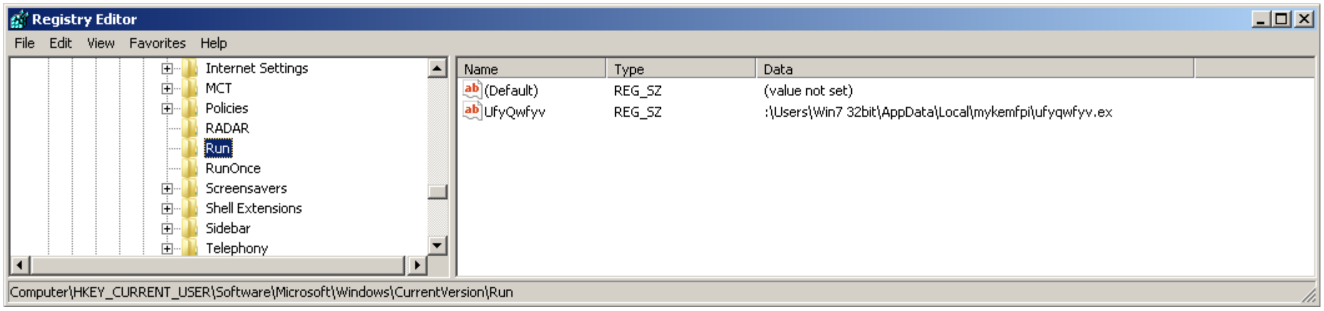
Event Time	Event Type	Local Address	Remote Address	Remote Host Name	Local Port	Remote Port	Process ID	Process Name	Process Path
8/23/2017 1:06:08 PM	Listen	0.0.0.0	0.0.0.0		777	0	3332	tracert.exe	C:\Windows\system32\tracert.exe
8/23/2017 1:06:38 PM	Open	192.168.204.135	46.173.213.134		50198	443	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:06:47 PM	Close	192.168.204.135	46.173.213.134		50198	443	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:07:05 PM	Open	192.168.204.135	216.58.216.14	lax02s21-in-f14.1e100.net	50199	80	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:07:17 PM	Open	192.168.204.135	46.173.213.134		50200	443	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:07:25 PM	Close	192.168.204.135	46.173.213.134		50200	443	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:07:55 PM	Open	192.168.204.135	46.173.213.134		50201	443	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:08:01 PM	Close	192.168.204.135	46.173.213.134		50201	443	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:08:17 PM	Open	192.168.204.135	216.58.216.14	lax02s21-in-f14.1e100.net	50202	80	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:08:32 PM	Open	192.168.204.135	46.173.213.134		50203	443	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:08:37 PM	Close	192.168.204.135	46.173.213.134		50203	443	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:09:08 PM	Open	192.168.204.135	46.173.213.134		50204	443	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:09:13 PM	Close	192.168.204.135	46.173.213.134		50204	443	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:09:27 PM	Open	192.168.204.135	216.58.216.14	lax02s21-in-f14.1e100.net	50205	80	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:09:44 PM	Open	192.168.204.135	46.173.213.134		50206	443	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:09:51 PM	Close	192.168.204.135	46.173.213.134		50206	443	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:09:54 PM	Close	192.168.204.135	216.58.216.14	lax02s21-in-f14.1e100.net	50196	80	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:10:23 PM	Open	192.168.204.135	46.173.213.134		50207	443	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:10:28 PM	Close	192.168.204.135	46.173.213.134		50207	443	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:10:40 PM	Open	192.168.204.135	216.58.216.14	lax02s21-in-f14.1e100.net	50208	80	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:10:59 PM	Open	192.168.204.135	46.173.213.134		50209	443	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:11:05 PM	Close	192.168.204.135	46.173.213.134		50209	443	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:11:05 PM	Close	192.168.204.135	216.58.216.14	lax02s21-in-f14.1e100.net	50199	80	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:11:36 PM	Open	192.168.204.135	46.173.213.134		50210	443	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:11:42 PM	Close	192.168.204.135	46.173.213.134		50210	443	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:11:52 PM	Open	192.168.204.135	216.58.216.14	lax02s21-in-f14.1e100.net	50211	80	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:12:12 PM	Open	192.168.204.135	46.173.213.134		50212	443	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:12:17 PM	Close	192.168.204.135	216.58.216.14	lax02s21-in-f14.1e100.net	50202	80	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:12:18 PM	Close	192.168.204.135	46.173.213.134		50212	443	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:12:48 PM	Open	192.168.204.135	46.173.213.134		50213	443	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:12:54 PM	Close	192.168.204.135	46.173.213.134		50213	443	3428	svchost.exe	C:\Windows\system32\svchost.exe
8/23/2017 1:13:03 PM	Open	192.168.204.135	216.58.216.14	lax02s21-in-f14.1e100.net	50214	80	3428	svchost.exe	C:\Windows\system32\svchost.exe

45 item(s)

NirSoft Freeware. http://www.nirsoft.net

Shows socket information and includes the name and ID of the process responsible for the connection

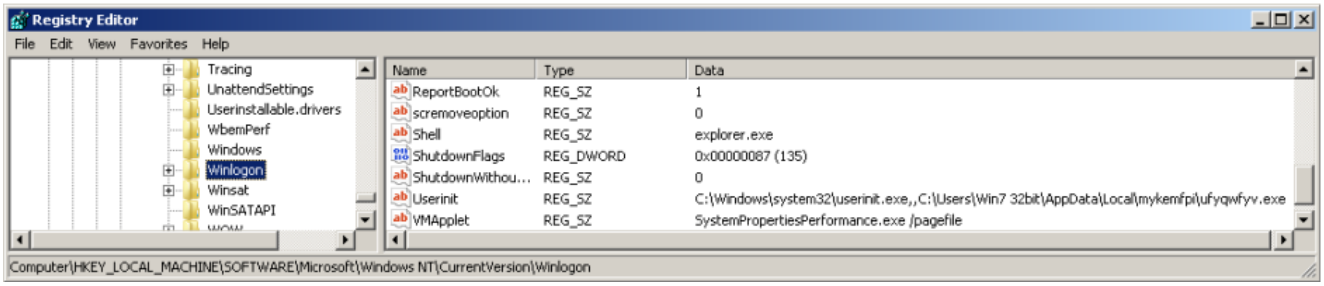
We can also see that the malware creates various methods of persistence on the system, including creating a file in Startup and setting some values in the registry:



Name	Type	Data
(Default)	REG_SZ	(value not set)
UfyQwfyv	REG_SZ	:\Users\Win7 32bit\AppData\Local\mykemfpi\ufyqwfyv.ex

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

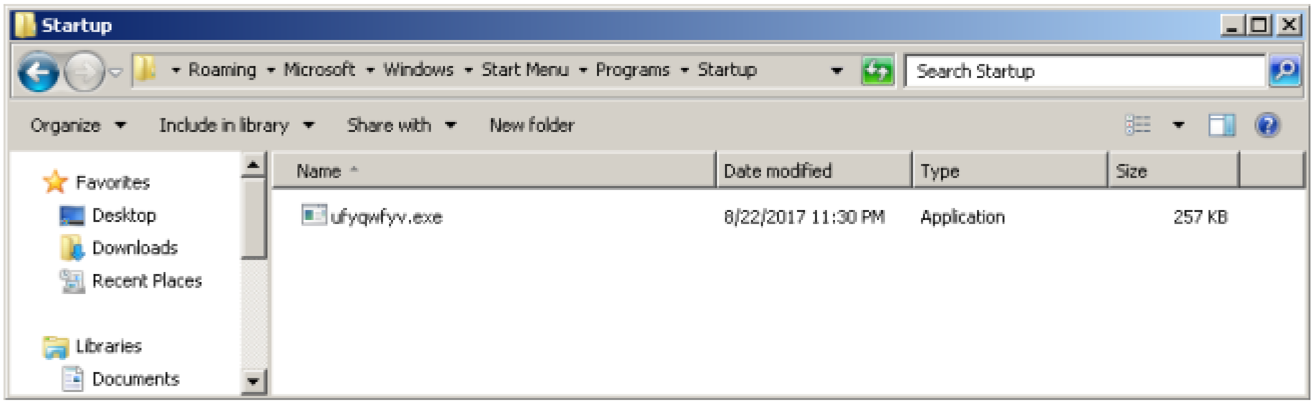
SETVAL; Path: HKCUSOFTWAREMICROSOFTWINDOWSCURRENTVERSIONRUN



Name	Type	Data
ReportBootOk	REG_SZ	1
scremoveoption	REG_SZ	0
Shell	REG_SZ	explorer.exe
ShutdownFlags	REG_DWORD	0x00000087 (135)
ShutdownWithou...	REG_SZ	0
Userinit	REG_SZ	C:\Windows\system32\userinit.exe,,C:\Users\Win7 32bit\AppData\Local\mykemfpi\ufyqwfyv.exe
VMApplet	REG_SZ	SystemPropertiesPerformance.exe /pagefile

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

SETVAL; Path: HKLMSOFTWAREMICROSOFTWINDOWS NTCURRENTVERSIONWINLOGON



Name	Date modified	Type	Size
ufyqwfyv.exe	8/22/2017 11:30 PM	Application	257 KB

Malware is set to run at startup

IOCs

Pre-infection:
194.58.40.48 – IP literal hostname used by the Seamless campaign
188.225.74.81 – IP literal hostname used by RIG EK

Post-infection:
DNS queries for h62yeey62tqgshy.com
Connections to 46.173.213.134 via TCP port 443

Hashes

SHA256: ff1184382121f67d04aafb09879bddbd449b1e95b2ca50933fce1574ffb84b50
File name: RigEK landing page from 188.225.74.81.txt

SHA256: cbf7dfc2226e592149ef45539c9a4f109c4e66533fe061037241fb88c245ce57
File name: RigEK Flash exploit from 188.225.74.81.swf

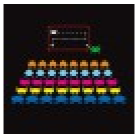
SHA256: 62687447bd28623e2a584e4c0e761b5ed365bfe057621523a29025d4210fcada
File name: o32.tmp

SHA256: 8995e321efc5cedbc979e43d9f7c84440b346573dbeb71b7a3c941052ad87428
File name: 949ideuf.exe
Hybrid-Analysis Report

Downloads

Seamless RigEK Ramnit Malicious Artifacts 082217.zip
Password is “infected”

Until next time!



Published by malwarebreakdown

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