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

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)

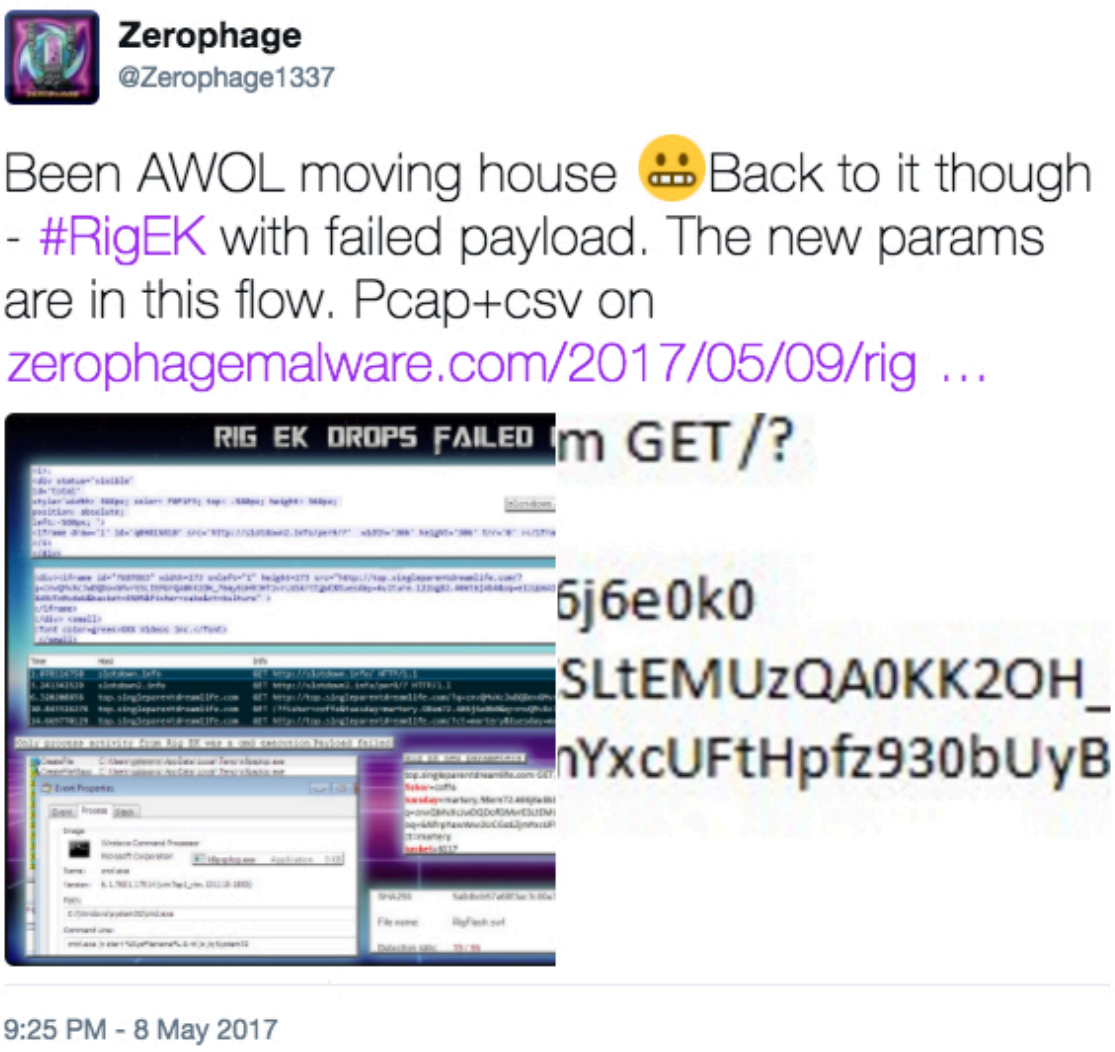
> - 2017-05-09-Rig-EK-sends-Bunitu.pcap (554,307 bytes)

- 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)

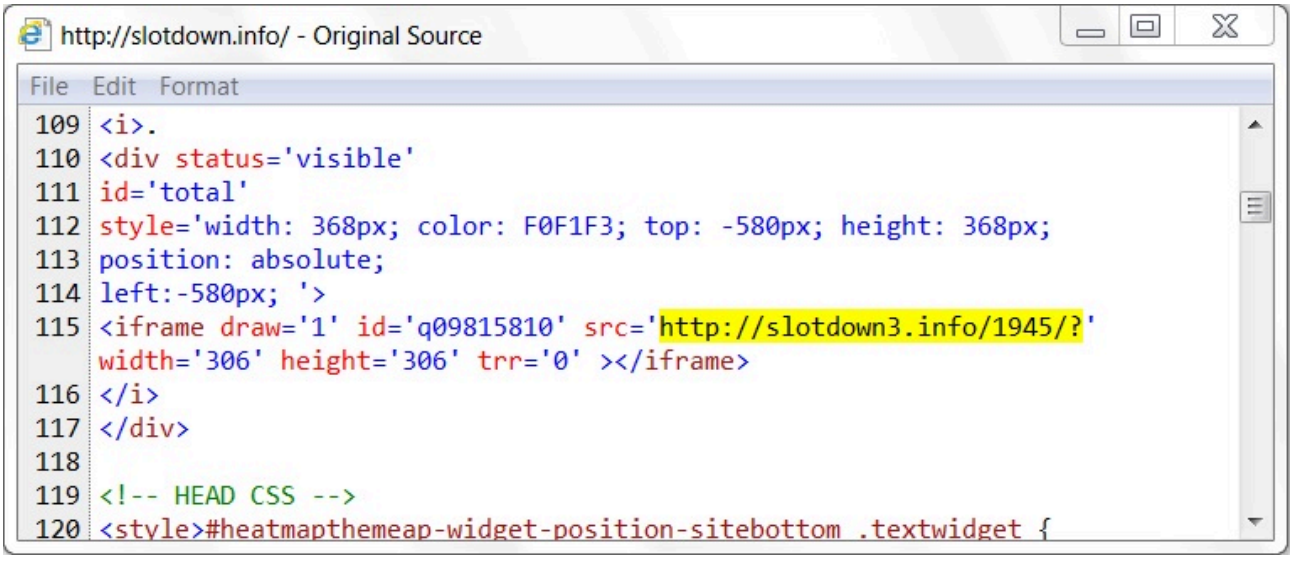
NOTES:

- I generated traffic baseed 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.

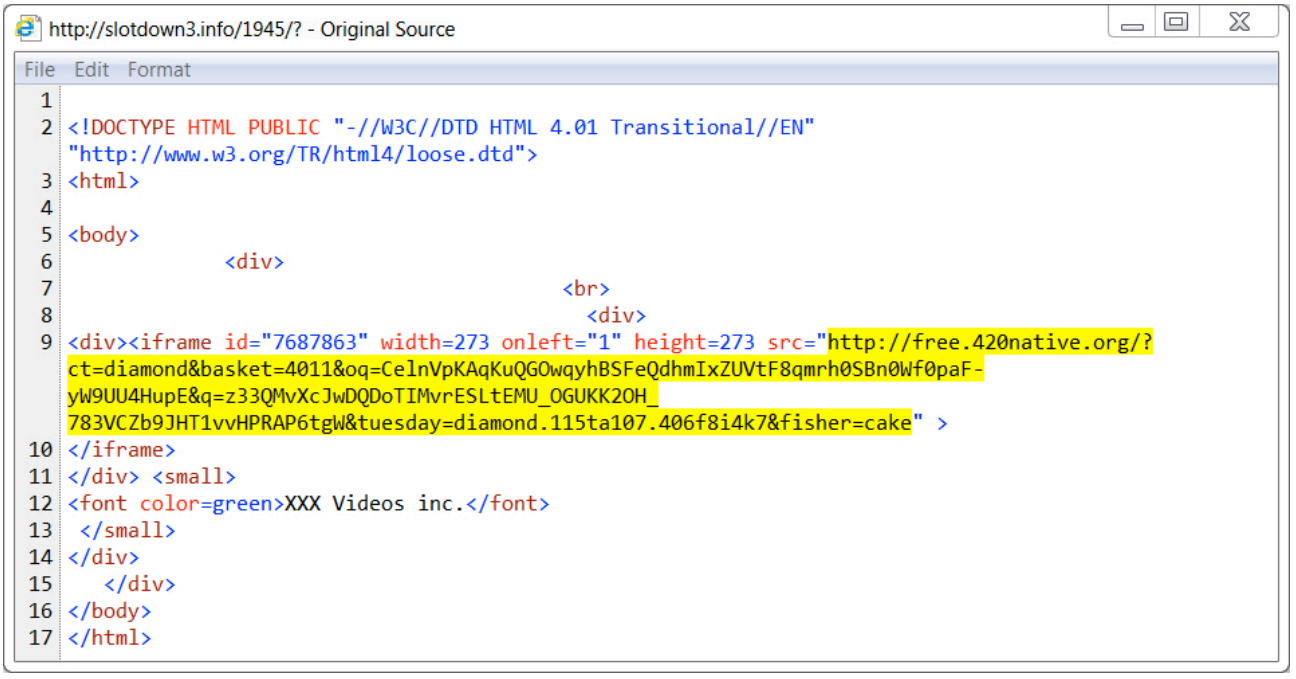


Shown above: Tweet by @Zerophage1337 about this activity.

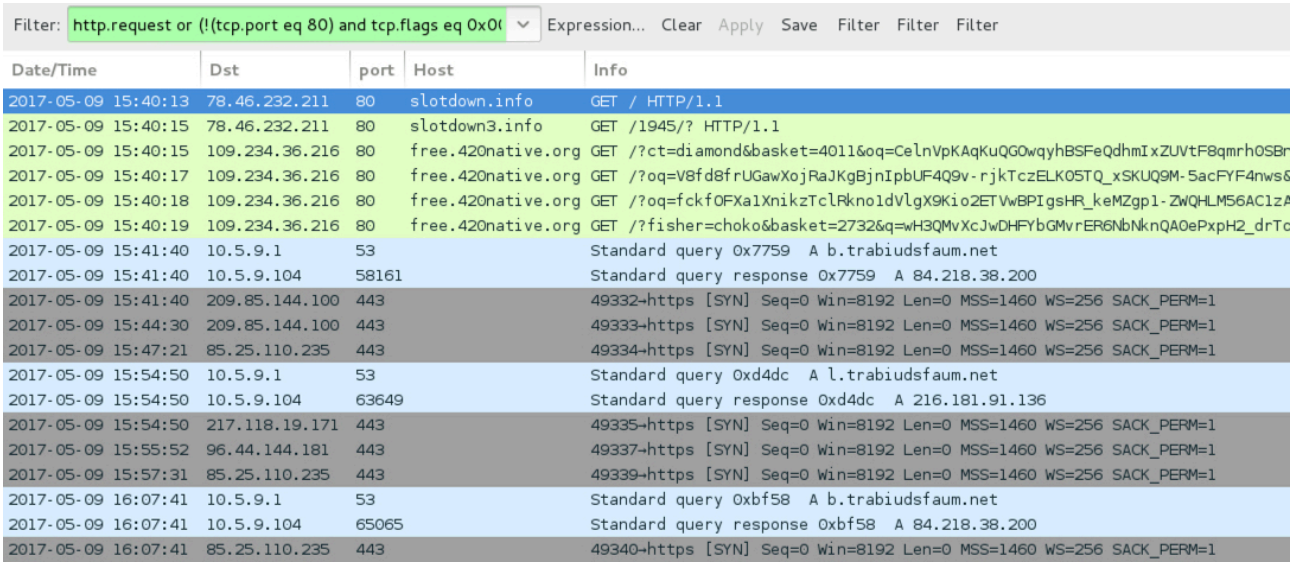
TRAFFIC



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



Shown above: Script leading to Rig EK landing page.



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:

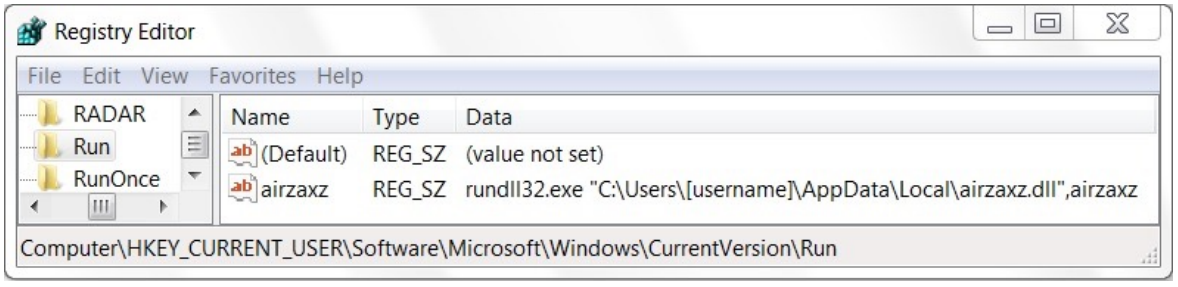
- SHA256 hash: 81549d2ea47649a750bd4fc6e7be0b971c3fc6711a31af2f77ba437218ff63d1
  File size: 16,500 bytes

RIG EK PAYLOAD (BUNITU):

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

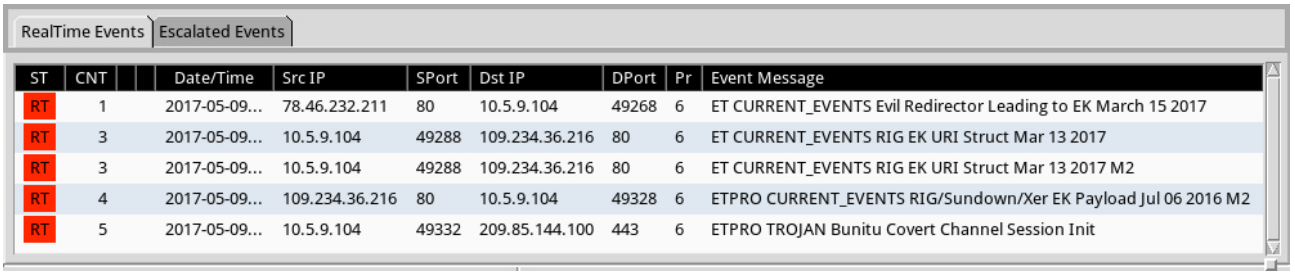
ARTIFACT FROM THE INFECTED HOST:

- 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

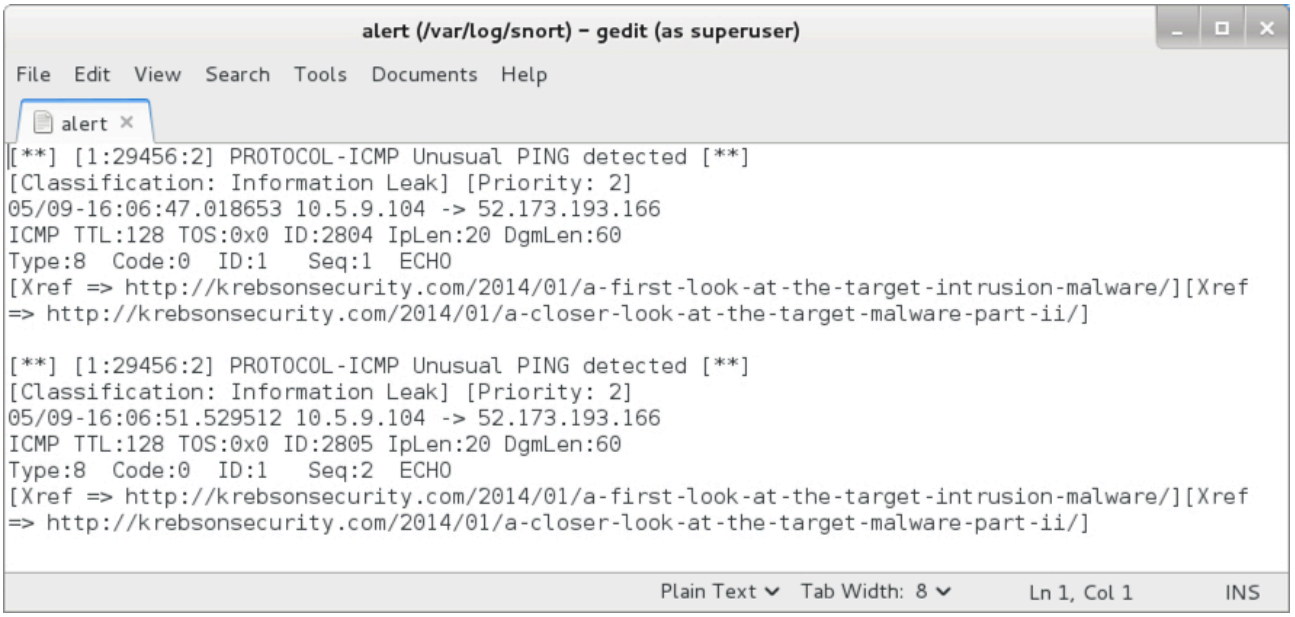


Shown above: Some alerts on the traffic from the Emerging Threats and ETPRO rulesets using Sguil and tcpreplay on Security Onion.

RealTime Events | Escalated Events

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.



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.
