Malware-Traffic-Analysis.net - 2017-04-25 - "Good Man" campaign Rig EK sends Latentbot

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:

- 2017-04-25-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)

- Z2017-04-25-Good-Man-campaign-Rig-EK-and-Latentbot-malware-and-artifacts.zip 319.6 kB (319,550 bytes)

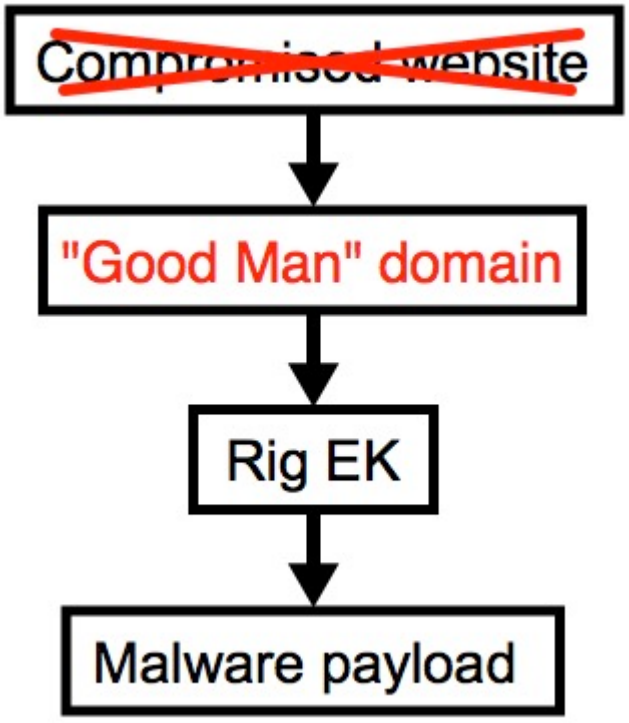
> - 2017-04-25-Goodma-campaign-Rig-EK-payload-Latentbot.exe (312,832 bytes)
> - 2017-04-25-Rig-EK-artifact-o32.tmp.txt (1,141 bytes)
> - 2017-04-25-Rig-EK-flash-exploit.swf (16,428 bytes)
> - 2017-04-25-Rig-EK-landing-page.txt (117,853 bytes)
> - 2017-04-25-page-from-hurtmehard_net-with-injected-script-for-Rig-EK-landing-page.txt (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.
- Background on this campaign was posted on 2017-03-10 on the Malware Breakdown site in an article titled "Finding A 'Good Man'" (Internet Archive link).

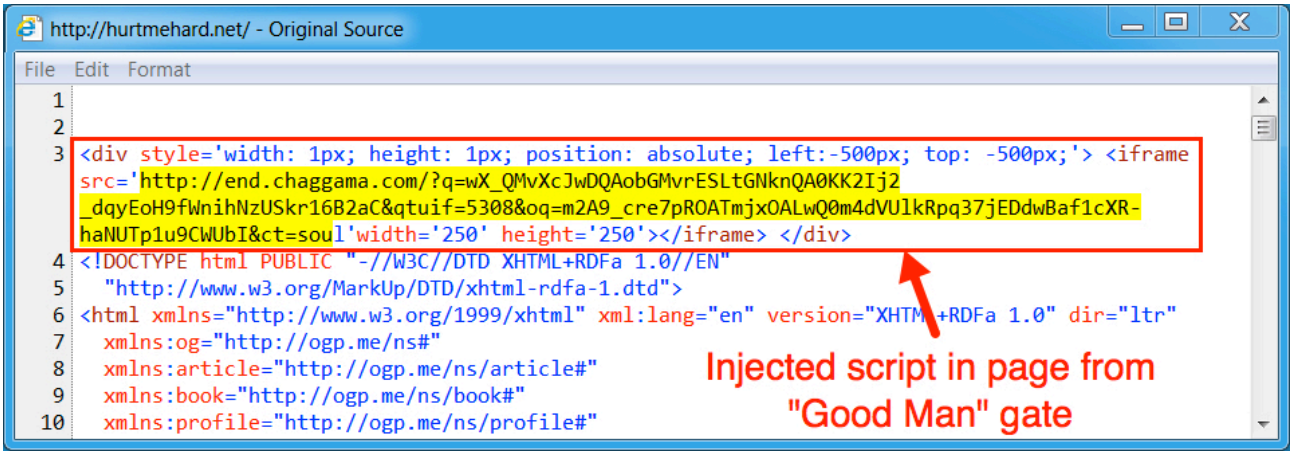
BACKGROUND ON LATENTBOT:

- Although post-infection traffic triggers alerts for the GrayBird Trojan on the EmergingThreats ruleset, more recent variants have been dubbed "Latentbot."
- FireEye published an analysis of Latentbot named "LATENTBOT: Trace Me If You Can."

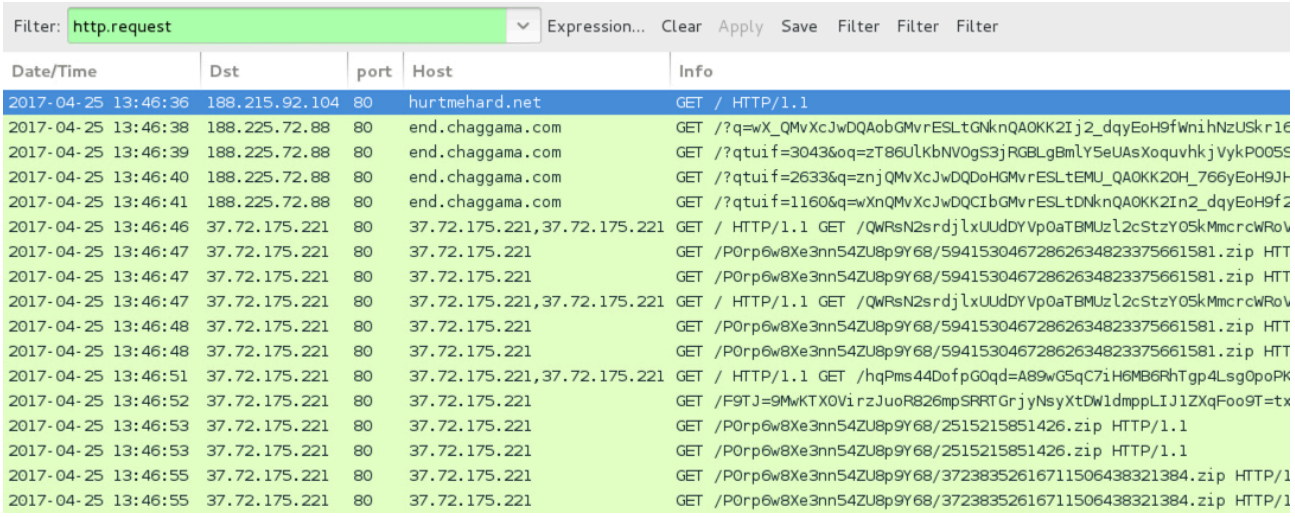


Shown above: Flowchart for this infection traffic.

TRAFFIC



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



Filter: http.request — Expression... Clear Apply Save Filter Filter Filter

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_QMvXcJwDQAobGMvrESLtGNknQA0KK2Ij2_dqyEoH9fWnihNzUSkr16
2017-04-25 13:46:39	188.225.72.88	80	end.chaggama.com	GET /?qtuif=3043&oq=zT86UlKbNVOgS3jRGBLgBmlY5eUAsXoquvhkjVykPO05S
2017-04-25 13:46:40	188.225.72.88	80	end.chaggama.com	GET /?qtuif=2633&q=znjQMvXcJwDQDoHGMvrESLtEMU_QA0KK2OH_766yEoH9JH
2017-04-25 13:46:41	188.225.72.88	80	end.chaggama.com	GET /?qtuif=1160&q=wXnQMvXcJwDQCIbGMvrESLtDNknQA0KK2In2_dqyEoH9f2
2017-04-25 13:46:46	37.72.175.221	80	37.72.175.221,37.72.175.221	GET / HTTP/1.1 GET /QWRsN2srdjlxUUdDYVpOaTBMUzl2cStzY05kMmcrcWRoV
2017-04-25 13:46:47	37.72.175.221	80	37.72.175.221	GET /POrp6w8Xe3nn54ZU8p9Y68/59415304672862634823375661581.zip HTT
2017-04-25 13:46:47	37.72.175.221	80	37.72.175.221	GET /POrp6w8Xe3nn54ZU8p9Y68/59415304672862634823375661581.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 /QWRsN2srdjlxUUdDYVpOaTBMUzl2cStzY05kMmcrcWRoV
2017-04-25 13:46:48	37.72.175.221	80	37.72.175.221	GET /POrp6w8Xe3nn54ZU8p9Y68/59415304672862634823375661581.zip HTT
2017-04-25 13:46:48	37.72.175.221	80	37.72.175.221	GET /POrp6w8Xe3nn54ZU8p9Y68/59415304672862634823375661581.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 /hqPms44DofpGOqd=A89wG5qC7iH6MB6RhTgp4LsgOpoPK
2017-04-25 13:46:52	37.72.175.221	80	37.72.175.221	GET /F9TJ=9MwKTXOVirzJuoR826mpSRRTGrjyNsyXtDW1dmppLIJ1ZXqFoo9T=tx
2017-04-25 13:46:53	37.72.175.221	80	37.72.175.221	GET /POrp6w8Xe3nn54ZU8p9Y68/2515215851426.zip HTTP/1.1
2017-04-25 13:46:53	37.72.175.221	80	37.72.175.221	GET /POrp6w8Xe3nn54ZU8p9Y68/2515215851426.zip HTTP/1.1
2017-04-25 13:46:55	37.72.175.221	80	37.72.175.221	GET /POrp6w8Xe3nn54ZU8p9Y68/37238352616711506438321384.zip HTTP/1
2017-04-25 13:46:55	37.72.175.221	80	37.72.175.221	GET /POrp6w8Xe3nn54ZU8p9Y68/37238352616711506438321384.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

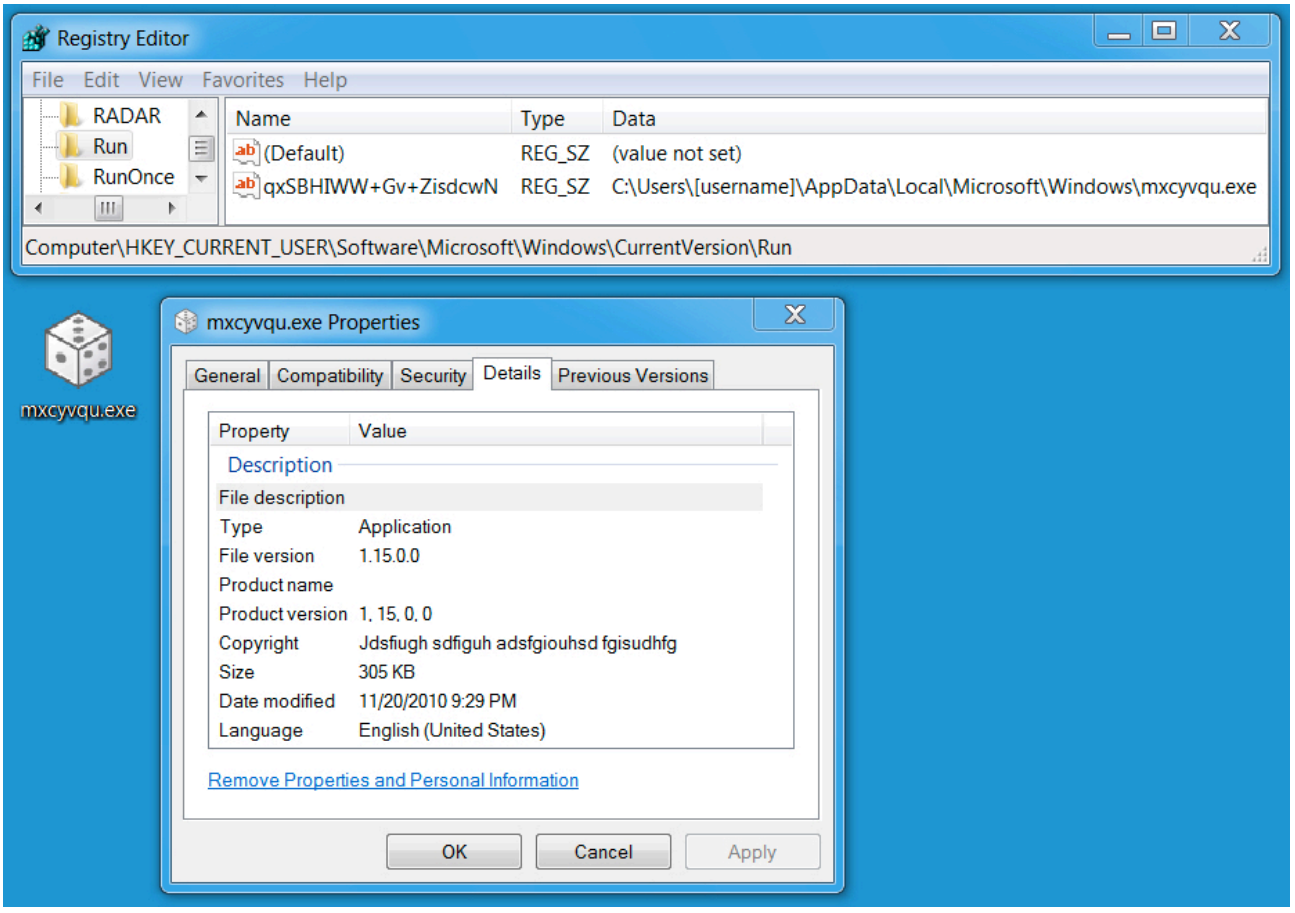
FLASH EXPLOIT:

- SHA256 hash: 9d56d491f0fca9a16daeb0ce5ef6ba96206fea93b5b12f42c442aa10a0d487ea
  File size: 16,428 bytes
  File description: Rig EK flash exploit seen on 2017-04-25

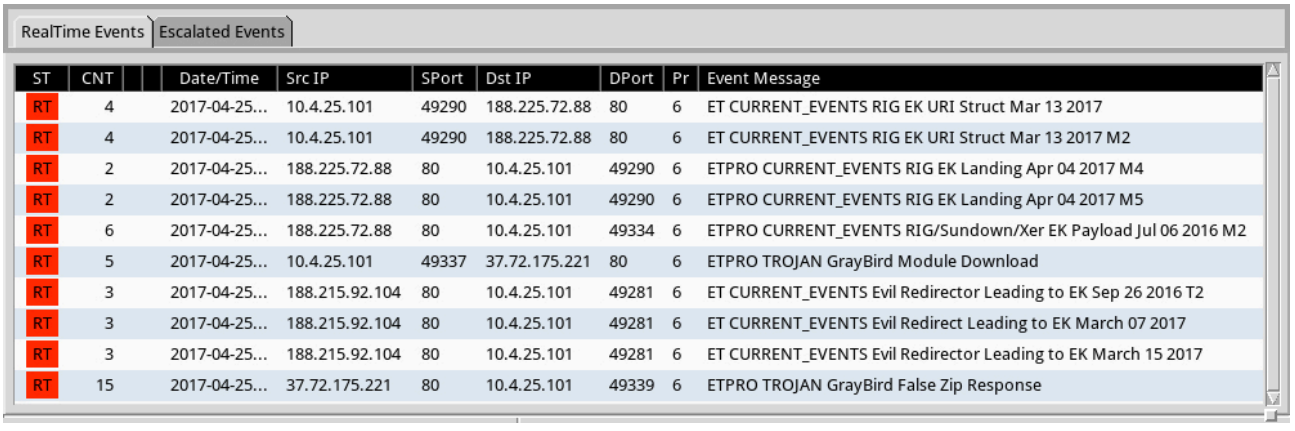
PAYLOAD (LATENTBOT):

- SHA256 hash: 092fd4caf46ec36e07fdc9c8b156ce05cda0fb2abd7c49ba8dddfe8ac6cdbb67
  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

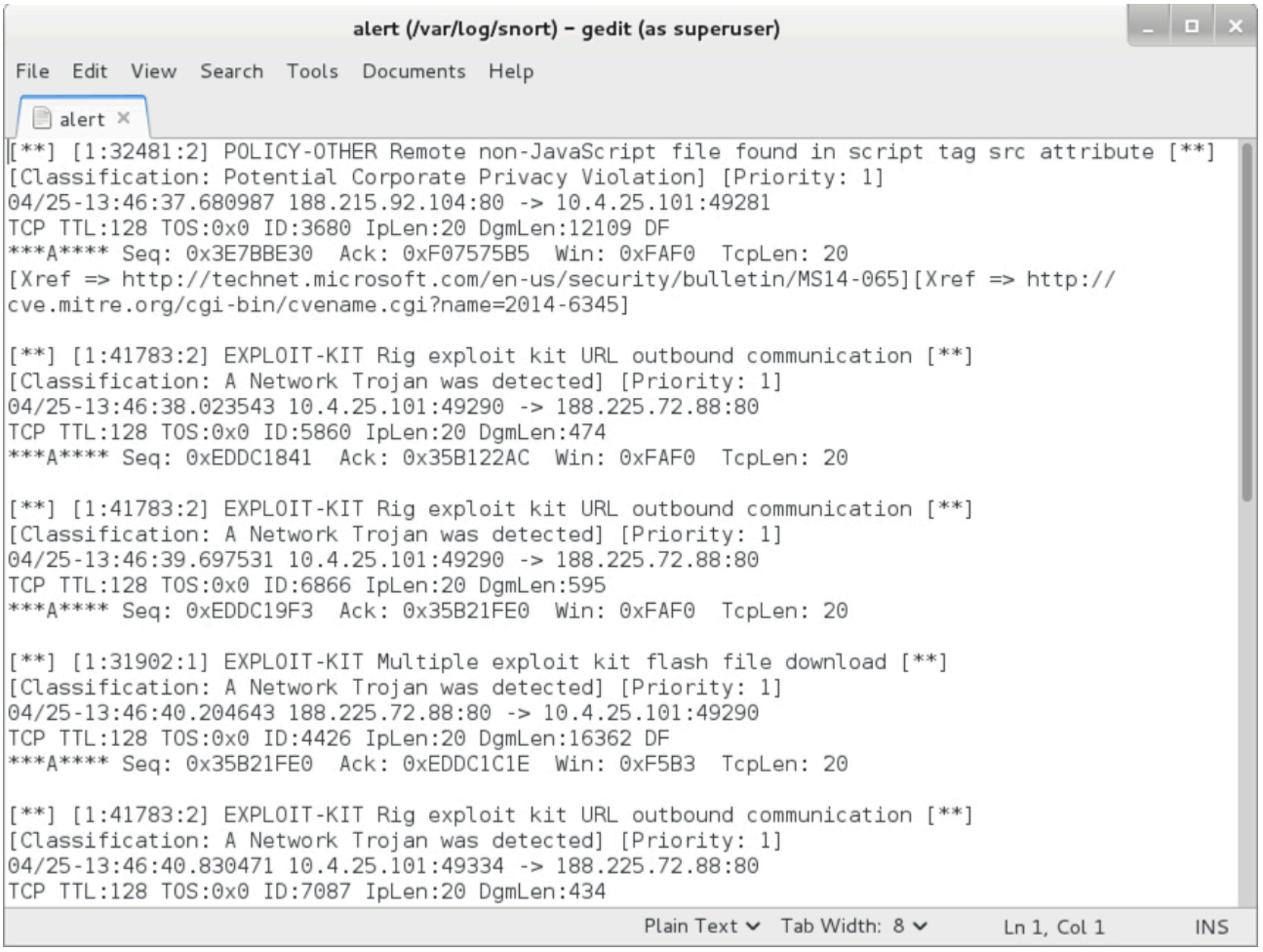


Shown above: Latentbot malware made persistent on the infected Windows host.



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.



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

Click here to return to the main page.
