2016-05-09 - PSEUDO-DARKLEECH ANGLER EK FROM 185.118.66.154 SENDS BEDEP/CRYPTXXX

malware-traffic-analysis.net/2016/05/09/index.html

ASSOCIATED FILES:

ZIP archive of the pcaps: 2016-05-09-pseudo-Darkleech-Angler-EK-pcaps.zip 4.4 MB (4,390,349 bytes)

- 2016-05-09-pseudo-Darkleech-Angler-EK-on-a-VM.pcap (780,111 bytes)
- 2016-05-09-pseudo-Darkleech-Angler-EK-on-a-normal-host-sends-Bedep-CryptXXX.pcap (4,114,289 bytes)

ZIP archive of the malware and artifacts: 2016-05-09-pseudo-Darkleech-Angler-EK-malware-and-artifacts.zip 660.8 kB (660,816 bytes)

- 2016-05-09-CryptXXX-decrypt-instructions.bmp (2,023,254 bytes)
- 2016-05-09-CryptXXX-decrypt-instructions.html (14,193 bytes)
- 2016-05-09-CryptXXX-decrypt-instructions.txt (1,755 bytes)
- 2016-05-09-CryptXXX-ransomware.dll (266,240 bytes)
- 2016-05-09-click-fraud-malware.dll (910,496 bytes)
- 2016-05-09-page-from-justmyvegas.com-with-pseudo-Darkleech-script.txt (16,848 bytes)
- 2016-05-09-pseudo-Darkleech-Angler-EK-flash-exploit.swf (66,870 bytes)
- 2016-05-09-pseudo-Darkleech-Angler-EK-landing-page.txt (169,412 bytes)

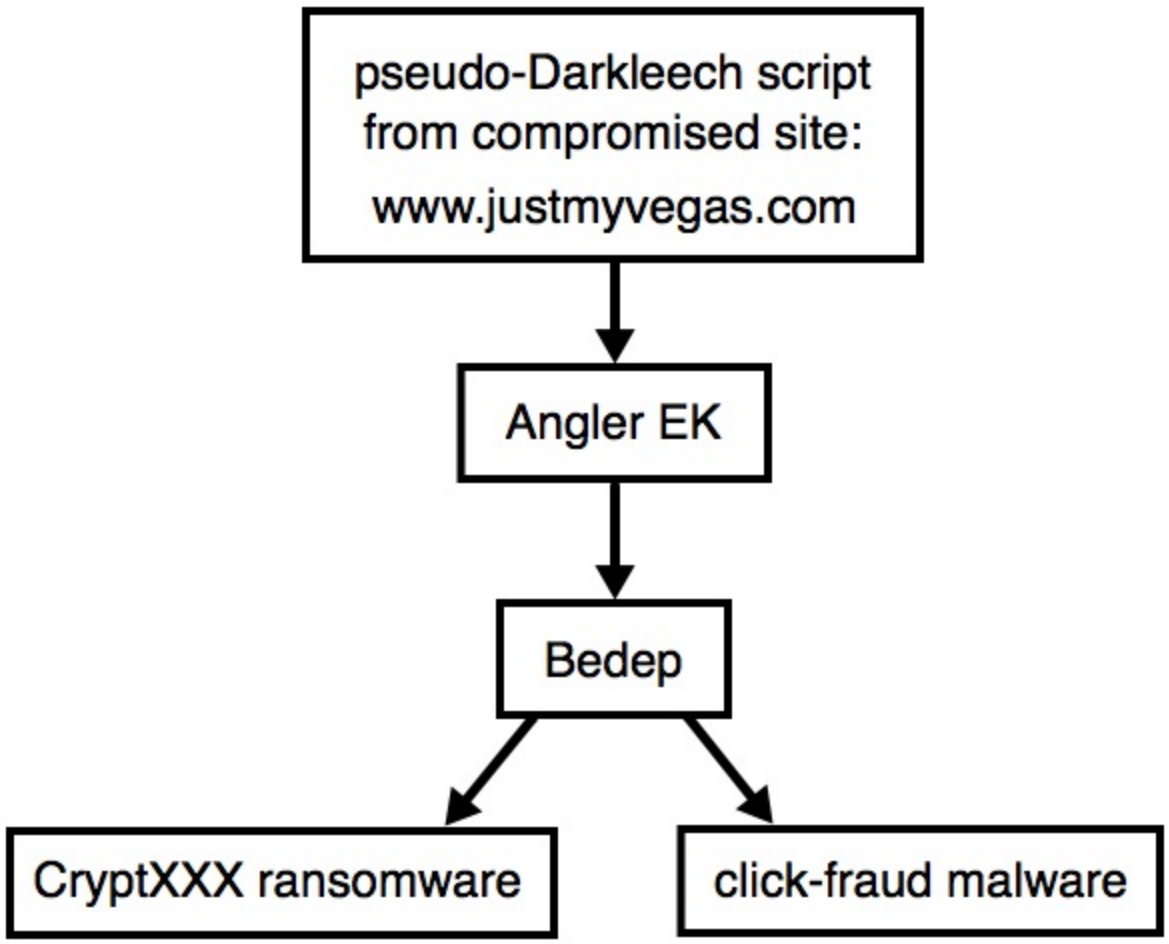
NOTES:

- On Friday 2016-04-29, I saw ***svchost.exe*** (actually: rundll32.exe) in the same folder as the CryptXXX ransomware. It was used to run the CryptXXX .dll file.
- By Monday 2016-05-02, things were back to normal, with just the CryptXXX .dll file by itself in the folder.
- A week later (Monday 2016-05-09), I see ***svchost.exe*** again, dropped in the same folder as the CryptXXX .dll file.

- Today's CryptXXX behavior is slightly different than before, and the decryption instructions are formatted a little differently.

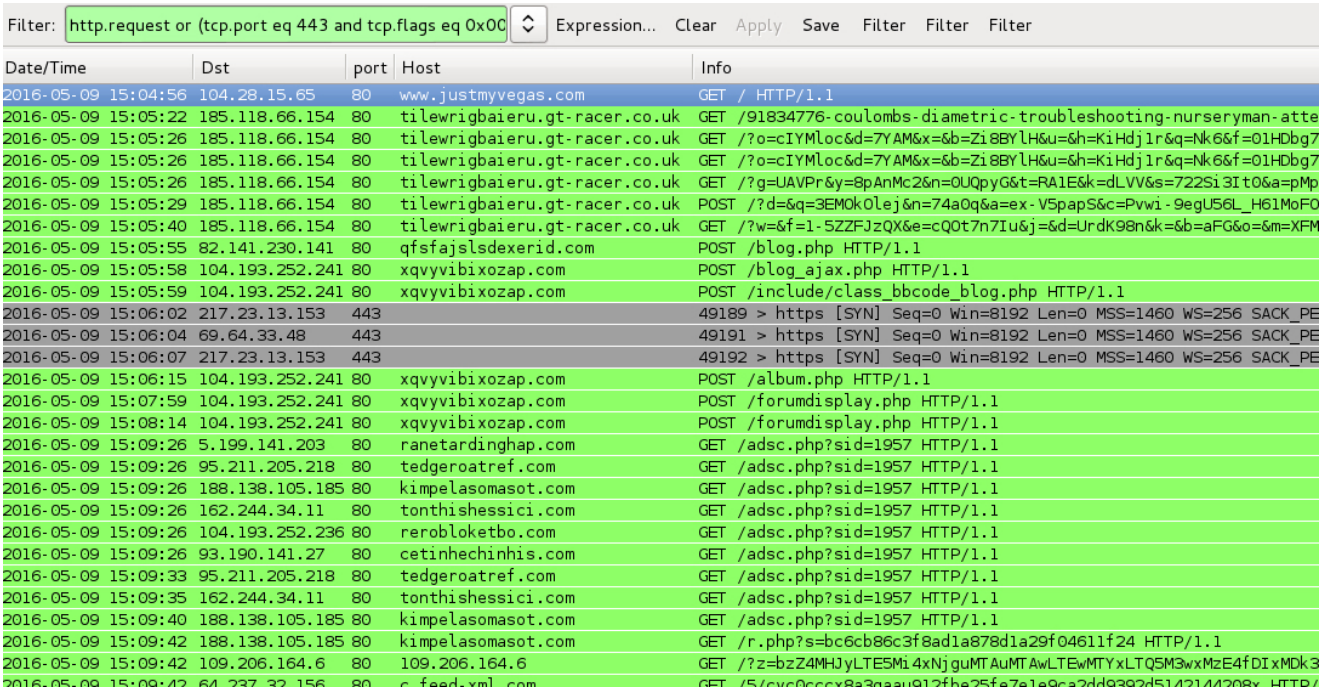
- Today's Click-fraud malware: C:\ProgramData\{9A88E103-A20A-4EA5-8636-C73B709A5BF8}\d3d10.dll
- Today's CryptXXX ransomware: C:\Users\[username]\AppData\Local\Temp\{98D13E48-E0E4-429B-9E7B-633FD7689461}\api-ms-win-system-framebuf-l1-1-0.dll

- Background on the pseudo-Darkleech campaign is available here.
- Proofpoint's blog on Angler EK spreading CryptXXX can be found here.
- An ISC diary I wrote about pseudo-Darkleech causing Angler EK/Bedep/CryptXXX infections is located here.



Shown above: Chain of events for today's infection.

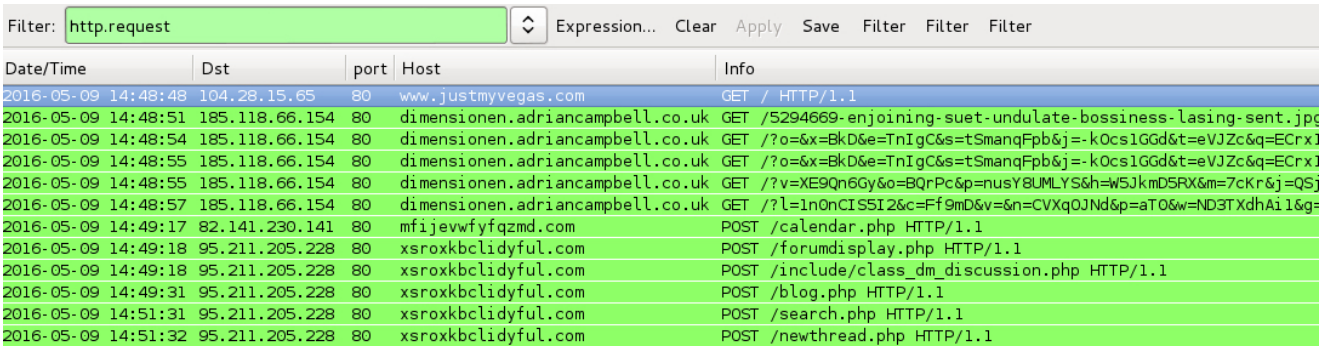
TRAFFIC



Filter: http.request or (tcp.port eq 443 and tcp.flags eq 0x00

Date/Time	Dst	port	Host	Info
2016-05-09 15:04:56	104.28.15.65	80	www.justmyvegas.com	GET / HTTP/1.1
2016-05-09 15:05:22	185.118.66.154	80	tilewrigbaieru.gt-racer.co.uk	GET /91834776-coulombs-diametric-troubleshooting-nurseryman-atte
2016-05-09 15:05:26	185.118.66.154	80	tilewrigbaieru.gt-racer.co.uk	GET /?o=cIYMloc&d=7YAM&x=&b=Zi8BYlH&u=&h=KiHdj1r&q=Nk6&f=01HDbg7
2016-05-09 15:05:26	185.118.66.154	80	tilewrigbaieru.gt-racer.co.uk	GET /?o=cIYMloc&d=7YAM&x=&b=Zi8BYlH&u=&h=KiHdj1r&q=Nk6&f=01HDbg7
2016-05-09 15:05:26	185.118.66.154	80	tilewrigbaieru.gt-racer.co.uk	GET /?g=UAVPr&y=8pAnMc2&n=0UQpyG&t=RA1E&k=dLVV&s=722Si3It0&a=pMp
2016-05-09 15:05:29	185.118.66.154	80	tilewrigbaieru.gt-racer.co.uk	POST /?d=&q=3EMOkOlej&n=74a0q&a=ex-V5papS&c=Pvwi-9egU56L_H61MoFO
2016-05-09 15:05:40	185.118.66.154	80	tilewrigbaieru.gt-racer.co.uk	GET /?w=&f=1-5ZZFJzQX&e=cQOt7n7Iu&j=&d=UrdK98n&k=&b=aFG&o=&m=XFM
2016-05-09 15:05:55	82.141.230.141	80	qfsfajslsdexerid.com	POST /blog.php HTTP/1.1
2016-05-09 15:05:58	104.193.252.241	80	xqvyvibixozap.com	POST /blog_ajax.php HTTP/1.1
2016-05-09 15:05:59	104.193.252.241	80	xqvyvibixozap.com	POST /include/class_bbcode_blog.php HTTP/1.1
2016-05-09 15:06:02	217.23.13.153	443		49189 > https [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PE
2016-05-09 15:06:04	69.64.33.48	443		49191 > https [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PE
2016-05-09 15:06:07	217.23.13.153	443		49192 > https [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PE
2016-05-09 15:06:15	104.193.252.241	80	xqvyvibixozap.com	POST /album.php HTTP/1.1
2016-05-09 15:07:59	104.193.252.241	80	xqvyvibixozap.com	POST /forumdisplay.php HTTP/1.1
2016-05-09 15:08:14	104.193.252.241	80	xqvyvibixozap.com	POST /forumdisplay.php HTTP/1.1
2016-05-09 15:09:26	5.199.141.203	80	ranetardinghap.com	GET /adsc.php?sid=1957 HTTP/1.1
2016-05-09 15:09:26	95.211.205.218	80	tedgeroatref.com	GET /adsc.php?sid=1957 HTTP/1.1
2016-05-09 15:09:26	188.138.105.185	80	kimpelasomasot.com	GET /adsc.php?sid=1957 HTTP/1.1
2016-05-09 15:09:26	162.244.34.11	80	tonthishessici.com	GET /adsc.php?sid=1957 HTTP/1.1
2016-05-09 15:09:26	104.193.252.236	80	rerobloketbo.com	GET /adsc.php?sid=1957 HTTP/1.1
2016-05-09 15:09:26	93.190.141.27	80	cetinhechinhis.com	GET /adsc.php?sid=1957 HTTP/1.1
2016-05-09 15:09:33	95.211.205.218	80	tedgeroatref.com	GET /adsc.php?sid=1957 HTTP/1.1
2016-05-09 15:09:35	162.244.34.11	80	tonthishessici.com	GET /adsc.php?sid=1957 HTTP/1.1
2016-05-09 15:09:40	188.138.105.185	80	kimpelasomasot.com	GET /adsc.php?sid=1957 HTTP/1.1
2016-05-09 15:09:42	188.138.105.185	80	kimpelasomasot.com	GET /r.php?s=bc6cb86c3f8ad1a878d1a29f04611f24 HTTP/1.1
2016-05-09 15:09:42	109.206.164.6	80	109.206.164.6	GET /?z=bzZ4MHJyLTE5Mi4xNjguMTAuMTAwLTEwMTYxLTQ5M3wxMzE4fDIxMDk3
2016-05-09 15:09:42	64.237.32.156	80	c.feed.xml.com	GET /5/cyc0cccx8a3qeau912fbe25fe7e1e9ca2dd9392d5142144208x HTTP/

Shown above: Pcap of the traffic on a normal host filtered in Wireshark. ***http.request or (tcp.port eq 443 and tcp.flags eq 0x0002)***



Filter: http.request

Date/Time	Dst	port	Host	Info
2016-05-09 14:48:48	104.28.15.65	80	www.justmyvegas.com	GET / HTTP/1.1
2016-05-09 14:48:51	185.118.66.154	80	dimensionen.adriancampbell.co.uk	GET /5294669-enjoining-suet-undulate-bossiness-lasing-sent.jpg
2016-05-09 14:48:54	185.118.66.154	80	dimensionen.adriancampbell.co.uk	GET /?o=&x=BkD&e=TnIgC&s=tSmanqFpb&j=-kOcs1GGd&t=eVJZc&q=ECrx1
2016-05-09 14:48:55	185.118.66.154	80	dimensionen.adriancampbell.co.uk	GET /?o=&x=BkD&e=TnIgC&s=tSmanqFpb&j=-kOcs1GGd&t=eVJZc&q=ECrx1
2016-05-09 14:48:55	185.118.66.154	80	dimensionen.adriancampbell.co.uk	GET /?v=XE9Qn6Gy&o=BQrPc&p=nusY8UMLYS&h=W5JkmD5RX&m=7cKr&j=QSj
2016-05-09 14:48:57	185.118.66.154	80	dimensionen.adriancampbell.co.uk	GET /?l=1n0nCIS5I2&c=Ff9mD&v=&n=CVXqOJNd&p=aT0&w=ND3TXdhAi1&g=
2016-05-09 14:49:17	82.141.230.141	80	mfijevwfyfqzmd.com	POST /calendar.php HTTP/1.1
2016-05-09 14:49:18	95.211.205.228	80	xsroxkbclidyful.com	POST /forumdisplay.php HTTP/1.1
2016-05-09 14:49:18	95.211.205.228	80	xsroxkbclidyful.com	POST /include/class_dm_discussion.php HTTP/1.1
2016-05-09 14:49:31	95.211.205.228	80	xsroxkbclidyful.com	POST /blog.php HTTP/1.1
2016-05-09 14:51:31	95.211.205.228	80	xsroxkbclidyful.com	POST /search.php HTTP/1.1
2016-05-09 14:51:32	95.211.205.228	80	xsroxkbclidyful.com	POST /newthread.php HTTP/1.1

Shown above: Pcap of the traffic on a VM filtered in Wireshark. It's good up through the first Bedep post-infection traffic on 82.141.230.141.

After that, Bedep acts differently. You'll see Bedep contacting 95.211.205.228 after Bedep detects it's running on a VM, and it will download different malware.

As usual, no CryptXXX when doing the Angler EK/Bedep infection with a VM, and any click-fraud traffic is a ruse.

@Kafeine discusses this recent change in Bedep behavior here.

ASSOCIATED DOMAINS:

185.118.66.154 port 80 - **tilewrigbaieru.gt-racer.co.uk** - Angler EK

TRAFFIC CAUSED BY BEDEP:

- 82.141.230.141 port 80 - **qfsfajslsdexerid.com** - POST /blog.php
- 104.193.252.241 port 80 - **xqvyvibixozap.com** - POST /blog_ajax.php

- 104.193.252.241 port 80 - **xqvyvibixozap.com** - POST /include/class_bbcode_blog.php
- 104.193.252.241 port 80 - **xqvyvibixozap.com** - POST /album.php
- 104.193.252.241 port 80 - **xqvyvibixozap.com** - POST /forumdisplay.php
- 104.193.252.241 port 80 - **xqvyvibixozap.com** - POST /forumdisplay.php

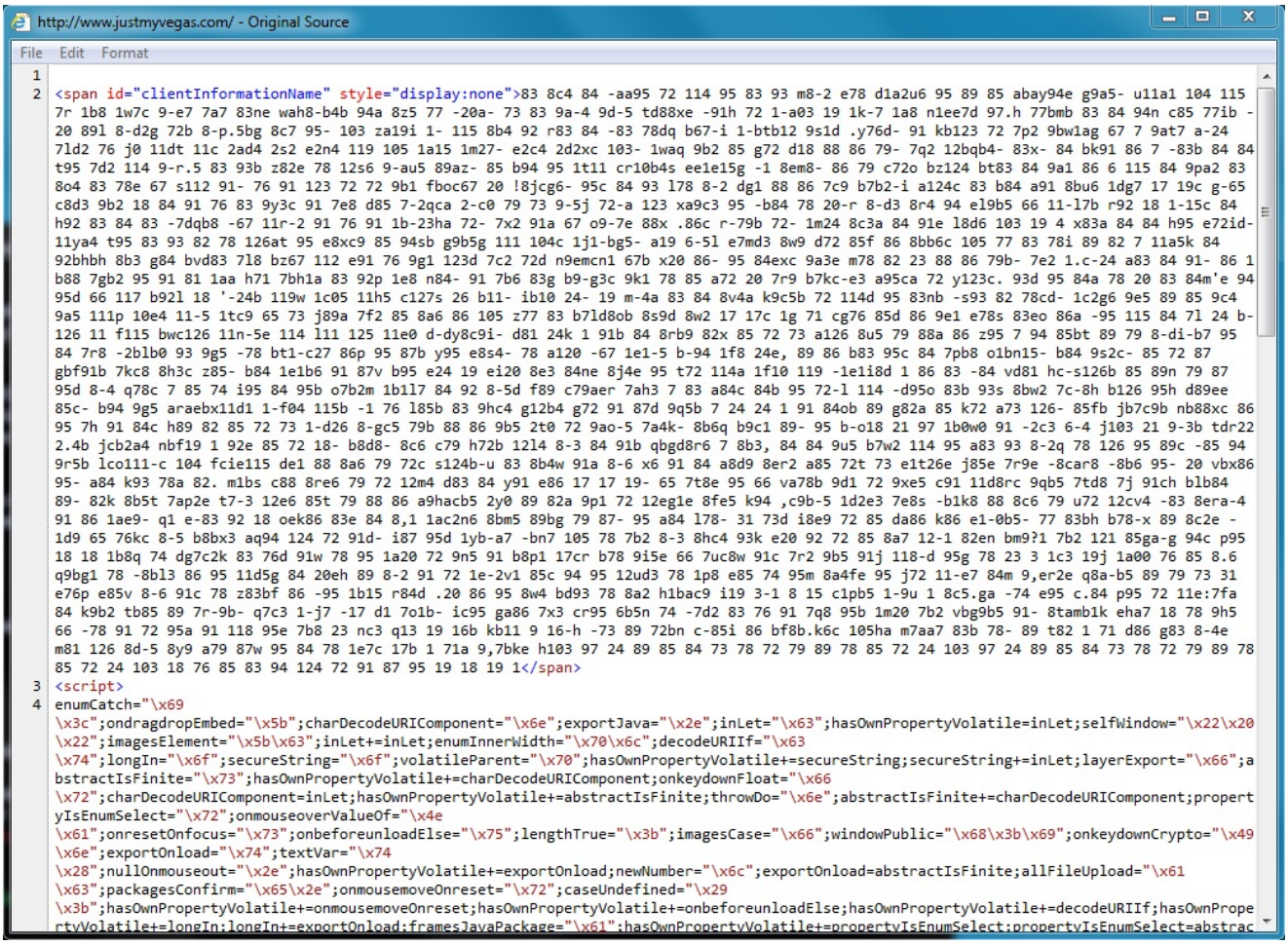
TRAFFIC CAUSED BY CRYPTXXX:

- 217.23.13.153 port 443 - TCP traffic, custom encoding
- 69.64.33.48 port 443 - TCP traffic, custom encoding

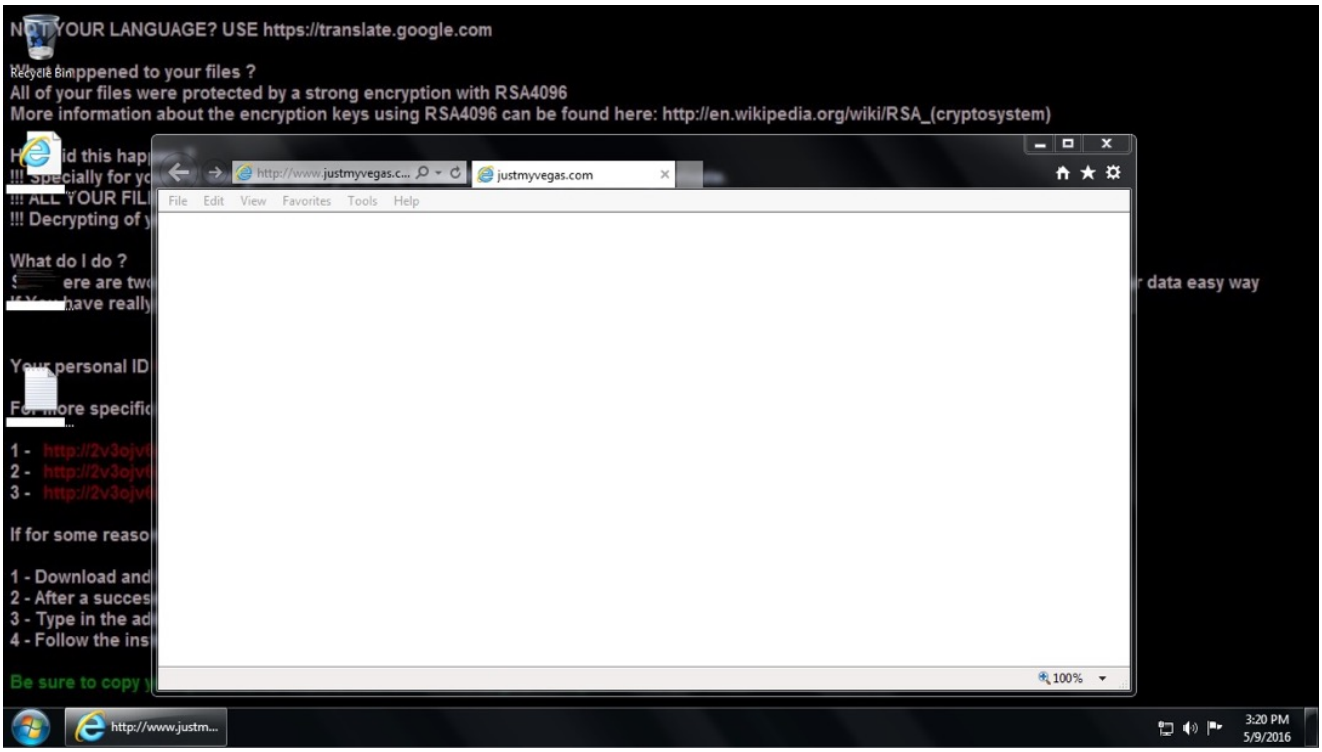
TRAFFIC CAUSED BY CLICK-FRAUD MALWARE:

- 5.199.141.203 port 80 - **ranetardinghap.com** - GET /adsc.php?sid=1957
- 93.190.141.27 port 80 - **cetinhechinhis.com** - GET /adsc.php?sid=1957
- 95.211.205.218 port 80 - **tedgeroatref.com** - GET /adsc.php?sid=1957
- 104.193.252.236 port 80 - **rerobloketbo.com** - GET /adsc.php?sid=1957
- 162.244.34.11 port 80 - **tonthishessici.com** - GET /adsc.php?sid=1957
- 188.138.105.185 port 80 - **kimpelasomasot.com** - GET /adsc.php?sid=1957

IMAGES



Shown above: Start of pseudo-Darkleech script returned from compromised website.



Shown above: Desktop of the Windows host after today's Angler EK/Bedep/CryptXXX infection.

FINAL NOTES

Once again, here are the associated files:

- ZIP archive of the pcaps: 2016-05-09-pseudo-Darkleech-Angler-EK-pcaps.zip 4.4 MB (4,390,349 bytes)
- ZIP archive of the malware and artifacts: 2016-05-09-pseudo-Darkleech-Angler-EK-malware-and-artifacts.zip 660.8 kB (660,816 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.