Malware-Traffic-Analysis.net - 2016-05-09 - pseudo-Darkleech Angler EK from 185.118.66[.]154 sends Bedep/CryptXXX ransomware

Archived: 2026-04-10 02:27:54 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:

- 2016-05-09-pseudo-Darkleech-Angler-EK-2-pcaps.zip 4.4 MB (4,390,783 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-and-CryptXXX-ransomware.pcap (4,114,289 bytes)

- 2016-05-09-pseudo-Darkleech-Angler-EK-and-CryptXXX-ransomware-files.zip 662.2 kB (662,234 bytes)

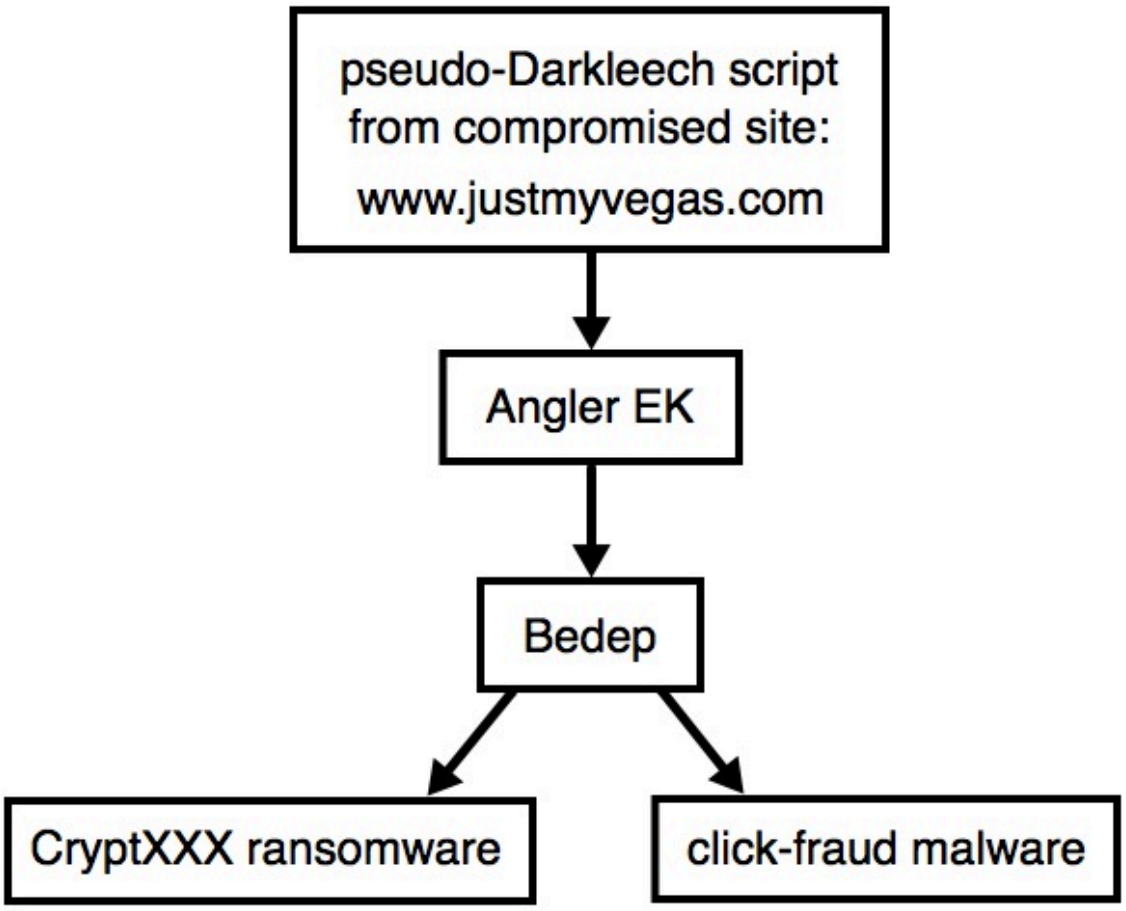
> - 2016-05-09-CryptXXX-ransomware-decrypt-instructions.bmp (2,023,254 bytes)
> - 2016-05-09-CryptXXX-ransomware-decrypt-instructions.html (14,193 bytes)
> - 2016-05-09-CryptXXX-ransomware-decrypt-instructions.txt (1,755 bytes)
> - 2016-05-09-CryptXXX-ransomware.dll (266,240 bytes)
> - 2016-05-09-click-fraud-malware.dll (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 ransomware .dll file.
- By Monday 2016-05-02, things were back to normal, with just the CryptXXX ransomware .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 ransomware .dll file.
- Today's CryptXXX ransomware behavior is slightly different than before, and the decryption instructions are formatted a little differently.

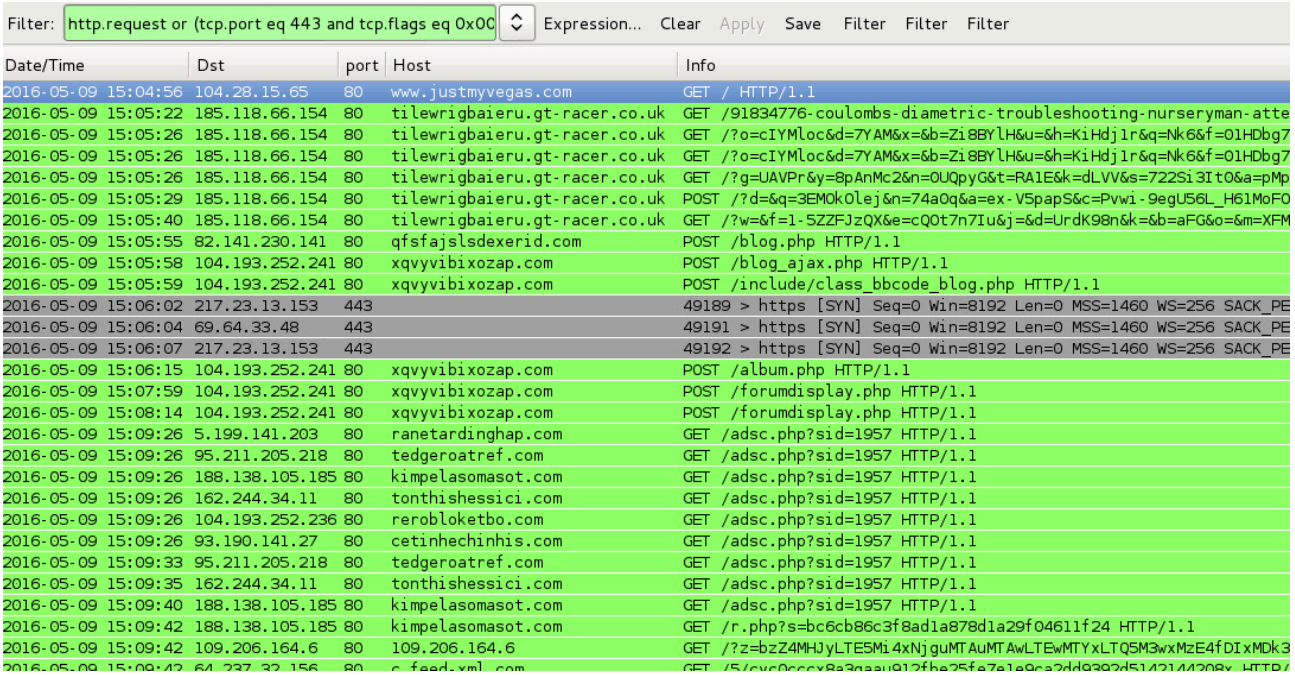
- Today's Click-fraud malware: C:\ProgramData\{9A88E103-A20A-4EA5-8636-C73B709A5BF8}\d3d10.dll
- Today's CryptXXX ransomware: C:\Users\[username]\AppData\Local\Temp\{98D13E48-E0E4-429B-9E7B-633FD7689461}\api-ms-win-system-framebuf-l1-1-0.dll

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

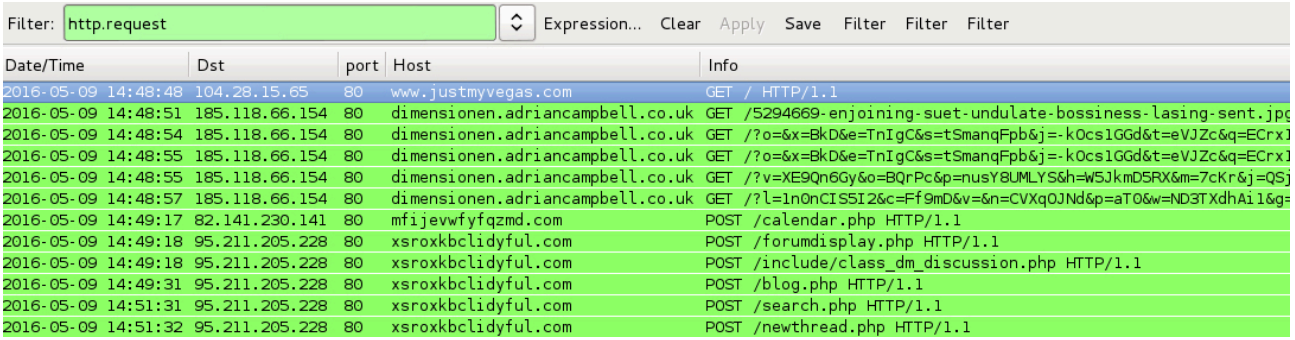


Shown above: Chain of events for today's infection.

TRAFFIC



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)***



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 ransomware 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

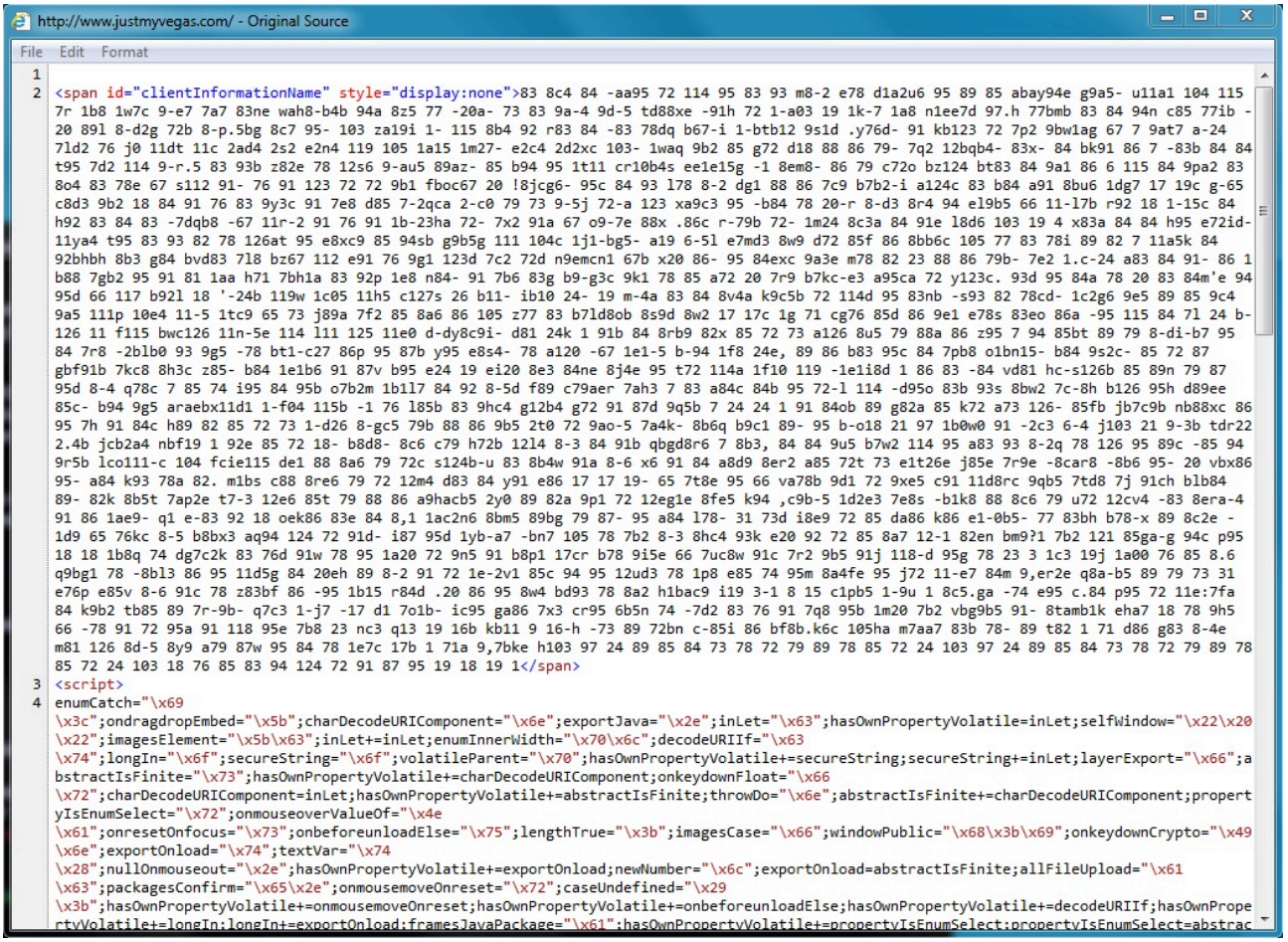
TRAFFIC CAUSED BY CRYPTXXX RANSOMWARE:

- 217.23.13[.]153 port 443 - TCP traffic, custom encoding
- 69.64.33[.]48 port 443 - TCP traffic, custom encoding

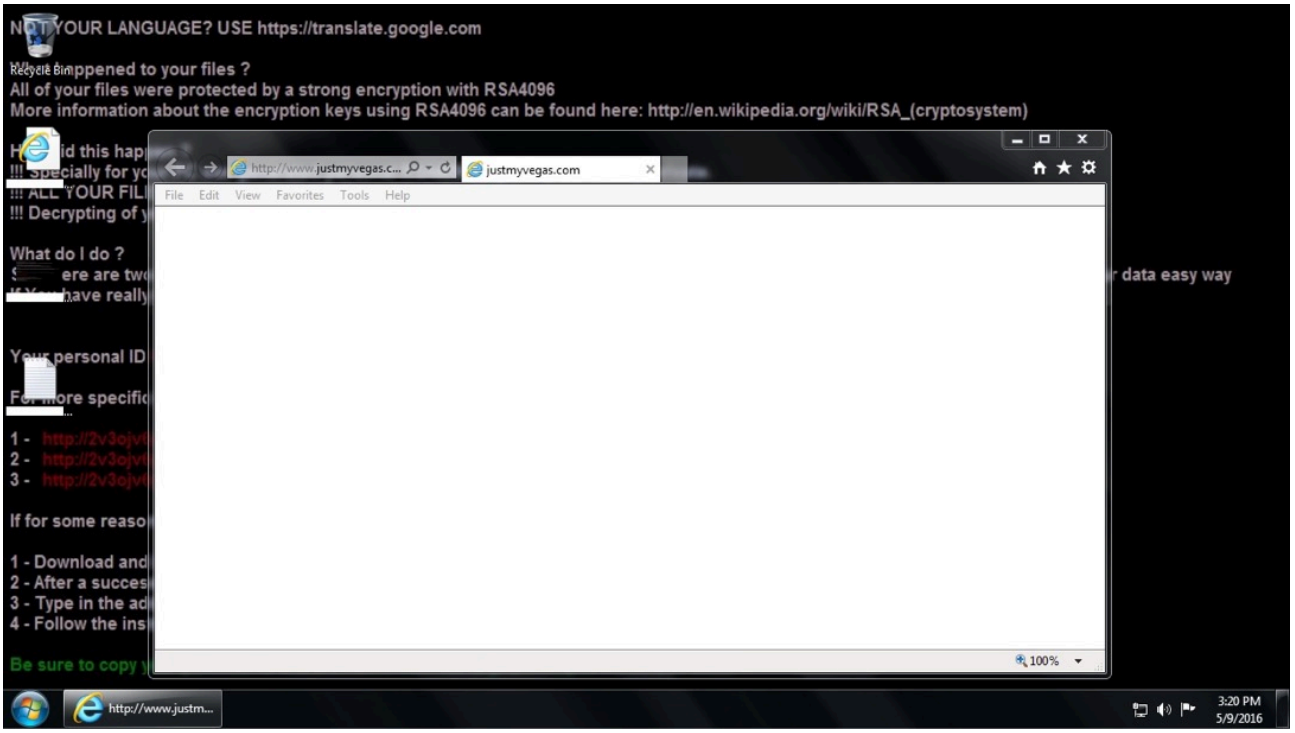
TRAFFIC CAUSED BY CLICK-FRAUD MALWARE:

- 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.

Click here to return to the main page.
