# TDL4 - Purple Haze (Pihar) Variant - sample and analysis

**a** contagiodump.blogspot.com/2012/02/purple-haze-bootkit.html





Lately things just don't seem the same Actin' funny, but I don't know why 'Scuse me...... while I kiss the sky Jimi Hendrix "Purple Haze"

I recently ran into an interesting piece of malware that was downloaded on a victim's computer. I thought it was TDL/TDSS or maybe a new version of it as it had same components as TDL4 bootkit with a functionality of a mass scale PPC (pay-per-click) fraud. TDL had this functionality too and it is most likely spread by the same Russian-speaking gangs using the Blackhole exploit kit. It did not have the same type of config file that you may find in TDL4 (and first I could not find it at all). I call it "Purple Haze" thanks to the strings found in the code.

I shared it with Alexander Matrosov from ESET. He and Eugene Rodionov analyzed it and posted an article on the ESET blog: <u>"TDL4 reloaded: Purple Haze all in my brain" (edited by David Harley)</u>

Eset also updated the removal tool for this variant - direct download link: <u>OlmarikTDL4</u> <u>remover</u>

### Distribution

The exploit host is <u>featured on CleanMX</u>. The domain was repossessed by GoDaddy after January 24, 2012 by but you can see some of the URLs. Infection happened via Blackhole exploit kit **95.211.115.228** 

### **General File Information**

File: w.php.exe Size: 130560 MD5: A1B3E59AE17BA6F940AFAF86485E5907

### Download

Download purplehazetdl.zip as a password protected archive (contact me if you need

the password)

Download pcap BIN\_purplehaze-pihar-A1B3E59AE17BA6F940AFAF86485E5907-2012-02.zip (235MB)

### Automatic scans

Original scan was only 2/43 but it is better now. It gets detected as a generic trojan or rootkit or as TDL/TDSS/Alureon. Virustotal SHA256: 9746b4f684b9d7d346ff131cd024e68d1b06e1b81571ce6d3c5067f0829d7932 SHA1: 6d07cf72201234a07ab57fb3fc00b9e5a0b3678e MD5: a1b3e59ae17ba6f940afaf86485e5907 File size: 127.5 KB (130560 bytes) File name: w.php.exe Win32 EXE File type: Detection ratio: 24 / 43

2012-02-02 06:50:05 UTC (1 minute ago) Analysis date: AntiVir TR/Alureon.FK.93 20120201 Avast Win32:Rootkit-gen [Rtk] 20120202 BitDefender Trojan.Generic.7154539 20120202 Comodo TrojWare.Win32.Trojan.Agent.Gen 20120202 BackDoor.Tdss.5231 DrWeb 20120202 Emsisoft Trojan.Win32.FakeAV!IK 20120202 eSafe Win32.Rorpian.C 20120130

F-Secure Trojan.Generic.7154539 20120202 Fortinet W32/Rorpian.C!tr 20120202 GData Trojan.Generic.7154539 20120202 Ikarus Trojan.Win32.FakeAV 20120202 Kaspersky Trojan.Win32.FakeAV.kpsj (TDSS Killer detects it as Pihar.b) 20120202 McAfee-GW-Edition Artemis!A1B3E59AE17B 20120202 Microsoft Trojan:Win32/Alureon.FK 20120202 NOD32 Win32/Olmarik.AYD 20120202 Norman W32/Troj Generic.LPAP 20120201 Sophos Mal/Generic-L 20120202 TrendMicro-HouseCall TROJ SPNR.16AQ12 20120202 VBA32 -20120131 VIPRE Trojan.Win32.Generic!BT 20120202

## Desription

You can read more detailed binary analysis on the ESET blog (Feb.2 2012) : <u>"TDL4</u> reloaded: Purple Haze all in my brain"

### Update. Feb 2, 2012

I heard today it is a recent but known variant detected by Kaspersky as "Pihar", which is supposedly a member of the TDL/TDSS/Olmarik/Alureon/ - Maxss family that does not encrypt the hidden container. I have to say I saw that Kaspersky detected it as Pihar.b via TDSS Killer (the dropper is detected as FakeAV) but it was a totally different name and I could not find any explanation of how Pihar is different from TDL4 - whether it is a misdetection, a different rootkit, some generic signature name, or a different variant of TDL. With the number of malware variants these days in the wild, it does not surprise me that it was known to them but there was no analysis posted (or I did not find it). I hope this analysis and the work done by ESET will make the family description more complete. TDSS Killer also removes it.

It is a kernel mode rootkit compatible with x86 and x64 Windows. It uses dll injection ph.dll and phx.dll (for x64). It creates a hidden VFS to store all the data.

The list of hidden system files:

- 1. Phdata [PurpleHaze] pn=161 all=ph.dll allx=phx.dll wait=3600
- 2. phm (original master boot record)
- 3. ph.dll (payload dll for x86)
- 4. phx.dll (payload dll for x64)

- 5. phd (driver x86)
- 6. phdx (driver x64)
- 7. phs (RC4 encrypted list of CC Urls, the key is phs see the ESET post. In this case they are

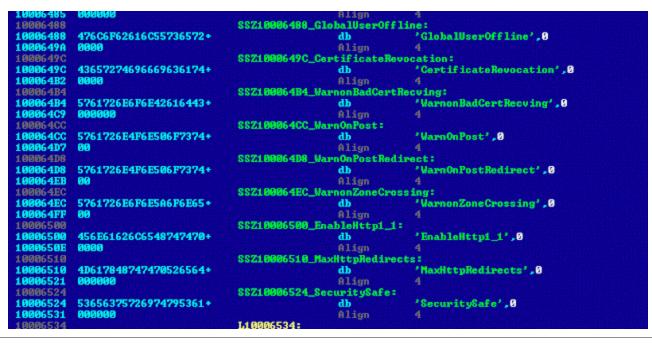
http://howtodoitman[.]com http://ntvgljvty[.]com http://chucjhomepage[.]com http://ebuyadult[.]com http://141.136.16.152 http://piratesmustdie[.]com http://gjhyjljvty[.]com

- 8. phld (16-bit loader code)
- 9. phln (rootkit driver replacing kdcom.dll for x86)
- 10. phlx (rootkit driver replaceing kdcom.dll for x64)

It lowers internet security settings to enable the clicker component perform extensive browsing without any alerts or pop-ups.

1000668C		SSZ1000668C	
	255B5E2E5D2E255B5E28+	db	'x[^,],x[^C](x[^)])',8
1000669F	00	Align	4
10006660		\$\$2100066A0_wait:	
	7761697488	dh	'wait',0
100066A5	000000	Align	4
10006648		SSZ100066A8_PurpleHaze:	
10006668	50757270606548617865+	db	'PurpleHaze'.8
10006683	09	Align	4
10006684		SSZ10006684_ph_s_s_s_s	
10006684	78687025737025737025+	db	'phixs ixs ixs ixs', 0
10006603	09	Alian	4
100066C4		L188866C4:	
100066C4	2D	dh	2Dh ; '='
10006605	00	db	895
10006666	00		89h
10006607	09	46	80h
100066C8		SSZ188866C8_HTTP_1_1_288_01	
100066C8	485454582F312E312832+	dh	'HTTP/1.1 200 OK',0
10006608		SSZ188866D8_Content_Typet	
10006608	436F6E74656E742D5479+	dh	'Centent-Type: text/html',8
100066F0		SSZ188866F8_Content_Length	
100066F0	436F6E74656E742D4C65+	dh	'Centent-Length: Xd',8
10006703	00	Align	4
10006704		\$\$218886784_Cache_Control_	must revalidate :
10006704	43616368652D436F6E74+	dh	'Cache-Control: must-revalidate, no-cache, no-store'.8
10006737	00	Align	4
10006738		SSZ10006738 Pragma_no_cacl	
10006738	507261676D6130206E6F+	db	'Pragna: no-cache',8
10006749	000000	Alian	4
1000674C		SSZ1888674C Expires Sat 8	11 Jan 2000 00 00 :
10006740	457878697265733A2853+	dh	'Expires: Sat, 01 Jan 2000 00:00:00 GMT',0
10006773	68	Alian	4
10006774		SSZ18886774_Connection_clo	ate I
10006774	436F6E6E656374696F6E+	db	'Connection: close'.8
10006786	0000	Align	4
10006788		L10006788:	
10001000	A.5		A01 1 1

Purple Haze



Change IE settings

## Traffic

Pay-per-click fraud generates significant revenue for the botnet owners. <u>The 'Advertising'</u> <u>Botnet" article from Securelist explains the click fraud scheme in great detail.</u>

"Advertising Botnet" by Securelist

#### C&C check-in upon install

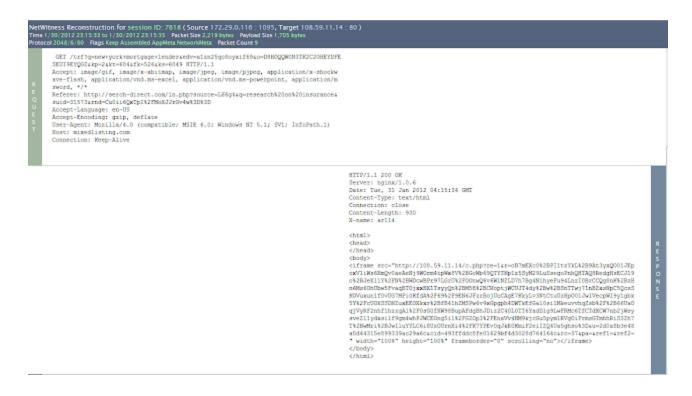
	22:17:47.20333	172.29.0.110	0.0.0.0	DNS	Standard query A howtodolitean.com
2	22:17:47.284888	75.75.75.75	172.29.0.116	DNS	Standard query response A 141.136.16.158
	22:17:47.285176	172, 29, 0, 116	141.136.16.156	TEP	dka > http://swn/ seq=0.wfm=66240.cen=0.Min=1460.nark_FEEM=1
	22117147.423618	141,136,16,156	172, 29.0, 116	TCP	http://dka.[shn, Ack] seq-0 Ack-1 win-85555 Len-0 Ass-1460 SACK_PC84-1
		172, 29, 0, 116	141.136.16.156	TOP	ticka > http: [ack] Seq-1 ack-1 win-60240 Len-0
	22:17:47.423657				
	22117147,423980	172, 29.0, 116	141,136,16,156	HTTP	GET /2d0gvEcjAB0hSqqSelNdkSvpDkCOW/l2lcx11g== HTTP/1.0
7	22:17:47.565273	141,136,16,156	172, 29, 0, 116	TEP	http > dka [ACK] Seq-1 Ack-101 Win-65535 Len-0
	22:17:47.572307	141.136.16.156	172.29.0.116	TEP	[tcr segment of a reassembled etu]
	22:17:47.372585	141,136,16,156	172, 29.0, 116	HTTP	HTTP/1.1 200 0K (text/html)
	22:17:47.572627	172, 29.0, 116	141.136.16.156	704	dka > http [ark] seq-101 ark-184 win-66058 Len-0
	22:17:47.373117	172, 29, 0, 116	141,130,16,156	TCP	dka > http://fin.ack/ Seq-101 Ack-154 win-64058 Len=0
	22:17:47.711760	141,136,16,156	172, 29, 0, 116	TCP	http > dka [AEK] Seq=184 AEk=102 win=65514 Len=0
15	22117148.602793	172, 29.0, 116	141,136,16,156	TOP	prat > http (svn) seg=0 win=64240 Len=0 MSS=1460 SACK_PERM=1
2.4	22:17:48.745384	141,136,16,156	172,29.0,116	TCP	http > prat (SYN, ACK) Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM=1
	22:17:48.745454	172.29.0.116	141.136.16.156	70.0	prat > http://arx/ seg-1 ark-1 win-64240 ien-0
	22:17:48,745841	172, 29, 0, 116	141,136,16,136	HTTP	GET /2000/Cc/AAV75ac8vF10m55+0PLrP11vx01fg1yfEbuC0xrmTx11/TbqPxej75uAL40G7mfjcDm4uLw+ HTTP/1.0
	22:17:48.902072	\$41,136,16,156	\$72,29.0.316	40P	http > prat [Ark] seq=1 Ark=141 win=65535 ten=0
	22:17:48.912641	141.136.16.136	172, 29.0, 116	TEP	[TCP segment of a reassembled PD0]
	22:17:48.912096	141,176,16,156	172, 29, 0, 116	REDP	HTTP/1.1 200 CK (text/html)
20	22117148.913149	172, 29, 0, 116	141.136.16.156	TCP	prat > http://ackj.seg-041.ack-252.win-63590_Len=0
23	22:17:48.913461	172, 29, 0, 116	141,136,16,156	TCP	prat > http (FIN, ACK) Seq-141 Ack-252 win-63990 Len-0
	22117148.920087	172.29.0.116	141.136.16.156	TOP	dssTapl > http [SYN] seg-0 win-64240 Len-0 MSS-1460 SACK_PTIM-1
	22:17:49.054824	141.136.16.136	172, 29, 0, 116	TCP	http > prat (ACK) Seq=252 Ack=142 win=65514 Len=0
	22:17:49.071658	141.136.16.156	172.29.0.116	101	http > dssiapi [sym, ack] seq-0 ack-3 win-65535 sen-0 MSS-1460 sack_MEDM-1
	22:17:49.071090	172, 29.0, 116	141,136,16,136	TEP	dssiapi > http://www.seq-1.ack=1.win=64240.cen=0
26	22:17:49.072057	172, 29, 0, 116	141.136.16.156	HTTP	tar /dkix3ingkuv6iyct#bcfra54#ran7ac20ca HTTP/1.0
27	22117:49,207190	141,136,16,156	172, 29, 0, 110	TCP	http:>:dssiapi [ACK] seg=1 ACK=97 win=65535 Len=0
	22:17:49.207512	141.116.16.156	172.29.0.116		HTTP/1.1 200 OK (application/octet-stream)
	22117149.207547	172.29.0.116	141.136.16.156	TOP	dss1apl > http [ACK] seg=97 ACk=373 win=63869 Len=0
	22:17:49.207905	172, 29.0, 116	141,136,16,156	TEP	dustapt > http [FIN, ACK] Seq-97 Ack-371 Win-63669 Len-0
	22:17:49.344513	141.136.16.156	172.29.0.116	TOP	http://dssiapi_[ack]_seq=373_ack=98_win=65534_tem=0
	22:19:34.299346	-172,29.0,110	372,29.0,235		Local Master Announcement XPSP1-R93-OFC2D, Workstation, Server, NT Workstation, Potential Browser, Master Drowser
- 22	22:19:57.147236	172.29.0.1	172.29.0.116	709	fuscript > icslap (kit) sec-1 win-0 Len-0
34	22:20:17.258192	172,29,0,110	75.75.75.75	DNS	standard overy A x-web, in
	22:20:17.331255	75.75.75.75	172.29.0.116	DACS	Standard query response A 178,218,213,156
	22120117.331642	172.29.0.116	178.238.233.156	TEP	dellpwraphs > http [Syn] Seg-0 win-64240 Len-0 MSS-1460 SACK FEM-1
	22:20:17,451434	178,238,233,156	172,29.0,116	TCP	
					http > dellpwrappks [SYN, ACK] Seq=0 Ack=1 win=65515 Len=0 MSS=1460 SACK_PE8M=1
	22120117.451473	172, 29.0, 116	178.238.233.156	TOP	dellpwrappks > http [ack] seq=1 Ack=1 win=64240 ten=0
19	22:20:17.451779	172, 29, 0, 110	178,238,233,136	NTTP	GET /Y2x8H542f02H2jg0HjRH00FTYHNj0Tc3Y2FkZjLx2jk32GR1NjdHf062HQ-= HTTP/1.0
40	22:20:17.575616	178,238,233,156	\$72,29.0,516	TEP	http > dellgwrappks [ack] seg-1 Ack-218 win-65535 Len-0
	22:20:27.216096	172, 29.0, 110	. 172, 29. 0, 253		Domain/Workgroup Announcement MSHONE, NT Workstation, Domain Enum
	22:20:29.806382	178,228,232,156	172, 29. 0. 116	HTTP	HTTP/1.1 200 ck (text/plain)
	22120129.806416			TCP	http://dellowrapsks/fith, ACN/ seg-1309 ACK-218 win-65535 Len-0
		178,238,233,156	172, 29, 0, 116		
	22:20:29.806494	172, 29.0, 216	278,238,233,156	TEP	dellpwrappks > http://dckj Seq-218 Ack-1170 win-52872 cen-0
- 45	22:20:29.806494 22:20:29.807276	172,29.0,116 172,29.0,116	178.238.233.156 178.238.233.156	TEP	dellpwrappkn > http: [ACK] Seq-218 Ack-1370 win-62872 Len-0 dellpwrappks > http: [FIN, ACK] seq-238 Ack-1370 win-62872 Len-0
- 45	22:20:29.806494	172, 29.0, 216	278,238,233,156	TEP	dellpwrappks > http://dckj Seq-218 Ack-1170 win-52872 cen-0
45 46	22:20:29.806494 22:20:29.807276 22:20:29.812872	172.29.0.116 172.29.0.116 172.29.0.116	178.238.233.156 178.238.233.156 178.238.233.156	TEP	dmllpmrappks > http://ackj.sep=208.ack=1270.wtm=02822.tem=0 dmllpmrappks > http://stm.ackj.sep=028.ack=1270.wtm=02822.tem=0 epc > http://stmp0.wtm=04240.tem=0.MSS=1460.Sack_FE80=1
45 46 47	22:20:29.806494 22:20:29.807276 22:20:29.812872 22:20:29.924428	172, 29, 0, 216 172, 29, 0, 116 172, 29, 0, 216 178, 238, 233, 156	278,238,233,156 178,238,233,156 178,238,233,156 178,238,233,156 172,29.0,116	TCP TCP TCP TCP	dellperaphis > http:[Ack] Seq=210 Ack=1270 with=02152 Len=0 dellperaphis > http:[Th], Ack] Seq=210 Ack=1270 with=02152 Len=0 epc > http:[Sh] Seq=0 Win=64240 Len=0 WISS=1440 SACK_FERM=0 http: > dellperaphis Lack] Seq=1370 Ack=210 Win=65210 Len=0
45 46 47 48	22:20:29.806494 22:20:29.807276 22:20:29.812872 22:20:29.924428 22:20:29.931609	172, 29, 0, 216 172, 29, 0, 116 172, 29, 0, 216 178, 238, 233, 156 178, 238, 233, 136	176,218,233,156 178,238,233,156 178,238,233,156 178,238,233,136 172,29,0,116 172,29,0,116	1CP 1CP 1CP 1CP 1CP	dellperappks > http://acki_sep-210.kck=1170_wtm=02102_ten=0 dellperappks > http://sni.acki_sep-20.kck=1370_wtm=02102_ten=0 epc > http://sni/b_sep-0_wtm=04040_ten=0_MSS=1440_SACK_#EMM=1 http:> dellperappks_tarksep_1170_ack=210_wtm=0518t_ten=0 http:> epc_(Sni, Acki_sep=0_acki_st_min=0518t_ten=0
45 46 47 48 49	22:20:29,806494 22:20:29,807276 22:20:29,82772 22:20:29,924428 22:20:29,931009 22:20:29,931681	172, 29, 0, 216 172, 29, 0, 316 172, 29, 0, 316 178, 238, 233, 156 178, 238, 233, 156 178, 238, 235, 156	178,218,213,156 178,218,233,156 178,238,233,156 172,29,0,116 172,29,0,116 179,238,232,156	1CP 1CP 1CP 1CP 1CP 1CP	dellperaphics > http: [Ack] Seq=218 Ack=120 with=02182 cen=0 dellperaphic > http: [Thm, Ack] Seq=218 Ack=120 with=02182 cen=0 epc > http: [Sth] Seq=0 win=64240 cen=0 wiss=1440 SACK_FERM=0 http: > dellperaphic Tack] Seq=170 Ack=210 win=652514 cen=0 http: > exp [Sth, Ack] Seq=0 Ack=1 win=69350 cen=0 %SS=1400 SACK_FERM=0 http: > http: [Ack] Seq=0 Ack=1 win=69310 cen=0
45 46 47 48 49 50	22:20:29.806494 22:20:29.80276 22:20:29.80276 22:20:29.924428 22:20:29.931861 22:20:29.931681 22:20:29.931681 22:20:29.932681	172, 29, 0, 216 172, 29, 0, 316 172, 29, 0, 316 178, 218, 213, 156 178, 238, 235, 136 172, 29, 0, 116 172, 29, 0, 316	276,238,233,156 178,238,233,156 178,238,233,156 177,29,0,116 172,29,0,116 179,230,232,156 178,238,233,156	ТСР ТСР ТСР ТСР ТСР ТСР ТСР КТТР	dellperappks > http:[http://sep-218.ktk-1170.wtm-62122.ten-0 dellperappks > http:[http://sep-218.ktk-1170.wtm-62122.ten-0 epc > http:[SNN] Sep-0 wtm-64340.ten-0 MSS-1460.5atK,#E8M-1 http:> dellperappks [stm] Sep-0 ktk-130.mtm-6358.ten-0 http:> dellperappks [stm] Sep-0 ktk-130.mtm-6358.ten-0 http:> epc [SNN_kX]_Sep-0 ktk-130.mtm-6358.ten-0 sepc > http:[stm] Sep-0 ktk-130.mtm-6358.ten-0 epc > http:[stm] Sep-0 ktk-130.mtm-64340.sen-0 ct_1722e862.tfcms[]go8[]sepconfThms[]off274182[]stm2[]k2608[%]deff0209[]= mtTP/1.0
45 46 47 48 49 50	22:20:29.80/276 22:20:29.80/276 22:20:29.80/276 22:20:29.92428 22:20:29.931609 22:20:29.931609 22:20:29.931609 22:20:29.931609 22:20:29.931609	172, 29, 0, 216 172, 29, 0, 316 172, 29, 0, 316 178, 238, 233, 156 178, 238, 233, 156 177, 29, 0, 316 172, 29, 0, 316	274,216,213,156 178,218,213,156 178,218,213,156 172,29,0,116 172,29,0,116 172,29,0,116 178,218,213,156 178,238,233,156	ТСР ТСР ТСР ТСР ТСР ТСР ТСР ВТТР	dellperaphics > http: [Ack] Seq=218 Ack=120 with=02182 Len=0 dellperaphics > http: [Thm, Ack] Seq=218 Ack=120 with=02182 Len=0 eps > http: [Sth] Seq=0 Win=04240 Len=0 MSS=1440 SACL_FERM=3 http: > dellperaphic Tack] Seq=170 Ack=210 win=053518 Len=0 http: > exp [Sth, Ack] Seq=0 Ack=1 Win=03103 Len=0 MSS=1400 SACL_FERM=1 http: > ktp: [Sth] Seq=170 Ack=1 Win=03103 Len=0 MSS=1400 SACL_FERM=1 http: > http: [Sth] Seq=170 Ack=1 Win=03103 Len=0 MSS=1400 SACL_FERMINET_CONTINUET_CON
45 46 47 48 49 50 50	22:20:29.80494 22:20:29.80/276 22:20:29.81287 22:20:29.81287 22:20:29.931605 22:20:29.931605 22:20:29.911681 22:20:29.911681 22:20:29.931079 22:20:29.931079	172,29.0,116 172,29.0,116 172,29.0,116 178,218,213,156 178,218,213,156 172,29.0,116 172,29.0,116 172,29.0,116 172,29.0,116 178,218,233,156	276,236,233,136 178,238,233,136 176,238,233,136 172,29,0,116 172,29,0,116 178,238,233,136 178,238,233,136 178,238,233,136 178,238,233,136	ТСР ТСР ТСР ТСР ТСР ТСР ЕТТР ТСР ТСР	dellperaphic > http:[hack] seq=210 kack=1270 win=62102 ten=0 dellperaphic > http:[hack] seq=210 kack=1270 win=62872 ten=0 eps > http:[StN] seq=0 win=66380 ten=0 MSS=1640 Sack, #E8M3 http:> dellperaphic [stN] seq=0 kack=1 win=6538 ten=0 http:> dellperaphic [stN] seq=0 kack=1 win=6538 ten=0 MSS=1640 Sack_FE8M3 eps > http:[StN] seq=0 kack=1 win=66380 ten=0 for //v28MSS=20000 [seq=0 MV2804580/ens26[seg30000 htms]spr24v2828[seg3000155500000 Htms]spr24v280 http://secs1.seq=1 acks:1 win=1000000000000000000000000000000000000
45 46 47 48 49 50 50 50 52 52	22:20:29.80444 22:20:29.8124 22:20:29.8124 22:20:29.8124 22:20:29.8124 22:20:29.8124 22:20:29.93109 22:20:29.93109 22:20:29.931079 22:20:29.931079 22:20:35.001392 22:20:35.03399	172, 29.0, 216 172, 29.0, 316 172, 29.0, 316 178, 218, 218, 215, 156 178, 218, 235, 156 172, 29.0, 316 172, 29.0, 316 172, 29.0, 316 178, 238, 233, 156 172, 29.0, 316	278,238,238,233,156 178,238,238,233,156 178,238,233,136 172,29,0,136 172,29,0,136 178,238,233,136 178,238,233,136 178,238,233,136 177,237,25,75	ТСР ТСР ТСР ТСР ТСР ТСР ТСР ВТТР ВТТР ПТР ТСР БКБ	dellperaphics > http: [Ack] Seq=218 Ack=120 with=02122 Len=0 dellperaphic > http: [Ack] Ack] = 100 with=02122 Len=0 ept > http: [Sth] Seq=0 win=04240 Len=0 wiss=1440 SACL_FERM=1 http: > dellperaphic Tack] seq=170 Ack=210 win=0555140 SACL_FERM=1 http: > dellperaphic Tack] seq=170 Ack=210 win=0555140 SACL_FERM=1 ept > http: [Ack] Seq=0 Ack=4 win=04303 Len=0 #S5=1400 SACL_FERM=1 ept > http: [Ack] Seq=0 Ack=4 win=04303 Len=0 Act //2280542700x8[j004]Booof TweJortK2[J02[k1204]kjdffC2M0== #TTP/1.0 http: seq: [Sth] Ack=4 win=04303 Len=0 Act //2280542700x8[j004]Booof TweJortK2[J02[k1204]kjdffC2M0== #TTP/1.0 http: seq: [Ack] Seq=0 Ack=3 win=05335 Len=0 Standard gapery A widdrower.http://science.act.net
45 46 47 48 49 50 50 50 52 52	22:20:29.80494 22:20:29.80/276 22:20:29.81287 22:20:29.81287 22:20:29.931605 22:20:29.931605 22:20:29.911681 22:20:29.911681 22:20:29.931079 22:20:29.931079	172,29.0,116 172,29.0,116 172,29.0,116 178,218,213,156 178,218,213,156 172,29.0,116 172,29.0,116 172,29.0,116 172,29.0,116 178,218,233,156	278,238,238,233,156 178,238,238,233,156 178,238,233,136 172,29,0,136 172,29,0,136 178,238,233,136 178,238,233,136 178,238,233,136 177,237,25,75	ТСР ТСР ТСР ТСР ТСР ТСР ЕТТР ТСР ТСР	dellperaphic > http:[hack] seq=210 kack=1270 win=62102 ten=0 dellperaphic > http:[hack] seq=210 kack=1270 win=62872 ten=0 eps > http:[StN] seq=0 win=66380 ten=0 MSS=1640 Sack, #E8M3 http:> dellperaphic [stN] seq=0 kack=1 win=6538 ten=0 http:> dellperaphic [stN] seq=0 kack=1 win=6538 ten=0 MSS=1640 Sack_FE8M3 eps > http:[StN] seq=0 kack=1 win=66380 ten=0 for //v28MSS=20000 [seq=0 MV2804580/ens26[seg30000 htms]spr24v2828[seg3000155500000 Htms]spr24v280 http://secs1.seq=1 acks:1 win=1000000000000000000000000000000000000
45 46 47 48 49 50 50 52 53 54	22:20:29.80644 22:20:29.80/276 22:20:29.80/276 22:20:29.802872 22:20:29.812872 22:20:29.81069 22:20:29.411611 22:20:29.81207 22:20:29.81207 22:20:39.81207 22:20:39.81261 22:20:39.81261 22:20:39.8084 22:20:5.81266 22:20:5.91266 20:20:5.9126 20:2	172, 29, 0, 316 172, 29, 0, 316 172, 29, 0, 316 172, 29, 0, 316 174, 238, 238, 136 172, 29, 0, 316 172, 29, 0, 316 172, 29, 0, 316 174, 28, 238, 156 174, 29, 0, 316 174, 29, 0, 316 174, 29, 0, 316	274, 216, 213, 156 178, 218, 233, 156 177, 236, 235, 156 172, 29, 0, 116 172, 210, 215, 156 174, 210, 216, 215 178, 218, 235, 156 177, 29, 0, 116 172, 29, 0, 116 175, 75, 75, 75 157, 75, 75	TCP TCP TCP TCP TCP TCP TCP TCP TCP DAS DAS	dellperaphis > http: [Ark] Seq=210 Ark=1270 with=02122 ten=0 dellperaphis > http: [Ark, Ark] Seq=210 Ark=1270 with=02122 ten=0 epc > http: [SN] Sup=0 win=64300 ten=0 MSS=1400 SAK, MEMMA http: > dellperaphis Tark] Seq=1270 Ark=1 win=63303 ten=0 MSS=1400 SAK, MEMMA http: > dellperaphis Tark] Seq=1270 Ark=1 win=63303 ten=0 MSS=1400 SAK, MEMMA http: > dellperaphis Tark] Seq=1270 Ark=1 win=63303 ten=0 MSS=1400 SAK, MEMMA http: > tenp: [SN], Ark] Seq=0 Ark=1 win=63303 ten=0 MSS=1400 SAK, MEMMA http: > tenp: [SN], Ark] Seq=0 Ark=1 win=63303 ten=0 MSS=1400 SAK, MEMMA http: > tenp: [SN], Ark] Seq=0 Ark=1 win=63303 ten=0 MSS=1400 SAK, MEMMA http: > tenp: [SN], Seq=1 Ark=1 win=63303 ten=0 MSS=1400 SAK, MEMMA ten; YZ28065210000 (MSM) MYSSE12022 Registrations() provided tension () Http: > ten; [SN], Seq=1 Ark=1 win=63303 ten=0 Standard query: A withrewser.html; vaccomeat, met Standard query: A withrewser.html; vaccomeat, met
45 46 47 48 49 30 30 30 50 52 53 54 53	22 : 20 : 20 : 50 : 64 : 44 : 22 : 20 : 29 : 50 : 24 : 27 : 20 : 29 : 81 : 87 : 2 22 : 20 : 29 : 81 : 87 : 2 22 : 20 : 29 : 94 : 42 : 8 22 : 20 : 29 : 93 : 00 : 9 22 : 20 : 29 : 93 : 00 : 9 22 : 20 : 29 : 93 : 00 : 3 22 : 20 : 29 : 93 : 00 : 35 : 2 22 : 20 : 35 : 93 : 04 : 35 : 2 22 : 20 : 35 : 93 : 04 : 36 : 40 : 35 : 2 22 : 20 : 35 : 93 : 94 : 66 : 46 : 66 : 66 : 75 : 75 : 75 : 75 : 75 : 7	172, 29, 0, 116 172, 29, 0, 116 172, 29, 0, 116 178, 238, 213, 136 178, 238, 213, 136 172, 29, 0, 116 172, 29, 0, 116	278, 218, 233, 156 378, 218, 233, 156 178, 218, 233, 156 178, 218, 233, 156 172, 29, 0, 136 172, 29, 0, 136 178, 238, 233, 156 178, 238, 233, 156 178, 238, 233, 156 172, 29, 0, 136 172, 25, 0, 136 172, 25, 0, 136	TCP TCP TCP TCP TCP TCP HTP HTP TCP DAS DAS	dellperaphics > http: [Ack] Seq=218 Ack=120 with=02122 Len=0 dellperaphics > http: [Enx], Ack] Seq=218 Ack=120 with=02122 Len=0 eps > http: [SN] Seq=0 win=04240 Len=0 wiss=1440 SACL_FERM=1 http: > dellperaphic Tack] Seq=170 Ack=10 win=03353 Len=0 Mittp: > http: [Ack] Seq=0 Ack=1 win=04310 Len=0 WSS=1400 SACL_FERM=1 http: > http: [Ack] Seq=0 Ack=1 win=04310 Len=0 Set: //2280542700x8[j004]Boord Twe10743742[j122][k12041k]deffC2M0== WTE/2.0 Http: Seq. [Ack] Seq=0 Ack=1 win=04303 Len=0 Set: //2280542700x8[j004]Boord Twe10743742[j122][k12041k]deffC2M0== WTE/2.0 Http: > epc. [Ack] Seq=0 Ack=1 win=04303 Len=0 Set: //2280542700x8[j004]Boord Twe10743742[j122][k12041k]deffC2M0== WTE/2.0 Http: > epc. [Ack] Seq=0 Ack=1 win=043033 Len=0 Set: //2280542[store: http://208040] Set: //2280542[store: http://228040] Set: //2280542[sto
45 46 47 48 49 30 30 30 30 30 30 30 30 30 30 30 30 30	22 : 20 : 20 : 50 c4 44 22 : 20 : 20 : 40 · 20 · 27 22 : 20 : 20 : 40 · 27 22 : 20 : 20 · 40 · 32 22 : 20 : 20 · 40 · 32 22 : 20 : 20 · 50 · 32 22 : 20 : 20 · 50 · 32 22 : 20 : 20 · 50 · 32 22 : 20 : 25 · 90 · 944 22 : 20 : 25 · 90 · 944 22 : 20 : 25 · 90 · 944 22 : 20 : 55 · 94 · 90 · 94 22 : 20 : 55 · 94 · 90 · 94	172, 29, 0, 316 172, 29, 0, 316 172, 29, 0, 316 178, 238, 238, 238, 156 178, 238, 238, 136 172, 29, 0, 316 172, 29, 0, 316	278, 218, 213, 156 278, 218, 213, 156 278, 218, 213, 156 272, 218, 213, 156 272, 29, 0, 216 278, 218, 235, 136 278, 218, 235, 136 178, 258, 75, 75 172, 29, 0, 110 213, 174, 149, 74	TCP TCP TCP TCP TCP TCP RTIP TCP DAS DAS DAS DAS DAS	dellperaphis > http: [Ark] Seq-210 Ark-1170 with-02122 Len-0 dellperaphis > http: [Ark, ] Seq-210 Ark-1170 with-02122 Len-0 ept > http: [SN] Sup-0 with-04300 Len-0 MSS-1400 SAK, PERM-1 http: > ellperaphis [ark] Seq-210 Ark-11 with-02108 sine-02202 Len-0 http: > ellperaphis [ark] Seq-210 Ark-11 with-02108 sine-02202 Len-0 http: > ellperaphis [ark] Seq-210 Ark-11 with-02108 sine-02202 Her-0 http: > ellperaphis [ark] Seq-210 Ark-11 with-02108 sine-0202 SAK, PERM-1 http: > ellperaphis [ark] Seq-210 Ark-11 with-02108 sine-0200 SAK, PERM-1 Her-0200 SAK-11000 [one-01 way into:systex[strate]ere0400 SAK, PERM-1 Her-0200 SAK, Seq-140-0210 with systex[strate]ere0400 SAK, PERM-1 Her-0200 SAK, Seq-140-0210 with systex[strate]ere0400 SAK, PERM-1 Standard query: A stooset.html:systex[strate]ere0400 SAK, PERM-1 SAK, AND
45 46 47 48 49 50 50 50 50 50 50 51 55 56 57	22 22 22 29. 506444 22 20 29.29. 806276 22 20 29.29. 812877 22 20 29.29. 812877 22 20 29.49.4428 22 20 29.44428 22 20 29.44468 22 20 29.541681 22 20 29.541681 22 20 29.541681 22 20 25.54589 22 20 25.54698 22 20 25.54698 22 20 25.54698	372, 29.0, 316 372, 29.0, 316 372, 29.0, 316 378, 318, 218, 138, 156 372, 39.0, 318, 156 372, 39.0, 318, 156 372, 29.0, 316 372, 39.0, 316 372, 37, 37, 37, 37, 37, 37, 37, 37, 37, 37	$\begin{array}{c} 376, 216, 215, 136\\ 778, 218, 215, 136\\ 778, 218, 215, 136\\ 777, 210, 0, 136\\ 777, 210, 0, 136\\ 777, 120, 0, 136\\ 778, 128, 225, 136\\ 778, 128, 235, 136\\ 778, 128, 235, 136\\ 778, 128, 235, 136\\ 75, 75, 75, 75\\ 75, 75, 75, 75\\ 75, 75, 75, 75\\ 75, 75, 75, 75\\ 75, 75, 75, 75\\ 75, 75, 75, 75\\ 75, 75, 75\\ 75, 75, 75\\ 75, 75, 75\\ 75, 75, 75\\ 75, 75, 75\\ 75, 75, 75\\ 75, 75\\ 75, 75\\ 75, 75\\ 75, 75\\ 75, 75\\ 75, 75\\ 75, 75\\ 75, 75\\ 75, 75\\ 75\\ 75, 75\\ 75\\ 75\\ 75\\ 75\\ 75\\ 75\\ 75\\ 75\\ 75\\$	TCP TCP TCP TCP TCP TCP ENTP TCP CAS DAS DAS DAS DAS DAS	dellperaphis > http: [Ack] Sep-28 Ack-120 with-0272 Len-0 dellperaphis > http: [SN] Sep-0 Win-64240 Len-0 MSS-1460 SACK_FERM-3 http: > dellperaphis [Ack] Sep-0 Win-64240 Len-0 MSS-1460 SACK_FERM-3 http: > dellperaphis [Ack] Sep-0 Ack-14 Win-60330 Len-0 MSS-1460 SACK_FERM-3 http: > dellperaphis [Ack] Sep-0 Ack-14 Win-60330 Len-0 MSS-1460 SACK_FERM-1 eps > http: [Ack] Sep-1 Ack-14 Win-60330 Len-0 Act //228054270xx1[300] MSB-01 Win-65351 Len-0 Sep > http: [Ack] Sep-1 Ack-14 Win-60330 Len-0 MSS-1400 SiteConstrained Sack 14Win-60330 Len-0 MSS-1400 SiteConstrained Sack 14Win-60330 Len-0 MSS-1400 SiteConstrained Sack 14Win-60330 Len-0 Standard query & disconstrained Sack 14Win-60330 Len-0 Standard query & disconstrained Sack 14Win-60340 Sack_PERM-1 Standard query & disconstrained Sack 14Win-60340 Sack_PERM-1
45 46 47 48 49 50 50 50 50 50 52 53 54 55 55 57 58	22 22 20 20 30 400 276 22 20 20 20 40 400 276 22 20 20 20 40 400 276 22 20 20 20 40 40 276 22 20 20 20 40 40 40 22 20 20 25 40 40 40 22 20 25 5, 94 40 40 20 20 25 20 25 5, 94 40 20 20 20 25 20 25 5, 94 40 20 20 20 25 20 25 5, 94 40 20 20 20 25	272, 29, 0, 116 272, 29, 0, 116 272, 29, 0, 116 274, 278, 273, 126 276, 278, 275, 128 277, 29, 0, 116 277, 277, 277, 27	$\begin{array}{c} 176, 216, 213, 136\\ 776, 218, 213, 136\\ 776, 218, 213, 136\\ 776, 216, 213, 136\\ 772, 216, 0, 136\\ 772, 216, 0, 136\\ 776, 216, 213, 136\\ 776, 216, 213, 136\\ 757, 216, 213, 136\\ 757, 75, 75, 75\\ 757, 219, 0, 136\\ 757, 75, 75\\ 772, 29, 0, 136\\ 757, 75, 75\\ 772, 29, 0, 136\\ 757, 75, 75\\ 772, 29, 0, 136\\ 757, 75, 75\\ 772, 29, 0, 136\\ 757, 75, 75\\ 757, 75, 75\\ 757, 757\\ 757, 757$ 757 757 757 757 757, 757 757 757 757 757 757 757 75	TEP TEP TEP TEP TEP TEP ETTP HTTP MTTP DAS DAS DAS DAS DAS DAS	dellperaphis > http: [Ack] Seq=218 Ack=120 with=62822 Len=0 dellperaphis > http: [SN] Seq=218 Ack=120 with=62822 Len=0 ept > http: SNI[Seq=2 with=64340 Len=0 MSS=1460 SACK_PE88=3 http: Ack] Seq=2 with=64340 Len=0 MSS=1460 SACK_PE88=3 http: Ack] Seq=2 Ack_2180 Ack=218 with=65338 Len=0 MSS=2480 SACK_PE88=3 http: Ack] Seq=2 Ack_2180 Ack_2180 Len=0 MSS=1460 SACK_PE88=3 http: Ack_2180 Ack_2180 Ack_2180 Len=0 MSS=1460 SACK_PE88=3 http: Ack_2180 A
45 46 47 48 49 30 52 53 54 55 54 55 56 57 58 59	22 22 22 29. 506444 22 20 29.29. 806276 22 20 29.29. 812877 22 20 29.29. 812877 22 20 29.49.4428 22 20 29.44428 22 20 29.44468 22 20 29.541681 22 20 29.541681 22 20 29.541681 22 20 25.54589 22 20 25.54698 22 20 25.54698 22 20 25.54698	372, 29.0, 316 372, 29.0, 316 372, 29.0, 316 378, 318, 218, 138, 156 372, 39.0, 318, 156 372, 39.0, 318, 156 372, 29.0, 316 372, 39.0, 316 372, 37, 37, 37, 37, 37, 37, 37, 37, 37, 37	$\begin{array}{c} 376, 216, 215, 136\\ 778, 218, 215, 136\\ 778, 218, 215, 136\\ 777, 210, 0, 136\\ 777, 210, 0, 136\\ 777, 120, 0, 136\\ 778, 128, 225, 136\\ 778, 128, 235, 136\\ 778, 128, 235, 136\\ 778, 128, 235, 136\\ 75, 75, 75, 75\\ 75, 75, 75, 75\\ 75, 75, 75, 75\\ 75, 75, 75, 75\\ 75, 75, 75, 75\\ 75, 75, 75, 75\\ 75, 75, 75\\ 75, 75, 75\\ 75, 75, 75\\ 75, 75, 75\\ 75, 75, 75\\ 75, 75, 75\\ 75, 75\\ 75, 75\\ 75, 75\\ 75, 75\\ 75, 75\\ 75, 75\\ 75, 75\\ 75, 75\\ 75, 75\\ 75\\ 75, 75\\ 75\\ 75\\ 75\\ 75\\ 75\\ 75\\ 75\\ 75\\ 75\\$	TCP TCP TCP TCP TCP TCP ENTP TCP CAS DAS DAS DAS DAS DAS	dellperaphis > http: [Ack] Sep-28 Ack-120 with-0272 Len-0 dellperaphis > http: [SN] Sep-0 Win-64240 Len-0 MSS-1460 SACK_FERM-3 http: > dellperaphis [Ack] Sep-0 Win-64240 Len-0 MSS-1460 SACK_FERM-3 http: > dellperaphis [Ack] Sep-0 Ack-14 Win-60330 Len-0 MSS-1460 SACK_FERM-3 http: > dellperaphis [Ack] Sep-0 Ack-14 Win-60330 Len-0 MSS-1460 SACK_FERM-1 eps > http: [Ack] Sep-1 Ack-14 Win-60330 Len-0 Act //228054270xx1[300] MSB-01 Win-65351 Len-0 Sep > http: [Ack] Sep-1 Ack-14 Win-60330 Len-0 MSS-1400 SiteConstrained Sack 14Win-60330 Len-0 MSS-1400 SiteConstrained Sack 14Win-60330 Len-0 MSS-1400 SiteConstrained Sack 14Win-60330 Len-0 Standard query & disconstrained Sack 14Win-60330 Len-0 Standard query & disconstrained Sack 14Win-60340 Sack_PERM-1 Standard query & disconstrained Sack 14Win-60340 Sack_PERM-1

The bot generates high volume traffic to thousands of websites with ads, sites serving as referrers, as well as pages filled with ad links (over 800 sessions a minute) for approximately 2 hours and then stops. Most serious advertising companies easily detect large clicks from the same ip and block it. The botnet owners limit clicks to just a few and compensate it by programming the bot to click on thousands of ads.

Time Graph of Session	Traffic (Sessions Per Minute)			
750	888 Sessions 2012-01-30 23:15			
suoissae				
250 Jull 44				
< 2012-01-30 22:17	4			

Click to enlarge. 11 hours of traffic monitoring. 2 hour spike following the infection.

Traffic capture - Using fake referrer (serch-direct.com) and passing fake search strings to the C&C, which responds with iframe redirect to the ad link.



There are hundreds of fake search and referrer sites in use in this case, starting from pages containing nothing but ad links and ending with several ip ranges serving iframe. The list of servers is below



Fake referrer = serch

The list of servers serving iframe content is limited to several 108.59.x.x ranges.

They all are hosted

108.59.4.128/27 108.59.7.0/27 108.59.13.160/27

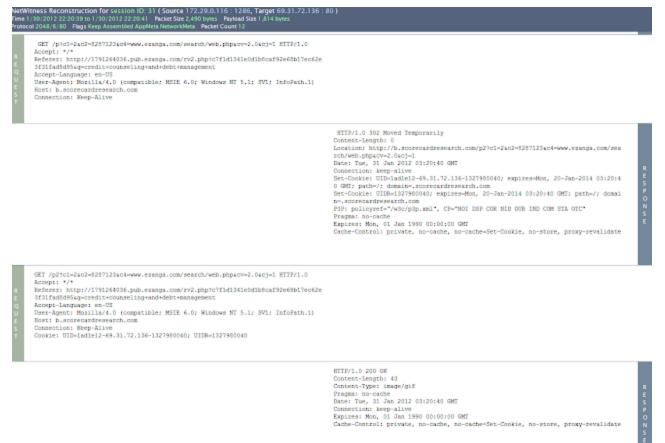
In all cases the registration information is as follows:

### DOMAINS:

hosted-by.leaseweb.com WhoisGuard WhoisGuard Protected () Fax: 11400 W. Olympic Blvd. Suite 200 Los Angeles, CA 90064 United States

IPs: Private Customer Private Residence Bryansk 241000 Russian Federation

In some cases, legitimate "traffic quality" providers were used as referrers, such as ezanga.com



GIF89a!,D;

The list of hosts involved (if you think you might be a PPC fraud victim, see if you are in the

list. ( I had to remove the list because it attracts too many false search result cluicks - like black SEO of sorts)

Query strings used (includes Parner / affiliate IDs - who gets paid for this traffic. The number in brackets shows the number of times it was used) (I had to remove the list because it attracts too many false search result cluicks - like black SEO of sorts)