

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

Archived: 2026-04-05 16:48:48 UTC

Distribution

The exploit host is [featured on CleanMX](#) . 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

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

File type: Win32 EXE

Detection ratio: 24 / 43

Analysis date: 2012-02-02 06:50:05 UTC (1 minute ago)

AntiVir TR/Alureon.FK.93 20120201

Avast Win32:Rootkit-gen [Rtk] 20120202

BitDefender Trojan.Generic.7154539 20120202

Comodo TrojWare.Win32.Trojan.Agent.Gen 20120202

DrWeb BackDoor.Tdss.5231 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 20120202 (TDSS Killer detects it as Pihar.b)

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

Description

You can read more detailed binary analysis on the ESET blog (Feb.2 2012) : ["TDL4 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 replacing kdcom.dll for x64)

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

```

1000668C      255B5E2E5D2E255B5E28+  SSZ1000669C_____?
1000668C      00                      db      'X[^.].X[^()Gt()D]',0
1000669F      00                      Align   4
100066A0      77616977400           SSZ100066A0_wait:
100066A5      00000000              db      'wait',0
100066A5      00000000              Align   4
100066A8      507572706C6548617065+ SSZ100066A8_PurpleHaze:
100066B3      00                      db      'PurpleHaze',0
100066B3      00                      Align   4
100066B4      70607C25737C25737C25+ SSZ100066B4_ph_s_s_s_s:
100066C3      00                      db      'ph!ze !ze !ze !ze',0
100066C3      00                      Align   4
100066C4      2D                      LI00066C4:
100066C5      00                      db      2Dh ; '-'
100066C6      00                      db      00h
100066C7      00                      db      00h
100066C8      00                      db      00h
100066C8      485454502F312E312032+ SSZ100066C8_HTTP_1_1_200_OK:
100066D0      00                      db      'HTTP/1.1 200 OK',0
100066D0      436F6E74656E742D5477+ SSZ100066D0_Content_Type__text_html:
100066E0      00                      db      'Content-Type: text/html',0
100066E0      436F6E74656E742D4C65+ SSZ100066E0_Content_Length__d:
10006703      00                      db      'Content-Length: xd',0
10006703      00                      Align   4
10006704      43616360652D436F6E74+ SSZ10006704_Cache_Control__must_revalidate__:
10006737      00                      db      'Cache-Control: must-revalidate, no-cache, no-store',0
10006737      00                      Align   4
10006738      507261676D613A206E6F+ SSZ10006738_Pragma__no_cache:
10006749      00000000              db      'Pragma: no-cache',0
10006749      00000000              Align   4
1000674C      457870697265733A2053+ SSZ1000674C_Expires__Sat_R1_Jan_2000_00_00_:
10006773      00                      db      'Expires: Sat. 01 Jan 2000 00:00:00 GMT',0
10006773      00                      Align   4
10006774      436F6E65656374696F6E+ SSZ10006774_Connection__close:
10006786      00000000              db      'Connection: close',0
10006786      00000000              Align   4
10006788      00                      LI0006788:

```

Purple Haze

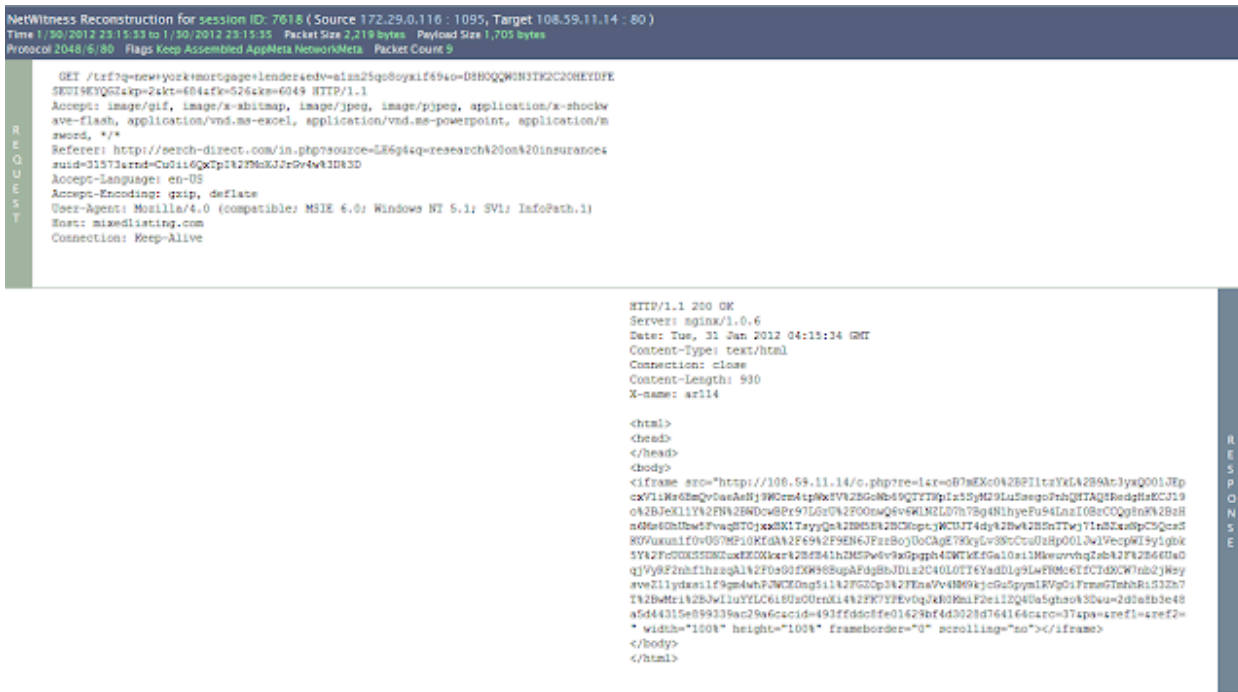
```
10006485 000000 Align 4
10006488 SSZ10006488_GlobalUserOffline:
10006488 476C6F62616C55736572+ db 'GlobalUserOffline',0
1000649A 0000 Align 4
1000649C SSZ1000649C_CertificateRevocation:
1000649C 43657274696669636174+ db 'CertificateRevocation',0
100064B2 0000 Align 4
100064B4 SSZ100064B4_WarnonBadCertReceiv:
100064B4 5761726E6F6E42616443+ db 'WarnonBadCertReceiv',0
100064C9 000000 Align 4
100064CC SSZ100064CC_WarnOnPost:
100064CC 5761726E4F6E506F7374+ db 'WarnOnPost',0
100064D7 00 Align 4
100064D8 SSZ100064D8_WarnOnPostRedirect:
100064D8 5761726E4F6E506F7374+ db 'WarnOnPostRedirect',0
100064EB 00 Align 4
100064EC SSZ100064EC_WarnonZoneCrossing:
100064EC 5761726E6F6E5A6F6E65+ db 'WarnonZoneCrossing',0
100064FF 00 Align 4
10006500 SSZ10006500_EnableHttp1_1:
10006500 456E61626C6548747470+ db 'EnableHttp1_1',0
1000650E 0000 Align 4
10006510 SSZ10006510_MaxHttpRedirects:
10006510 4D617848747470526564+ db 'MaxHttpRedirects',0
10006521 000000 Align 4
10006524 SSZ10006524_SecuritySafe:
10006524 53656375726974795361+ db 'SecuritySafe',0
10006531 000000 Align 4
10006534 L10006534:
```

Change IE settings

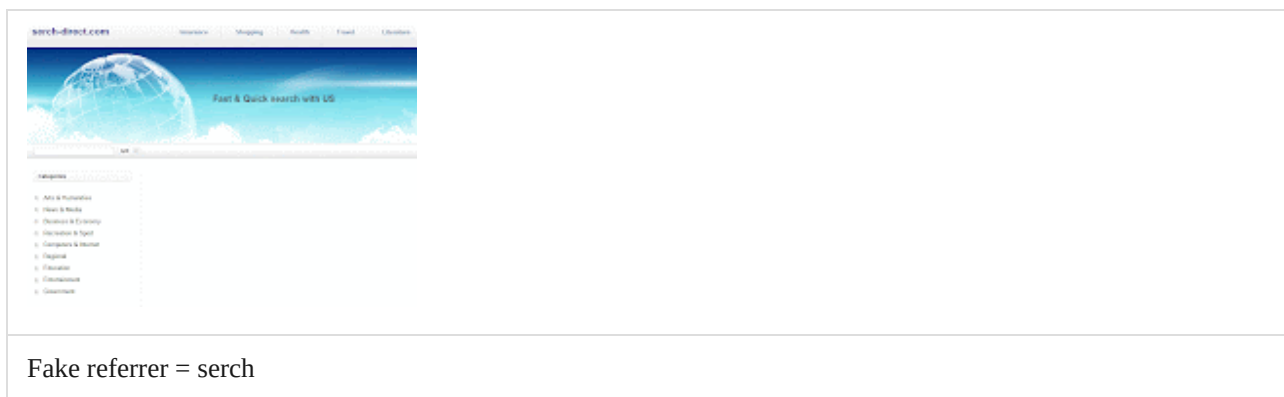
Traffic



"Advertising Botnet" by Securelist



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



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

```

NetWitness Reconstruction for session ID: 31 (Source 172.29.0.116:1286, Target 69.31.72.136:80)
Time 1/30/2012 22:20:39 to 1/30/2012 22:20:41 Packet Size 2,490 bytes Payload Size 1,814 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 12

```

| | | |
|---------------------------------|---|--------------------------------------|
| R E Q U E S T | <pre> GET /p?cl=2ac2=8287123&c4=www.ezanga.com/search/web.php?cv=2.0&cj=1 HTTP/1.0 Accept: */* Referer: http://1791244036.pub.ezanga.com/rv2.php?c?1d1341e0d1b8caf92e6817ec62e 3f31fad8d95q=credit+counseling+and+debt+management Accept-Language: en-US User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.1) Host: b.scorecardresearch.com Connection: Keep-Alive </pre> | |
| | <pre> HTTP/1.0 302 Moved Temporarily Content-Length: 0 Location: http://b.scorecardresearch.com/p?cl=2ac2=8287123&c4=www.ezanga.com/sea rch/web.php?cv=2.0&cj=1 Date: Tue, 31 Jan 2012 03:20:40 GMT Connection: keep-alive Set-Cookie: UID=1ad1e12-69.31.72.136-1327980040; expires=Mon, 20-Jan-2014 03:20:4 0 GMT; path=/; domain=.scorecardresearch.com Set-Cookie: UIDR=1327980040; expires=Mon, 20-Jan-2014 03:20:40 GMT; path=/; domai n=.scorecardresearch.com P3P: policyref="/w3o/p3p.xml", CP="NOI DSP COR NID OUR IMD COM STA OTC" Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Cache-Control: private, no-cache, no-cache=Set-Cookie, no-store, proxy-revalidate </pre> | R E S P O N S E |
| R E Q U E S T | <pre> GET /p?cl=2ac2=8287123&c4=www.ezanga.com/search/web.php?cv=2.0&cj=1 HTTP/1.0 Accept: */* Referer: http://1791244036.pub.ezanga.com/rv2.php?c?1d1341e0d1b8caf92e6817ec62e 3f31fad8d95q=credit+counseling+and+debt+management Accept-Language: en-US User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.1) Host: b.scorecardresearch.com Connection: Keep-Alive Cookie: UID=1ad1e12-69.31.72.136-1327980040; UIDR=1327980040 </pre> | |
| | <pre> HTTP/1.0 200 OK Content-Length: 43 Content-Type: image/gif Pragma: no-cache Date: Tue, 31 Jan 2012 03:20:40 GMT Connection: keep-alive Expires: Mon, 01 Jan 1990 00:00:00 GMT Cache-Control: private, no-cache, no-cache=Set-Cookie, no-store, proxy-revalidate GIF89a1,0: </pre> | R E S P O N S E |

Source: http://contagiodump.blogspot.com/2012/02/purple-haze-bootkit.html