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



### 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

## Desription

**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 replaceing kdcom.dll for x64)

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


**Purple Haze**

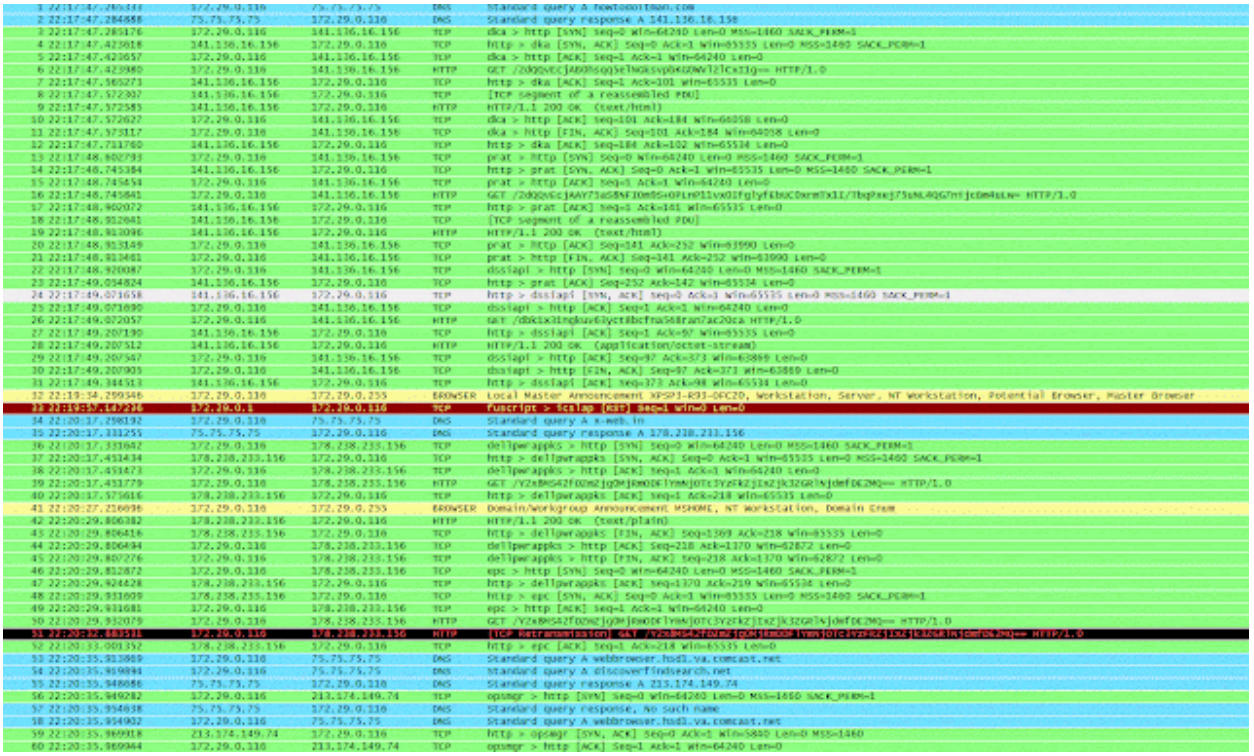
```
10006485  000000                          Align       4
10006488                        SSZ10006488_GlobalUserOffline:
10006488  476C6F62616C55736572+           db          'GlobalUserOffline',0
1000649A  0000                            Align       4
1000649C                        SSZ1000649C_CertificateRevocation:
1000649C  4365727469666963617+            db          'CertificateRevocation',0
100064B2  0000                            Align       4
100064B4                        SSZ100064B4_WarnonBadCertRecving:
100064B4  5761726E6F6E42616443+           db          'WarnonBadCertRecving',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  4D6178487474705265647+          db          'MaxHttpRedirects',0
10006521  000000                          Align       4
10006524                        SSZ10006524_SecuritySafe:
10006524  5365637572697479536+           db          'SecuritySafe',0
10006531  000000                          Align       4
10006534                        L10006534:
```

**Change IE settings**

## Traffic

"Advertising Botnet" by Securelist

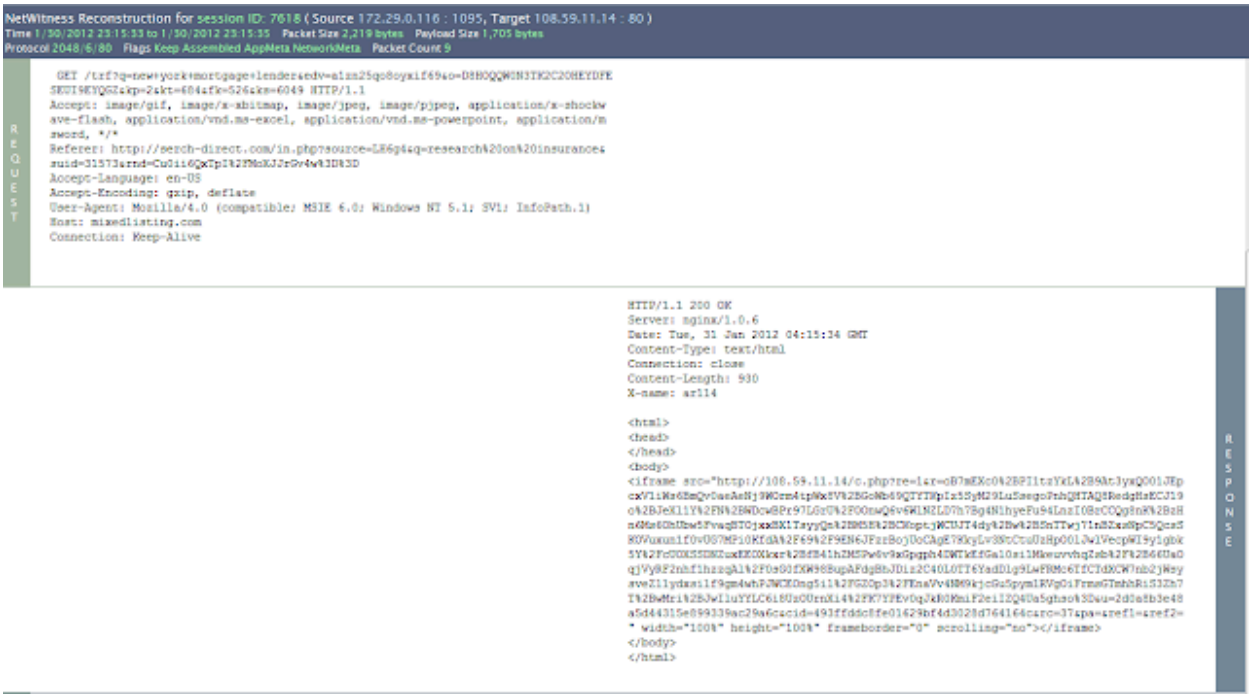
C&C check-in upon install



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.


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


---

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