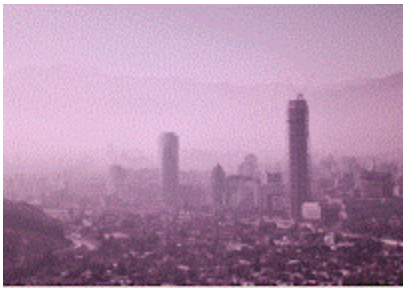
TDL4 - Purple Haze (Pihar) Variant - sample and analysis

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: "TDL4 reloaded: Purple Haze all in my brain" (edited by David Harley)
Eset also updated the removal tool for this variant - direct download link: OlmarikTDL4 remover

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

 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
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:

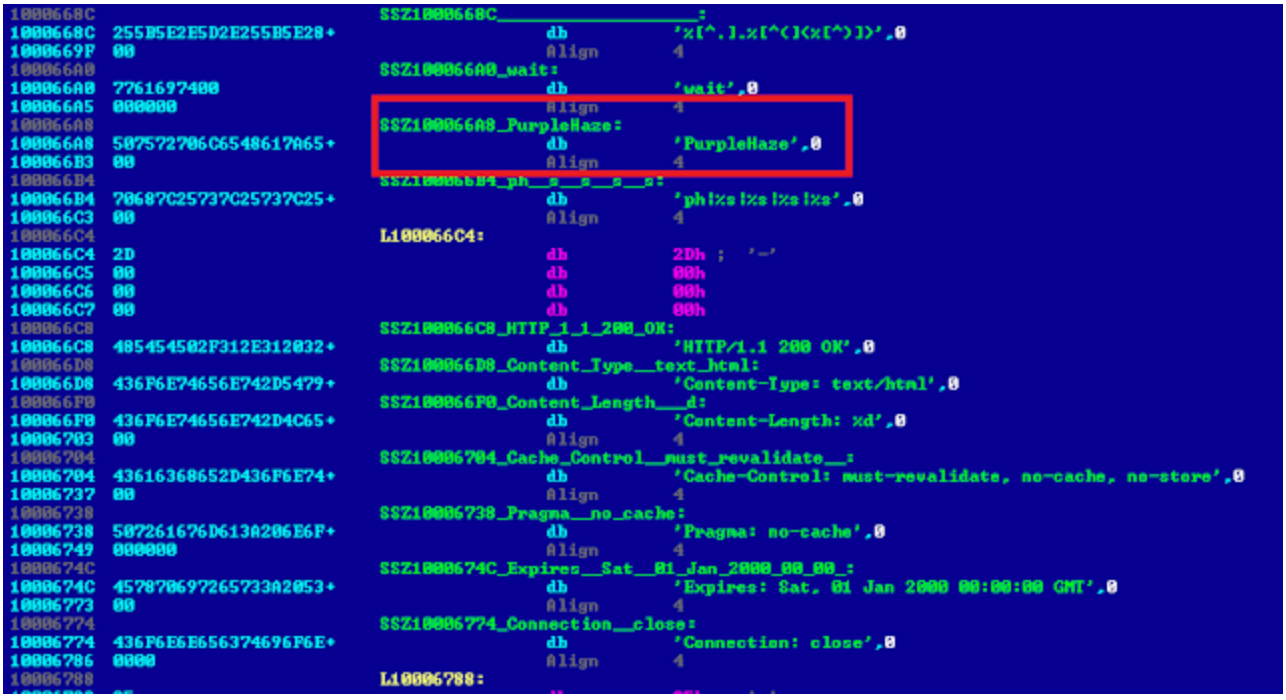
1. Phdata
   [PurpleHaze]
   pn=161
   all=ph.dll
   allx=phx.dll
   wait=3600
2. phm (original master boot record)
3. ph.dll (payload dll for x86)
4. phx.dll (payload dll for x64)

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.

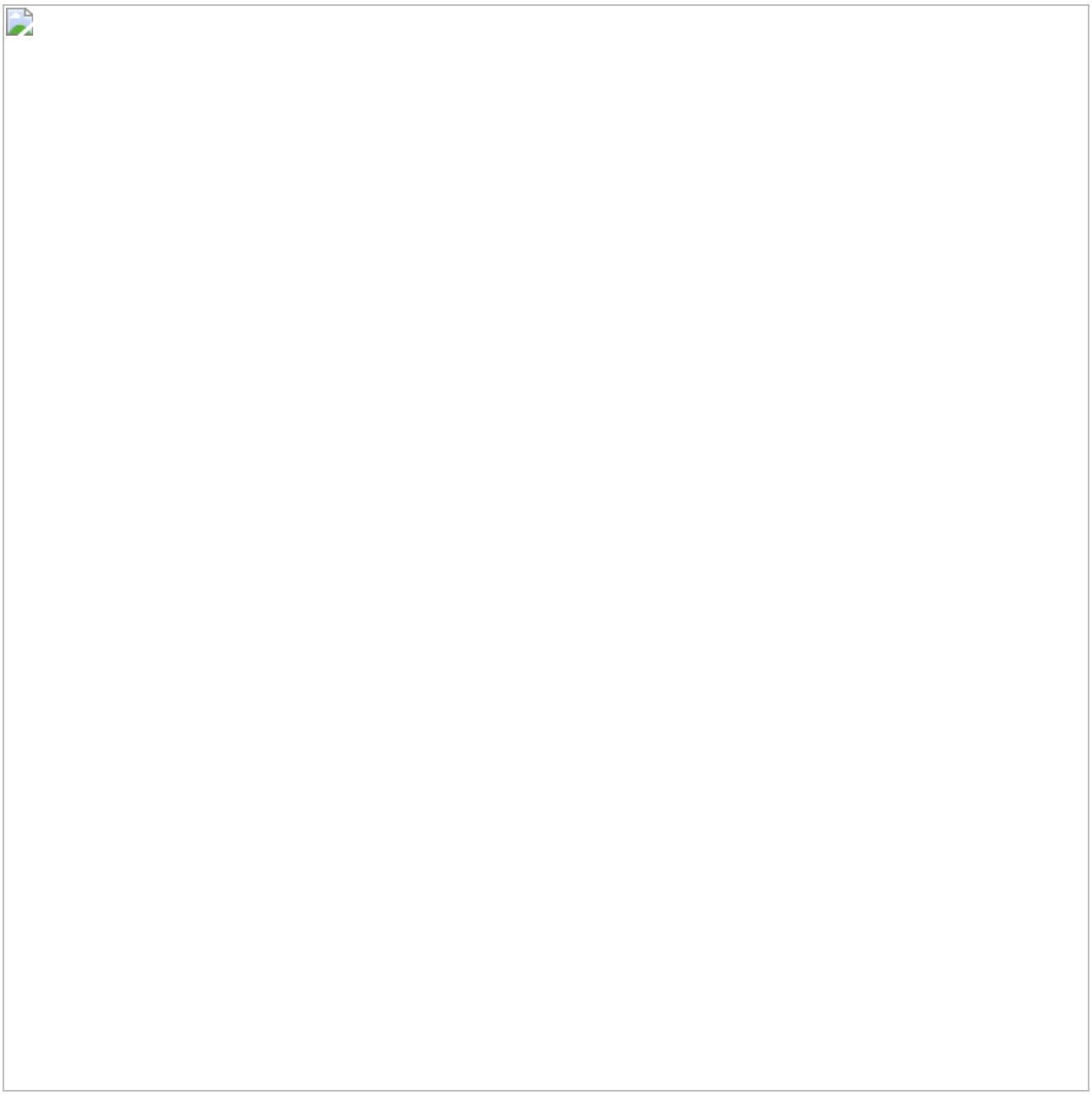


Purple Haze

Change IE settings

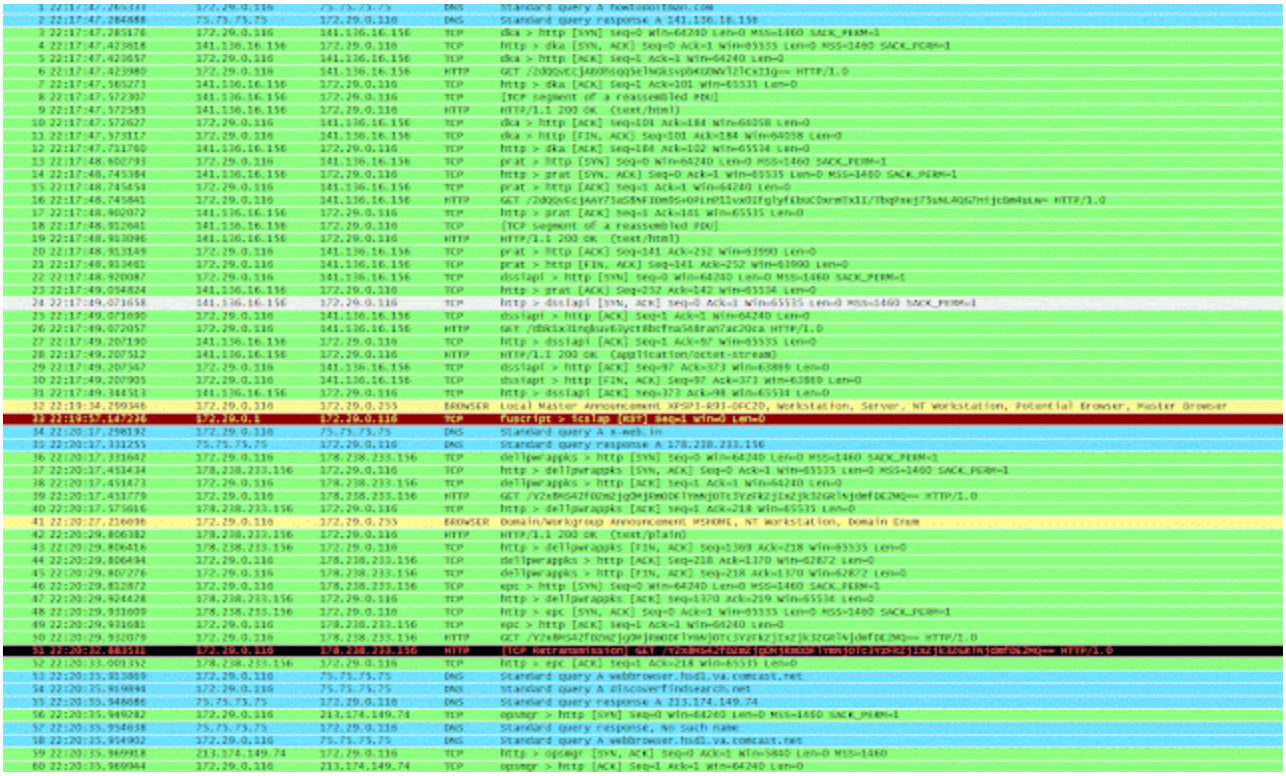
Traffic

Pay-per-click fraud generates significant revenue for the botnet owners. The ‘Advertising’ Botnet" article from Securelist explains the click fraud scheme in great detail.



"Advertising Botnet" by Securelist

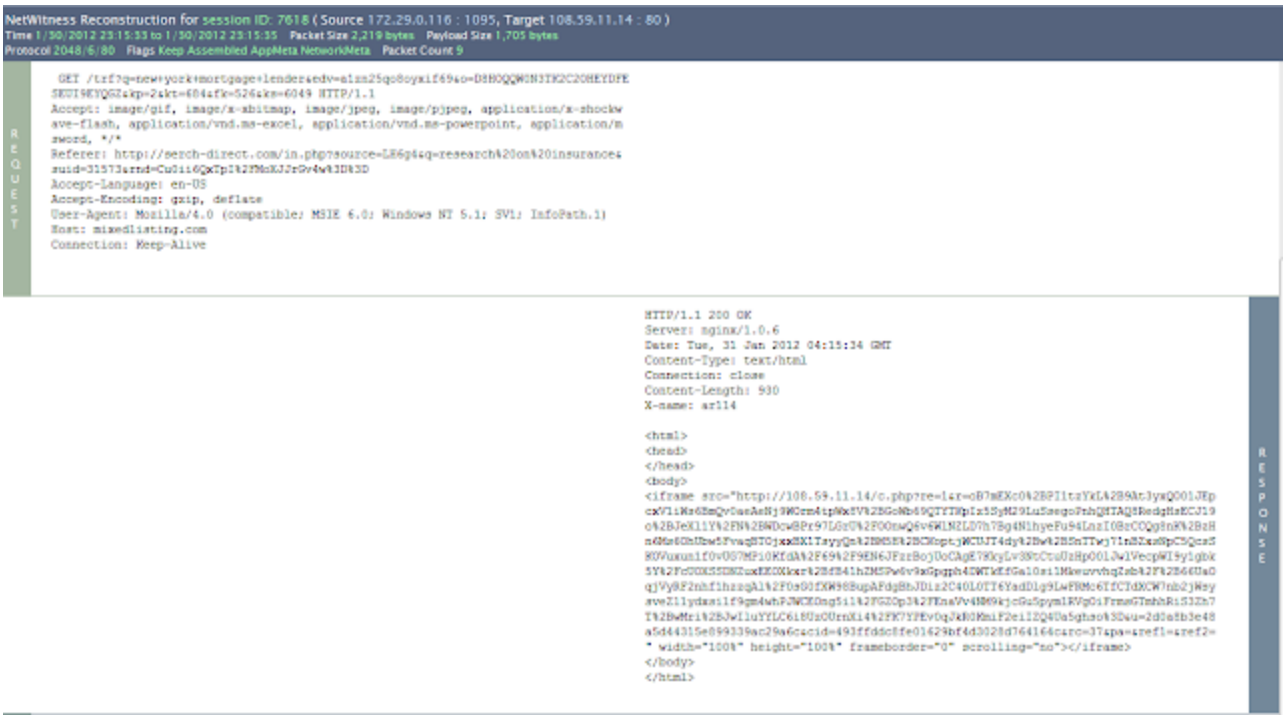
C&C check-in upon install



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

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)