A Forensic Review of TDSS

Tim Slaybaugh
US-CERT

June 18, 2012
Background

• TDSS first appeared in 2008.
• The authors of TDSS have rolled out four major version changes.
• TDSS Version 4 (TDL-4) first appeared around the end of July 2010.
• TDL-4 compromised nearly 4.5 million systems in its first three months (Kaspersky, TDL-4 Top Bot).
• According to the Shadowserver Foundation, TDL-4 continues to be one of the top four largest botnets currently active.
Characteristics of TDL-4

- Targets both 32 bit and 64 bit systems
- Survives reboot by modifying the Master Boot Record.
- Command and Control communication is RC4 encrypted and then base64 encoded.
- Intercepts and modifies the victim’s communications to the Internet.
- Stores its payload in Unused Disk Space and actively hides the data from the victim.
- Partners with a variety of malicious programs designed for revenue generation.
Characteristics of TDL-4

• The TDL-4 configuration contains modules designed for revenue generation.
• Search Engine Optimization (SEO) intercepts search engine queries and returns modified results linked to additional malware.
• Pay-per-Click function redirects the browser to servers hosting pay-per-click links.
• HTML documents downloaded by the victim may have ‘iframe’ or ‘object’ tags modified to link to additional malicious site.
Example of SEO

- **Connection to SEO Server:**
  - http://rollangarr0s.com/kam19t5d5E3mQiU7dmVyPTMuOTYmYmlkPWU4ZjE1YTM2MTBjNjE4YWE5MTbiMzk0MmU2YmRjYWRIeNDQzN2ZiZTMmYWI1PTMwMDAxJnNpZD0wJnJkPTAmZW5nPXd3dy5nb29nbGUuY29tJnE9aW1nYnVybg==

- **Translated from base64:**
  - ???????]??M?B%:ver=3.96&bid=e8f15a3610c618aa918b3942e6bdca4b437f6be3&aid=30001&sid=0&rd=0&eng=www.google.com&q=imgburn

- The request contains the Bot ID number, Affiliate ID number, search engine and the search term.
Characteristics of TDL-4

• To increase distribution of the bot, TDSS will partner with other affiliates.
Characteristics of TDL-4

One indicator of TDSS is the presence of unwanted or persistent software applications. A large number of programs can be introduced in the same manner as TDSS.
Notes on Analysis

• The victim systems in each analyzed case were running Windows XP with Service Pack 3. Windows XP is currently run on 43% of all personal computers, making it currently the largest distributed operating system in the world.

• Analysis was conducted on multiple systems from production networks as well as several systems in controlled environments.
Master Boot Record (MBR)

- This is an ASCII representation of a normal Master Boot Record. Note the standard Windows error messages.
Master Boot Record (MBR)

Samples of boot records overwritten with malicious code.

- **Modified Boot Record [1]:**
  - 3@·P<·@·X·>·|···9·|·s$Ph·-K{'9G·=*·RN·EbzD·-p·8&·-hb@·-#·-u·G·!·a·7&·-5A7·-#·-3b·A·Xh·-L·0·}{·bAJ@Oi!·S·0·+7Bj·-t·X·3·G·O·-p·Q·L·1R·F·G·-3·t·q·L·@3J@G@·-@·K·zh·E·-pnLu·-·b·v·y·}C·:Qx·-21|T6d·DkNpD6d·-#·YW·$·-k·xWn"<r·"G7@zE·]·@p5xd·-@7@D·a"q'8··c"5'8"·r·"u'8·S0vby(ll·0·-lWV·-f·0·s]|"p·Gh·J·L8pb·-uy1}@·@>T·-jl·-l·-J·@y·O·-jja·'·X·ing
  - system

- **Modified Boot Record [2]:**
  - 1@·P<·-f·-f·-F·-F·-4H·-~M·0P·-x·-..!·-A·-#·-|·-h·-e·}9·-f1[hx·6·-F·-D·-fa·-Kf·Wf·6·-f·-F·-f·6·-f·F·f·E·f·f@f]F·-F·-E·-F·4B·-~m·0R·-1@·-8h·-B·-B·-B·-h·-F·-Nu·)V·-V·-Cu1@·C·V·-Ab·-v·-v·C·-B·-h·-i0m
  - OB·-&0·-FJu_f·-f·-M·-f·-7V·-y·-0S·-#·-f·u·-f1[@f·E·fwP·-g2·-fB3·-fQhs·-f5·-8m·-KuqbgfwPff[9X0CupfaC·H·G·-B·-B·-B·-Cf·-N·-f·X·@·E·-k}f·E·8·h·-U·-s&·}·\t·c·a·G)Bwm0Ni·-AN·-D·-"-~"-YWAs$ac·-cE·-YWfaCtk}booth..................#+A·-~#?·-hth·-~h·-~h·-mh·-?·-................U*
Prefetch

TDSS may use the name of a legitimate file.

<table>
<thead>
<tr>
<th>File Name</th>
<th>Date/Time</th>
<th>Size</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNREGMP2.EXE-3AE687B3.pf</td>
<td>Apr 5, 2012 2:19 AM</td>
<td>12 KB</td>
<td>ICC Profile</td>
</tr>
<tr>
<td>UNREGMP2.EXE-07CACB61.pf</td>
<td>Feb 10, 2012 6:39 PM</td>
<td>29 KB</td>
<td>ICC Profile</td>
</tr>
</tbody>
</table>

Path to the legitimate file:

\DEVICE\HARDDISK\VOLUME1\WINDOWS\INF\UNREGMP2.EXE

Path to the malicious file:

\DEVICE\HARDDISK\VOLUME1\DOCUME~1\USER01\LOCALS~1\TEMP\UNREGMP2.EXE
Firewall Logs

• DNS Changer – a TDSS module.
• DNS Changer activity in the pfirewall.log can be an indicator that the Tcpip registry settings may have been modified.

- 012-03-23 12:30:09 OPEN UDP 192.168.1.20 93.188.162.136 1025 53 - - - - - - - - -
- 2012-03-23 12:30:14 OPEN UDP 192.168.1.20 93.188.162.136 1029 53 - - - - - - - - -
- 2012-03-23 12:30:10 OPEN UDP 192.168.1.20 93.188.160.16 1025 53 - - - - - - - - -
- 2012-03-23 12:30:15 OPEN UDP 192.168.1.20 93.188.160.16 1029 53 - - - - - - - - -
- 2012-03-23 12:31:20 OPEN TCP 192.168.1.20 192.168.1.100 1036 80 - - - - - - - - -
- 2012-03-23 12:31:23 CLOSE UDP 192.168.1.20 192.168.1.50 137 137 - - - - - - - - -
Registry

The DNS Changer module of TDSS modifies HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DefaultGateway</td>
<td>REG_MULTI</td>
<td>192.168.1.1</td>
</tr>
<tr>
<td>DefaultGatewayMetric</td>
<td>REG_MULTI</td>
<td>0</td>
</tr>
<tr>
<td>NameServer</td>
<td>REG_SZ</td>
<td>93.188.162.136, 93.188.160.16</td>
</tr>
<tr>
<td>Domain</td>
<td>REG_SZ</td>
<td></td>
</tr>
<tr>
<td>RegistrationEnabled</td>
<td>REG_DWORD</td>
<td>0x00000001</td>
</tr>
<tr>
<td>RegisterAdapterName</td>
<td>REG_DWORD</td>
<td>0x00000000</td>
</tr>
<tr>
<td>TCPAllowedPorts</td>
<td>REG_MULTI</td>
<td>0</td>
</tr>
<tr>
<td>UDPAllowedPorts</td>
<td>REG_MULTI</td>
<td>0</td>
</tr>
<tr>
<td>RawIPAllowedProtocols</td>
<td>REG_MULTI</td>
<td>0</td>
</tr>
<tr>
<td>NTEContextList</td>
<td>REG_MULTI</td>
<td>0x00000000</td>
</tr>
<tr>
<td>DhcpClassIdBin</td>
<td>REG_BINARY</td>
<td>00 00 00 00</td>
</tr>
<tr>
<td>DhcpNameServer</td>
<td>REG_SZ</td>
<td>93.188.162.136, 93.188.160.16</td>
</tr>
</tbody>
</table>
Registry

• Many of the affiliate programs will create processes in the System registry that appear to have legitimate names. Suspicious processes may be identified by simple misspellings and by correlating other events on the system:

HKLM\SYSTEM\ControlSet001\Services\itlperf   ImagePath
REG_EXPAND_SZ   %SystemRoot%\System32\svchost.exe -k itlsvc
HKLM\SYSTEM\ControlSet001\Services\itlperf   DisplayName
REG_SZ   Intel CPU
HKLM\SYSTEM\ControlSet001\Services\itlperf   ObjectName
REG_SZ   LocalSystem
HKLM\SYSTEM\ControlSet001\Services\itlperf   Description
REG_SZ   Intel CPU perfermons service.
Event Correlation

Event correlation tools like ‘log2timeline’ (Kristinn Gudjonsson) can help to link processes to other malicious activity on the system.

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Type</th>
<th>Event Type</th>
<th>Time Generated/Written</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/5/2011</td>
<td>14:15:43</td>
<td>MACB</td>
<td>EVT Event Log</td>
<td>Last Written</td>
<td>Service Control Manager/7036;Info;Intel CPU - running</td>
</tr>
<tr>
<td>4/5/2011</td>
<td>14:15:43</td>
<td>MACB</td>
<td>REG SYSTEM key</td>
<td>Last Written</td>
<td>/ControlSet001/Enum/Root/LEGACY_ITLPERF</td>
</tr>
<tr>
<td>4/5/2011</td>
<td>14:15:43</td>
<td>MACB</td>
<td>REG SYSTEM key</td>
<td>Last Written</td>
<td>/ControlSet002/Enum/Root/LEGACY_ITLPERF</td>
</tr>
<tr>
<td>4/5/2011</td>
<td>14:15:43</td>
<td>MACB</td>
<td>REG SYSTEM key</td>
<td>Last Written</td>
<td>/ControlSet002/Enum/Root/LEGACY_ITLPERF</td>
</tr>
<tr>
<td>4/5/2011</td>
<td>14:15:43</td>
<td>MACB</td>
<td>REG SYSTEM key</td>
<td>Last Written</td>
<td>/ControlSet001/Enum/Root/LEGACY_ITLPERF</td>
</tr>
</tbody>
</table>
Event Logs

- This process could easily be overlooked if not correlated with other activity on the system.

Event:
- Date: 4/6/2011
- Source: Service Control Manager
- Time: 9:35:39 AM
- Category: None
- Type: Information
- Event ID: 7036
- User: N/A
- Computer: [Redacted]

Description:
The Windows License Provider service entered the running state.

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.
Registry

This process appears to have a benign name however it is linked to an affiliated program of TDSS that sets up a proxy service on the victim’s system:

- `$$$PROTO.HIV\ControlSet001\Services\6to4` 
  ImagePath
  
  `REG_EXPAND_SZ \ %SystemRoot%\System32\svchost.exe -k netsvcs`

- `$$$PROTO.HIV\ControlSet001\Services\6to4` 
  DisplayName
  
  `REG_SZ Windows License Provider`

- `$$$PROTO.HIV\ControlSet001\Services\6to4` 
  ObjectName
  
  `REG_SZ LocalSystem`

- `$$$PROTO.HIV\ControlSet001\Services\6to4` 
  Description
  
  `REG_SZ Windows License Provider`
Event Logs

- Event Logs may often report Internet activity from TDSS affiliate programs:

```
Event

Date: 4/15/2011  Source: Symantec AntiVirus
Time: 9:19:52 AM  Category: None
Type: Error  Event ID: 51
User: N/A  Computer:

Description:
The description for Event ID 51 in Source (Symantec AntiVirus) cannot be found. The local computer may not have the necessary registry information or message DLL files to display messages from a remote computer. You may be able to use the /AUXSOURCE=C flag to retrieve this description; see Help and Support for details. The following information is part of the event:

```
Event Logs

Antivirus may identify downloaders associated with TDSS.

```
remote computer. You may be able to use the /AUXSOURCE= flag to retrieve this description; see Help and Support for details. The following information is part of the event:

Security Risk Found! Trojan.Zefarchigen5 in File: c:\Documents and Settings\Administrator\Local Settings\Temp\csxanewomr.tmp by:
Manual scan. Action: Cleaned by Deletion. Action Description: The file was deleted successfully.
```
Antivirus Logs

Alerts on downloaders and malware from affiliate programs can be indicators of a more serious infection on the system:

Begin Resource Scan
Scan ID:(F4E5BE9D-B5F4-40EE-AD70-9B759EFF407B)
Scan Source:8
Start Time:Tue Apr 05 2011 10:44:35
End Time:Tue Apr 05 2011 10:44:39
Explicit resource to scan
Resource Schema:file
Resource Path:C:\DOCUME~1\LOCALS~1\Temp\onwrsamcex.tmp-->(UPX)
Result Count:1
Threat Name: TrojanDownloader:Win32/Harnig.S
ID:2147638405
Severity:5
Number of Resources:2
Resource Schema:file
Resource Path:C:\Documents and Settings\Local Settings\Temp\onwrsamcex.tmp-->(UPX:
Extended Info:141256735666330
Resource Schema:containerfile
Resource Path:C:\Documents and Settings\Local Settings\Temp\onwrsamcex.tmp
Extended Info:0
End Scan

---------------------------------------------
Internet History

- This activity was associated with a pay-per-click ad fraud program affiliated with TDSS.

<table>
<thead>
<tr>
<th>system</th>
<th>10</th>
<th><a href="http://www.inmotionhosting.com/?id=devilboy77">http://www.inmotionhosting.com/?id=devilboy77</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>10</td>
<td><a href="http://www.webhostingpad.com/">http://www.webhostingpad.com/</a></td>
</tr>
<tr>
<td>system</td>
<td>10</td>
<td><a href="http://www.hostgator.com/">http://www.hostgator.com/</a></td>
</tr>
<tr>
<td>system</td>
<td>10</td>
<td><a href="http://www.hostrocket.com/">http://www.hostrocket.com/</a></td>
</tr>
<tr>
<td>system</td>
<td>10</td>
<td><a href="http://adultfriendfinder.com/go/g1243200">http://adultfriendfinder.com/go/g1243200</a></td>
</tr>
<tr>
<td>system</td>
<td>10</td>
<td><a href="http://adultfriendfinder.com/go/g1243200-pct">http://adultfriendfinder.com/go/g1243200-pct</a></td>
</tr>
<tr>
<td>system</td>
<td>10</td>
<td><a href="http://www.mobilemonopoly.com/?hop=devilboy77">http://www.mobilemonopoly.com/?hop=devilboy77</a></td>
</tr>
<tr>
<td>system</td>
<td>10</td>
<td><a href="http://www.dnforum.com/plans.php">http://www.dnforum.com/plans.php</a></td>
</tr>
<tr>
<td>system</td>
<td>10</td>
<td><a href="http://www.hostmonster.com/">http://www.hostmonster.com/</a></td>
</tr>
<tr>
<td>system</td>
<td>10</td>
<td><a href="http://www.bloggingtothebank.com/">http://www.bloggingtothebank.com/</a></td>
</tr>
<tr>
<td>system</td>
<td>10</td>
<td><a href="http://adultfriendfinder.com/go/g1243200-pmo">http://adultfriendfinder.com/go/g1243200-pmo</a></td>
</tr>
<tr>
<td>system</td>
<td>10</td>
<td><a href="http://indianfriendfinder.com/go/g1243200">http://indianfriendfinder.com/go/g1243200</a>.</td>
</tr>
</tbody>
</table>
Activity associated with TDSS is often identifiable by reviewing network traffic:
<table>
<thead>
<tr>
<th>IP Address</th>
<th>User Agent</th>
<th>Operating System</th>
<th>Date/Time</th>
<th>Server Name</th>
<th>Protocol</th>
<th>Port</th>
<th>Source/Target</th>
<th>Req ID</th>
<th>Compression</th>
<th>Domain Associated with TDSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.32.188</td>
<td>anonymous</td>
<td>Mozilla/4.0 (compatible; MSIE 1.0; Windows NT; CMD3)</td>
<td>2011-05-06 19:16:21</td>
<td>w3proxy SERVER</td>
<td>-</td>
<td>ch01cilewk.com</td>
<td>192.168.32.146</td>
<td>443</td>
<td>-</td>
<td>662 SSL-tunnel TCP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Inet</td>
<td>407</td>
<td>ch01cilewk.com:443</td>
<td></td>
<td></td>
<td>Internal</td>
</tr>
</tbody>
</table>

Domain associated with TDSS.

Unique UserAgent strings associated with TDSS.

Unique strings and domain names can be used to create detection rules addressed later.
Restore Point Forensics

Analysis of the Restore Point uncovers a malicious DLL previously stored in the Print Processor Provider directory. The file is indexed in a change.log file as ‘A0005311.dll’ and a copy is placed in the RP## folder.

- `\Device\HarddiskVolume1\System Volume Information\_restore\3`
- `8.6F7BBDF-8A8-4781-966A-44870EBF3F97\RP14\change.log\p`...
- `[««`...
- `...\Windows\system32\spool\prtpr...
- `ocs\w32x86\OC17\uOCE\d\l\l"...A0005311\d\l\l`
CollectedData_##.xml

This malicious DLL is linked to the ‘root’ Namespace indicating it runs with system level privileges. The ‘Win32_StartupCommand’ class indicates a command that runs automatically when a user logs on to a system.

- `<NAMESPACE NAME="root" />
- `<NAMESPACE NAME="cimv2" />
- `</LOCALNAMESPACEPATH>
- `</NAMESPACEPATH>
- `<INSTANCE NAME="Win32_StartupCommand">
  - `<KEYBINDING NAME="Command">
    - `<KEYVALUE VALUETYPE="string">rundll32.exe "C:\WINDOWS\anitahefozujezecaz.dll",Startup</KEYVALUE>`
Task Scheduler

This task was scheduled each time a reboot occurred. The job executed a file in the victim’s %Application Data% folder which called back to the C2 domain.

- "Task Scheduler Service"
  - Started at 3/23/2012 10:57:02 AM
- "a4e50120.job" (a4e50120.exe)
  - Started 3/23/2012 12:26:11 PM
  - Finished 3/23/2012 12:26:12 PM
  - Result: The task completed with an exit code of (0).
hosts file

This excerpt from the hosts file will redirect all searches in Google to the malicious host at 93.186.119.129:

- 93.186.119.129 www.google.com
- 93.186.119.129 google.com
- 93.186.119.129 google.com.au
- 93.186.119.129 www.google.com.au
- 93.186.119.129 google.be
- 93.186.119.129 www.google.be
- 93.186.119.129 google.com.br
- 93.186.119.129 www.google.com.br
- 93.186.119.129 google.ca
- 93.186.119.129 www.google.ca
Unused Disk Area

• TDSS often places its configuration data in the Unused Disk Area outside of partitioned space.

  • 00062A95 00062A95 0 <BtB.f
  • 00062C06 00062C06 0 [PurpleHaze]
  • 00062C14 00062C14 0 pn=161
  • 00062C1C 00062C1C 0 all=ph.dll
  • 00062C28 00062C28 0 allx=phx.dll
  • 00062C36 00062C36 0 wait=3600
  • <snip>
  • 000640C8 000640C8 0 {%08x-%04x-%04x-%04x-%04x%08x}
  • 00064332 00064332 0 *\..\globalroot%S
  • 0006434A 0006434A 0 PurpleHaze
  • 0006438A 0006438A 0 LoadLibraryExA
  • 0006439A 0006439A 0 GetProcAddress
  • 000643AA 000643AA 0 VirtualFree
  • 00064883 00064883 0 A\A\]
Unallocated Space

• Internet History carved from Unallocated Space.
• The server at clckil.com hosted multiple pay-per-click ad fraud links.

e7u7QyRU15671d82c38662d965
e86546394c0f93617A&xref=http://cornishrexe.org/
key/?qs=57d2776c56a7146bb643
eeafc20869102dfb524db6e6d9878ff0e9471df0b810e00ac0eboa2df50a86d6083c3b38c3df4
3&t=toconsolidatedebt.........................3Dc--------------------Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap
This data was recovered from the pagefile by searching for the physical path.
References to the domain, ‘esbigholtem.com’ are only found in memory or the pagefile.

- HKU\DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\esbigholtem.com

References to the domain, ‘esbigholtem.com’ are only found in memory or the pagefile.
Live Memory Forensics

• Malicious code injected into svchost.exe
## Live Memory Forensics

<table>
<thead>
<tr>
<th>Name</th>
<th>Pid</th>
<th>Start</th>
<th>End</th>
<th>Tag</th>
<th>Hits</th>
<th>Protect</th>
<th>Protect</th>
</tr>
</thead>
<tbody>
<tr>
<td>csrss.exe</td>
<td>680</td>
<td>0x00270000</td>
<td>0x0027AFFF</td>
<td>VadS</td>
<td>0</td>
<td>6 (MM_EXECUTE_READWRITE)</td>
<td></td>
</tr>
<tr>
<td>Dumped to:</td>
<td></td>
<td>/tmp/crss.exe,a5db1f8,00270000-0027afff,dmp</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x00270000</td>
<td>d4</td>
<td>5a 00 00</td>
<td>03 00 00</td>
<td>04 00 00</td>
<td>ff ff 00 00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x00270010</td>
<td>b8</td>
<td>00 00 00</td>
<td>00 00 00</td>
<td>00 00 00</td>
<td>40 00 00 00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x00270020</td>
<td>00</td>
<td>00 00 00</td>
<td>00 00 00</td>
<td>00 00 00</td>
<td>00 00 00 00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x00270030</td>
<td>00</td>
<td>00 00 00</td>
<td>00 00 00</td>
<td>00 00 00</td>
<td>00 00 00 00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x00270040</td>
<td>0e</td>
<td>1f ba 0e</td>
<td>00 b4 09</td>
<td>cd 21 b8</td>
<td>01 4c cd 21 54 68</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x00270050</td>
<td>69</td>
<td>73 20 70</td>
<td>70 6f 67</td>
<td>67 72 61 6d</td>
<td>20 63 61 6e 6e 6f</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x00270060</td>
<td>74</td>
<td>20 62 65</td>
<td>20 72 75</td>
<td>6e 20 69 6e</td>
<td>20 44 4f 53 20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x00270070</td>
<td>6d</td>
<td>6f 64 65 2e</td>
<td>0d 0d 0a 24</td>
<td>00 00 00 00</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

The program cannot be run in DOS mode. $........
Snort Rules

This rule looks for unique items in the UserAgent string, such as ‘MSIE 1.0’ and ‘CMD3’

- alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN"
  Possible TDSS User-Agent seen with HTTP CONNECT Traffic";
  flow:established,to_server; content:"CONNECT"; http_method;
  content:"User-Agent|3a| Mozilla/4.0 (compatible|3b| MSIE 1.0|3b| Windows NT|3b| CMD3)"; http_header; classtype:trojan-activity;)

20th Annual FIRST Conference
MALTA
17 - 22 June 2012
Snort Rules

This rule will detect one of the base64 encoded string associated with TDSS ‘GET’ requests

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN TDSS/TDL/Alureon MBR rootkit Checkin";
flow:established,to_server; content:"GET"; nocase; http_method; content:"HTTP/1."; content:"|0d 0a|Accept-Language|3a| "; distance:1; within:19;
content:"User-Agent|3a| Mozilla/4.0 |28|compatible|3b| MSIE";
fast_pattern:23,18; http_header; content:"Host|3a| "; distance:0;
http_header; content:"|3a| no-cache"; distance:0; http_header;
content:"!"Accept|3a| "; http_header; pcre:"/^\/[a-z0-9+\=]{16,400}$/Ui";
classstype:trojan-activity; sid:2011894; rev:15;)

References

Questions/Comments?