security is not an island
HILTONMALTA

24th Annual FIRST Conference

MALTA

17 - 22 June 2012

FIRST

Improving Security Together

A Forensic Review of TDSS

Tim Slaybaugh
US-CERT

June 18, 2012

24th Annual FIRST Conference
MALTA
17 - 22 June 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/kam19t5d5E3mQiU7dmVyPTMuOTYmYmlkPWU4ZjE1YTM2MTBjNjE4YWE5MThiMzk0MmU2YmRjYWRiNDQzN2ZiZTMmYWlkPTMwMDAxJnNpZD0wJnJkPTAmZW5nPXd3dy5nb29nbGUuY29tJnE9aW1nYnVybg==
- Translated from base64:
- ?????]?M?B%;ver=3.96&bid=e8f15a3610c618aa918b3942e6bdcadb4437fbe3&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)

- 3@·P<·|{P·P·|>·|···PW9e·s$K=>·1·8n·| u··E·btM··u·F·It·8,tv 5·4··p,<·t|;··4·M·kr·N·hF·s*~F··~··t··~··t· 6·uR·F···F···V
- ·h!·s· 6·k<·>~}U*t··~··tH 7·k)·|·W·uK···
- V·4·M·r#A$?·^
- |Cwc·Q·V1·RnBwb9V
- w#r·9F·s·8··;·|·N··V·M·sQOtN2dV·M·kd
- V·`;*U4AM·r6·{U*u0vA·t+a`j·j·□v
- □v·j·h·|j·j·4B·tM·aas·Ot·2d
- V·M·kVayCInvalid partition table·Error loading operating system·Missing operating system·····,Dc*CR+·····~□□?····dP ·····U*

- 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·fG···3□I···q`· L@3J@G@···@··K·zh·E·.pnLu··/··
·b□·v·y··}C:>Qx·····21|T6d·DkNpD6d·#·YW $-·k·xWn"<r "C7@zE·]·@p5xd···@7@D□·a"q'8··
c"5'8"·r·"u'8·S0vby(II·0··IWV··f·0·s□·|"·P·Gh·□·J·L8pb··uy1\]@·>T·~jI;·I:· I··)t@y·O-jja··' X·ing
system·····,Dc+;+;··· !··~□□··· D! ·····U*

- **Modified Boot Record [2]:**
- 1@·P<·|····f`···~F··~·4H>·~M·0P··x··.····!··A`·#·~·I··h··e>·}9··f1[hx·□6·~··F··^·h··D··fa··Kf`Wf□6·~f·F·f□6·~f·F·f·E·f
@f)F·f·^··E·F·4B··~nM·0R····1@:··>8}··B~~Cux·B~··h~·F~Nu·)V·V~Cuj1@ C·V·Ab ·v·~C·B~h[··i0m
OB~&0·FJuf_f·M·f·7V··y□□0S··#·f□u·f1@f E·fwP&g2·fB3·fQhs·f5 ·8m~KuqbgfwPf[f9X0CupfaC·H
G-B~·/B~·B~Cf`····N· ~·f X@ E·!<}f E·8
·h·□·~··U·|`s&·}~\·t·c·a·G)Bwm0Ni··AN_·D··`~·"~YWAs$ac·iE□YWfaCtk}\boot·····#+A·····~□?···hlh··
~□□·~□□'mh··'?·····U*

Prefetch

TDSS may use the name of a legitimate file.

UNREGMP2.EXE-3AE687B3.pf	Apr 5, 2012 2:19 AM	12 KB	ICC Profile
UNREGMP2.EXE-07CACB61.pf	Feb 10, 2012 6:39 PM	29 KB	ICC Profile

Path to the legitimate file:

```
\DEVICE\HARDDISKVOLUME1\WINDOWS\INF\UNREGMP2.EXE
```

Path to the malicious file:

```
\DEVICE\HARDDISKVOLUME1\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:

DefaultGateway	REG_MULTI...	192.168.1.1
DefaultGatewayMetric	REG_MULTI...	0
NameServer	REG_SZ	93.188.162.136,93.188.160.16
Domain	REG_SZ	
RegistrationEnabled	REG_DWORD	0x00000001
RegisterAdapterName	REG_DWORD	0x00000000
TCPAllowedPorts	REG_MULTI...	0
UDPAllowedPorts	REG_MULTI...	0
RawIPAllowedProtocols	REG_MULTI...	0
NTEContextList	REG_MULTI...	0x00000002
DhcpClassIdBin	REG_BINARY	00 00 00 00
DhcpNameServer	REG_SZ	93.188.162.136,93.188.160.16

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.
```

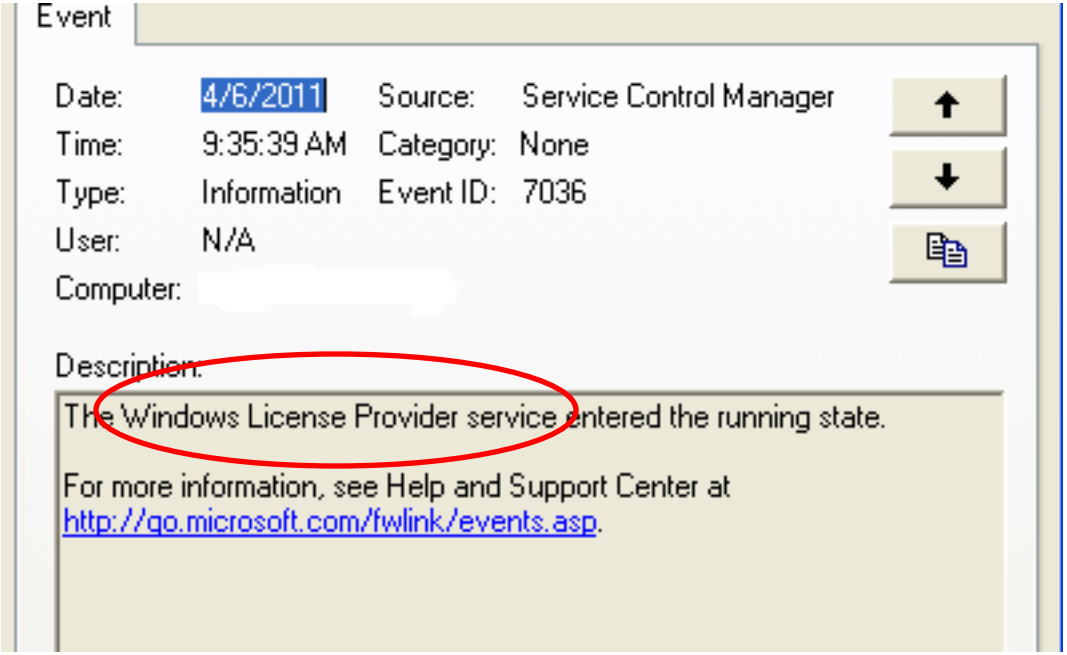
Event Correlation

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

4/5/2011	14:15:43	MACB	EVT	Event Log	Time generated/written	Service Control Manager/7036;Info;Intel CPU - running
4/5/2011	14:15:43	MACB	REG	SYSTEM key	Last Written	/ControlSet001/Enum/Root/LEGACY_ITLPERF
4/5/2011	14:15:43	MACB	REG	SYSTEM key	Last Written	/ControlSet002/Enum/Root/LEGACY_ITLPERF
4/5/2011	14:15:43	M.C.	FILE	NTFS $MFT	$SI [M.C.] time	C:/WINDOWS/Temp/ibni
4/5/2011	14:15:43	MACB	REG	SYSTEM key	Last Written	/ControlSet002/Enum/Root/LEGACY_ITLPERF
4/5/2011	14:15:43	MACB	REG	SYSTEM key	Last Written	/ControlSet001/Enum/Root/LEGACY_ITLPERF

Event Logs

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



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= flag to retrieve this description; see Help and Support for details. The following information is part of the event:

Security Risk Found!Tracking Cookies in File: Unavailable by: Manual scan. Action: Quarantine failed : Leave Alone failed. Action Description: The file was deleted successfully.

Event Logs

Antivirus may identify downloaders associated with TDSS.

Event

Date:	5/6/2011	Source:	Symantec AntiVirus
Time:	4:50:39 PM	Category:	None
Type:	Error	Event ID:	51
User:	N/A		
Computer:			

Description:

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.Zefarch!gen5 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.

system		10	http://www.inmotionhosting.com/?id=devilboy77
system		10	http://www.webhostingpad.com/
system		10	http://www.hostgator.com/
system		10	http://www.hostrocket.com/
system		10	http://adultfriendfinder.com/go/g1243200
system		10	http://adultfriendfinder.com/go/g1243200-pct
system		10	http://www.mobilemonopoly.com/?hop=devilboy77
system		10	http://www.dnforum.com/plans.php
system		10	http://www.hostmonster.com/
system		10	http://www.bloggingtothebank.com/
system		10	http://adultfriendfinder.com/go/g1243200-pmo
system		10	http://indianfriendfinder.com/go/g1243200.

Network Analysis – Proxy Log

- Activity associated with TDSS is often identifiable by reviewing network traffic:

http://crj711ki813ck.com/HCPy101ychsDQUBpLuYqlKwsUJCv3FdmUzbpj+6WczL0ayFN
0otfQR8hYR3QXjM012vJAnO4Nzspq1O70Fe/Hx/D46imInETbtzLK55F4UN3IiDFMqzTku
Z3oge1GCM22zxErEHa/zzb+jyvYyjHqA7h5+Oz8TU5kR8AwC6wYwAZaUCx3AG26SyeWT
XR2WLBQjuc4+VLNH4FfuYITBxHCtdJcIN8CVyKhx6ki31Ph0YJIpj9PI4Ms4+n0afctgPt5lM
11gPniptDeibGE/iGchd+weKBVGTWJsYMmCnBeZVciTiHvQGnQFrnRdlImLnIbzhF2FLS/L
ey9Da6VMePIyu2grwp2eoag3oDQv3EWTfRlz1M4CEbbtC1AsvdTrjy0xZyIHt+BvuBFyrx
wUUKsuDDZTkLo3J4SX+tG2XfZiKmk8IaFijM0vWv7PVlYAv7xWPoBSSSEja6+waf0DAzua
NKg36NAowgDOPINe9mVr7F9Mo/YTGNZ3T9CkquUe8DqOdj1bS7zeUjRZ6PUfW3R0Lv
HJylxTccHO/D8coMSfrEL8TbmwkF3MRCcf1XHzbzdkFaoQtR6HdQDP8eToHTaK8ph7kiqg
w/q15BjTCwcoZ2v3iZiGej4pwM6tzHpiCFLwskc+mxJZM5IlTsact/OzvD1NhSF+Jux5DGS8
LFYESl/cV0CcvDyLRTaZgf3bcN9kI/G3NBTmQA0yTZtHyL+rzO0dphGkQ+ekXhPFfxaj20X3
9GqPJ4RHhF2CwRjCp2x1o1gNFtDU6kek6ETW9VzuXQIjUAKaMBktx

Network Analysis – Proxy Log

- 192.168.32.188 anonymous Mozilla/4.0 (compatible; MSIE 1.0; Windows NT; CMD3) Y
  2011-05-06 19:16:21 w3proxy SERVER - ch01cilewk.com
  192.168.32.146 443 - - 662 SSL-tunnel TCP
  - ch01cilewk.com:443 - Inet 407 - Internet
  Req ID: 0a15636b; Req ID: 0a15636b; Compression: client=No, server=No, compress rate=0%
  decompress rate=0%, Compression: client=No, server=No, compress rate=0% decompress rate=0% Internal
  External 0x800 Allowed 2011-05-06 19:16:21 -

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.

- \·D·e·v·i·c·e·\·H·a·r·d·d·i·s·k·V·o·l·u·m·e·1·\·S·y·s·t·e·m· ·V·o·l·u·m·e· ·I·n·f·o·r·m·a·t·i·o·n·\·_·r·e·s·t·o·r·e·{·3·
- 8·6·F·7·B·B·D·-·F·8·A·8·-·4·7·8·1·-·9·6·6·A·- ·4·4·8·7·0·E·B·F·3·F·9·7·}·\·R·P·1·4·\·c·h·a·n·g·e·.·l·o·g···þ·····ï
- Í«····· ····a·····t·····\·W·I·N·D·O·W·S·\·s·y·s·t·e·m·3·2·\·s·p·o·o·l·\ ·p·r·t·p·r·
- o·c·s·\·w·3·2·x·8·6·\·O·C·1·7·u·O·C·E·I·.·d·l·l···"·····A·0·0·0·5·3·1·1·.·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>
- - <INSTANCENAME CLASSNAME="**Win32_StartupCommand**">
- - <KEYBINDING NAME="**Command**">
- <KEYVALUE VALUETYPE="**string**">**rundll32.exe "C:\WINDOWS\anitahefozujecaz.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
- "a4e50120.job" (a4e50120.exe)
- 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.

- h·t·t·p·:·/·/·c·l·c·k·i·l·.·c·o·m·/·?·x·u·r·l·=·h·t·t·p·:·/·/·c·l·c·k·i·l·.·c·o·m·/·y·Z·L·0·W·F·R·e·7·u·7·Q·y·R·U·1·5·6·7·1·d·8·2·c·3·8·6·6·2·d·9·6·5·e·8·6·5·4·6·3·9·4·c·0·f·9·3·6·1·7·A·&·x·r·e·f·=·h·t·t·p·:·/·/·c·o·r·n·i·s·h·r·e·x·.·o·r·g·/·k·e·y·/·?·q·s·=·5·7·d·2·7·7·6·c·5·6·a·7·1·4·6·b·b·6·4·3·e·e·f·c·2·0·8·6·9·1·0·2·d·f·b·5·2·4·d·b·6·e·6·d·9·8·7·8·f·f·0·e·9·4·7·1·d·f·0·b·8·1·0·e·0·0·a·c·0·e·b·a·2·d·f·5·0·a·8·6·d·6·0·8·3·c·3·b·3·8·c·3·d·f·4·3·&·t·=·t·o·+·c·o·n·s·o·l·i·d·a·t·e·+·d·e·b·t·····3Dc···□\·····S·o·f·t·w·a·r·e·\·M·i·c·r·o·s·o·f·t·\·W·i·n·d·o·w·s·\·C· u·r·r·e·n·t·V·e·r·s·i·o·n·\·I·n·t·e·r·n·e·t·S·e·t·t·i·n·g·s·\·Z·o·n·e·M·a·p

24th Annual FIRST Conference MALTA 17 - 22 June 2012

Pagefile.sys

- iexplore·am Files\Internet Explorer\IEXPLORE·EXE" -nohome·p·l·o·r·e·r·\·I·E·X·P·L·O·R·E·.·E·X·E·
- "· ·–·n·o·h·o·m·e·····
- ·····;·5.1 2600 SP3.0·····
- ·····C:\WINDOWS\Explorer.EXE·····
- ·····1715567821·····
- 351·····
- ·····8A;·0·····
- ·····Y#·0.03·····
- ·····D·0·····
- ·····o·
- 30001·····
- ·····pe8f15a3610c618aa918b3942
- e6bdcadb4437fbe3·····
- ·····P ;·\\?\globalroot\device\000004f0\494536f5·cmd.dll

Random Number

Build Date

Bootkit Version

Bot Identifier

Affiliate ID number

Path to the physical location on the disk

This data was recovered from the pagefile by searching for the physical path.

Pagefile.sys

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··Y·····vwE ··1·····da·}· M·4··@···~j ·····T··y]w`·vw_·vw!(·~·Y·~MB·~,K·~,J·~^0·~oD·wy<·w·N·w·L·w·K·wBJ·wEL·w>`·w·Z<·m <·n·<··7·|····`·5·····HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\esbigholtem.com

Live Memory Forensics

- Malicious code injected into svchost.exe

```
wininet.dll
wininet.dll
InternetCloseHandle
InternetConnectA
InternetOpenA
HttpOpenRequestA
InternetCrackUrlA
HttpSendRequestA
InternetReadFile
InternetCheckConnectionA
Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.9.1.1) GeckaSeka/20090911 Firefox/3.5.1
GET %s HTTP/1.0
Host: %s
User-Agent: %s
HTTP/1.0 200 OK
HTTP/1.1 200 OK
info
info
drv32
cmd32
drv32
drv32
```

Live Memory Forensics

```
Name                 Pid    Start      End        Tag    Hits Protect
csrss.exe            680 0x00270000 0x0027AFFF VadS      0      6 (MM_EXECUTE_READWRITE)
Dumped to: /tmp/csrss.exe.a5db1f8.00270000-0027afff.dmp
0x00270000   4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00    MZ..............
0x00270010   b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00    ........@.......
0x00270020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0x00270030   00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00    ................
0x00270040   0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68    ........!..L.!Th
0x00270050   69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f    is program canno
0x00270060   74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20    t be run in DOS 
0x00270070   6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00    mode....$.......


csrss.exe            680 0x00280000 0x00280FFF VadS      0      6 (MM_EXECUTE_READWRITE)
Dumped to: /tmp/csrss.exe.a5db1f8.00280000-00280fff.dmp
0x00280000   53 1d 80 7c 30 ae 80 7c 74 9b 80 7c 00 00 27 00    S..|0..|t..|..'.
0x00280010   2a 5c 5c 2e 5c 67 6c 6f 62 61 6c 72 6f 6f 74 5c    *\\.\globalroot\
0x00280020   64 65 76 69 63 65 5c 30 30 30 30 30 30 61 30 5c    device\000000a0\
0x00280030   7b 35 65 33 33 38 63 62 62 2d 32 34 33 62 2d 39    {5e338cbb-243b-9
0x00280040   66 66 38 2d 37 33 37 39 2d 33 36 66 35 36 34 34    ff8-7379-36f5644
0x00280050   39 35 31 31 38 7d 5c 70 68 2e 64 6c 6c 00 00 00    95118}\ph.dll...
0x00280060   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0x00280070   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
```

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;)

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";
classtype:trojan-activity; sid:2011894; rev:15;)
```

References

- C0decstuff. (2011). *Peeling Apart TDL4 and Other Seeds of Evil Part II*. Retrieved from URL
- Fisher, D. (2011). *TDSS Rootkit and DNSchanger: An Unholy Alliance*. Retrieved from URL
- Golovanov, S. and Rusakov, V. (2010). *TDSS*. Retrieved from URL
- Golovanov, S. and Soumenkov, I. (2011) *TDL4 – Top Bot*. Retrieved from URL
- Harley, D. (2012) *TDL4 reloaded: Purple Haze all in my brain*. Retrieved from URL
- Matrosov, A. (2011). *TDSS part 1: The x64 Dollar Question.* Retrieved from URL
- Matrosov, A. and Rodionov, E. (2010) *TDL3: The Rootkit of All Evil?.* ESET
- Matrosov, A. and Rodionov, E. (2011) *The Evolution of TDL: Conquering x64*. ESET
- Mila, (2012) *TDL4 – Purple Haze (Pihar) Variant –sample and analysis.* Retrieved from URL

Questions/Comments?