

Rootkit TDL-4 (TDSS, Alureon.DX, Olmarik, TDL) 32-bit and 64-bit Sample + Analysis links - Update July 7

 contagiodump.blogspot.com/2011/02/tdss-tdl-4-alureon-32-bit-and-64-bit.html



Old version 3 - See August 27, 2010 [TDL3 dropper \(x86 compatible with x64 systems\)](#).

General File Information - April 2011

This is an updated version of TDL4, which made a lot of news recently thanks to being named the 'indestructible' botnet. This is the last / current version and it is dated April 2011 (the previous version is from January 2011)

All the credits and many thanks for the files and comments go to [@EP_X0FF](#) [@InsaneKaos](#) [@markusg](#) [@USForce](#) from [KernelMode.info](#). I am posting the files and their comments here because of the the large number of inquiries for the updated version.

KernelMode.info:

Version TDL4 (April 2011 edition)

- 1) Bypassed Microsoft patch (STATUS_INVALID_IMAGE_HASH error overwritten) to be able again to infect x64 OS
- 2) Bypassed Microsoft patch to kdcom.dll (this version of TDL4 checks kdcom resource directory size on the x64 version of it, whether it is == 0x110 || 0xFA)
- 2) Improved disk minport filtering hook

Version history:

1. **0.01** firstly detected ITW in the end of July 2010
2. **0.02** August 2010, version with x64 support
3. **0.03** September 2010, small changes, new C&C library
4. In April 2011 Microsoft released [KB2506014](#) targeting 0.03 version, exactly boot loader and kd dll - and it was able to successfully prevent TDL4 from working. However, the rootkit support strike back within two weeks releasing their update, which could bypass the MS patch. The rootkit version wasn't changed.

Related articles:

List of samples included

File: TDL4.exe

Size: 146944

MD5: 4A052246C5551E83D2D55F80E72F03EB

[http://www.virustotal.com/file-scan/report.html?](http://www.virustotal.com/file-scan/report.html?id=b75fd580c29736abd11327eef949e449f6d466a05fb6fd343d3957684c8036e5-1305275113)

[id=b75fd580c29736abd11327eef949e449f6d466a05fb6fd343d3957684c8036e5-1305275113](http://www.virustotal.com/file-scan/report.html?id=b75fd580c29736abd11327eef949e449f6d466a05fb6fd343d3957684c8036e5-1305275113)

File: dll (2).exe

Size: 140288

MD5: D69B02C1ACD87B5A5C33B19693E24020

[http://www.virustotal.com/file-scan/report.html?](http://www.virustotal.com/file-scan/report.html?id=fe165840b709adb5b7765ea329c317f64d05a402873c8d8cea84873cbe192bf4-1304405700)

[id=fe165840b709adb5b7765ea329c317f64d05a402873c8d8cea84873cbe192bf4-1304405700](http://www.virustotal.com/file-scan/report.html?id=fe165840b709adb5b7765ea329c317f64d05a402873c8d8cea84873cbe192bf4-1304405700)

File: DLL.exe

Size: 140288

MD5: A1DE5B3607845F5C6597528BE02EBDA5

[http://www.virustotal.com/file-scan/report.html?](http://www.virustotal.com/file-scan/report.html?id=1aa5708519389ddcf96fa6206cf274844414c58bff6e3f8338188364449f4509-1304402425)

[id=1aa5708519389ddcf96fa6206cf274844414c58bff6e3f8338188364449f4509-1304402425](http://www.virustotal.com/file-scan/report.html?id=1aa5708519389ddcf96fa6206cf274844414c58bff6e3f8338188364449f4509-1304402425)



Download TDL4 - April 2011 edition files listed above as a password protected archive (contact me if you need the password)



General File Information - January 2011

List of components provided

cfg.ini	MD5 CB4AAD4D8D464E58461C867FFAD6462B
cmd.dll	MD5 03B82BE24271737CC0DA6C83CBB5A24F
cmd64.dll	MD5 E6B9F8C6726FA44DD833992A9A908907
drv32	MD5 528C67F455234CD413335246EBC136B7
drv64	MD5 F7E79B727D9EB24EB522204182D47FDD
ldr16	MD5 F4CBF6BEF6DF44213CFF3332422A0B78
ldr32	MD5 8B0B9ACEA732B91BC2305162C06ED8FC
ldr64	MD5 3EDD490066EA4A312E6FA6DC420AF6C6
keygen_v.45.23.4.ex1	MD531DB7A22DF02E1A91DB9AFDA4F02F3BF

The following information in the blue box is posted with thanks to **EP_X0FF** from **www.kernelmode.info**

Original post: <http://www.kernelmode.info/forum/viewtopic.php?f=16&t=19>
TDL4 common information

First kernel mode rootkit compatible with x64 Windows.

Uses bootkit technique to load itself and bypass drivers signing restriction on x64

Uses payload C&C dll injection (cmd.dll for x86 and cmd64.dll for x64).

To keep it's data uses own VFS where stored following files:

- cfg.ini (configuration text file, replaced previously used config.ini)
- cmd.dll (payload dll to be injected into x86 processes)
- cmd64.dll (the same but for x64)
- mbr (copy of original main boot record)
- ldr16 (rootkit loader parts, gets control from infected mbr and provides further rootkit loading)
- ldr32 (rootkit driver, representing fake KD dll, responsible for loading main rootkit driver)
- ldr64 (ldr32 version for x64 systems)
- drv32 (main rootkit driver, VFS support, modifications hiding)
- drv64 (drv32 version for x64 systems)

may store additional files or payload downloaded by cmd library.

Rootkit renders Windows XP (x86/x64), Windows 2003(x86/x64) into unbootable state after infection (infection method restriction).

Current versions

- rootkit 0.03
- C&C library version 0.163 (cmd.dll)



Download



[Download TDL4 as a password protected archive \(contact me if you need the password\) -with many thanks to anonymous friends](#)

Analysis

- Jan 25, 2011 Kaspersky Lab [TDSS. TDL-4](#) - great analysis by [Vyacheslav Rusakov](#)

- Dec 7, 2010 Kaspersky Lab [TDL4 Starts Using 0-Day Vulnerability!](#) by Sergey Golovanov
- Nov 15, 2010 [How the TDL4 rootkit gets around driver signing policy on a 64-bit machine](#) (Analysis by Chandra Prakash, Technical Fellow, GFI Labs)

Previous Versions:

- April 6, 2008 Kaspersky Lab [TDL-1 The Beginning: TDL-1](#)
- early 2009 Kaspersky Lab [TDL-2: the saga continues](#)
- Aug 05, 2010 Kaspersky Lab [TDL-3: the end of the story?](#)
- Oct 2010 Microsoft [Alureon: The First 64-Bit Windows Rootkit](#) by Joe Johnson

Automated Scans

Here are current scans

File name:keygen_v.45.23.4.ex1

<http://www.virustotal.com/file-scan/report.html?id=ba670c68a7e481c324bdc2e8c5c8c1c8ddc4a2772e991826771350ea8e03f2ce-1296794154>

Submission date:2011-02-04 04:35:54 (UTC)

Result:37/ 43 (86.0%)

AhnLab-V3	2011.01.27.01	2011.01.27	Win-Trojan/Tdss.123904.KD
AntiVir	7.11.2.68	2011.02.03	TR/Drop.TDss.usr
Antiy-AVL	2.0.3.7	2011.01.28	Trojan/Win32.TDSS.gen
Avast	4.8.1351.0	2011.02.03	Win32:Alureon-MT
Avast5	5.0.677.0	2011.02.03	Win32:Alureon-MT
AVG	10.0.0.1190	2011.02.04	Agent2.BXSP
BitDefender	7.2	2011.02.04	Gen:Variant.Kazy.5799
CAT-QuickHeal	11.00	2011.02.03	Win32.Trojan-Dropper.TDSS.uuc.6.a
ClamAV	0.96.4.0	2011.02.04	Trojan.Dropper-27337
CommTouch	5.2.11.5	2011.02.04	W32/MalwareF.TJXJ
Comodo	7584	2011.02.03	TrojWare.Win32.Trojan.Agent.Gen
DrWeb	5.0.2.03300	2011.02.04	BackDoor.Tdss.based.7
Emsisoft	5.1.0.2	2011.02.04	Trojan-Dropper.Win32.TDSS!IK
eTrust-Vet	36.1.8139	2011.02.03	Win32/TDSS.B!generic
F-Prot	4.6.2.117	2011.02.01	W32/MalwareF.TJXJ
F-Secure	9.0.16160.0	2011.02.04	Gen:Variant.Kazy.5799
GData	21	2011.02.04	Gen:Variant.Kazy.5799
Ikarus	T3.1.1.97.0	2011.02.04	Trojan-Dropper.Win32.TDSS
Jiangmin	13.0.900	2011.02.03	TrojanDropper.TDSS.clw

K7AntiVirus 9.81.3737 2011.02.03 Riskware
Kaspersky 7.0.0.125 2011.02.04 Trojan-Dropper.Win32.TDSS.usr
McAfee 5.400.0.1158 2011.02.04 Generic Dropper.va.gen.m
McAfee-GW-Edition 2010.1C 2011.02.03 Generic Dropper.va.gen.m
Microsoft 1.6502 2011.02.03 Trojan:Win32/Meredrop
NOD32 5844 2011.02.03 a variant of Win32/Olmarik.AJM
nProtect 2011-01-27.01 2011.02.02 Trojan-Dropper/W32.TDSS.123904.AI
Panda 10.0.3.5 2011.02.03 Generic Trojan
PCTools 7.0.3.5 2011.02.04 Trojan.Gen
Prevx 3.0 2011.02.04 High Risk Cloaked Malware
Rising 23.43.04.02 2011.02.04 Trojan.Win32.Generic.1261B216
Symantec 20101.3.0.103 2011.02.04 Trojan.Gen.2
TheHacker 6.7.0.1.123 2011.02.02 Trojan/Olmarik.ajm
TrendMicro 9.200.0.1012 2011.02.04 BKDR_TDSS.SMEO
TrendMicro-HouseCall 9.200.0.1012 2011.02.04 BKDR_TDSS.SMEO
VBA32 3.12.14.3 2011.02.02 OScope.Trojan.TTVV
VIPRE 8301 2011.02.04 Packed.Win32.Tdss.Gen (v)
VirusBuster 13.6.180.0 2011.02.03 Trojan.DR.TDSS!!liQY+NDfskl
MD5 : 31db7a22df02e1a91db9afda4f02f3bf
SHA1 : 6ede4482be1b06c90cca93bedf3e363c096102f5
SHA256: ba670c68a7e481c324bdc2e8c5c8c1c8ddc4a2772e991826771350ea8e03f2ce
ssdeep:
3072:ly+NYC1kAB4DtZ1VEY88vp3O/+AtyZ6g8J4Kgp98QH3a1/Qh/C7:ly+NYC1kfDtH8Q309N
2B98QH3a1YE
File size : 123904 bytes
First seen: 2010-12-14 14:25:05
Last seen : 2011-02-04 04:35:54
TrID:Win32 Executable Generic (42.3%)

cmd.dll

<http://www.virustotal.com/file-scan/report.html?id=bb05718936de0aa434806679088c27d58786ad40f89c4af9812d0eb5f804518c-1296793082>

Submission date:2011-02-04 04:18:02 (UTC)

Result:35/ 42 (83.3%)

AhnLab-V3 2011.01.27.01 2011.01.27 Win-Trojan/Xema.variant
AntiVir 7.11.2.68 2011.02.03 TR/Agent.8704.76
Antiy-AVL 2.0.3.7 2011.01.28 Trojan/Win32.Agent.gen
Avast 4.8.1351.0 2011.02.03 Win32:Alureon-LU
Avast5 5.0.677.0 2011.02.03 Win32:Alureon-LU
AVG 10.0.0.1190 2011.02.04 Agent_r.XJ
BitDefender 7.2 2011.02.04 Generic.Malware.FYddld.50835ADA

CAT-QuickHeal 11.00 2011.02.03 TrojanDownloader.Agent.exgl
Commtouch 5.2.11.5 2011.02.04 W32/MalwareF.UEA
Comodo 7584 2011.02.03 UnclassifiedMalware
DrWeb 5.0.2.03300 2011.02.04 Trojan.DownLoad2.17710
Emsisoft 5.1.0.2 2011.02.04 Virus.Win32.DNSChanger.VJ!IK
eTrust-Vet 36.1.8139 2011.02.03 Win32/Alureon.CFR
F-Prot 4.6.2.117 2011.02.01 W32/MalwareF.UEA
F-Secure 9.0.16160.0 2011.02.04 Generic.Malware.FYddld.50835ADA
GData 21 2011.02.04 Generic.Malware.FYddld.50835ADA
Ikarus T3.1.1.97.0 2011.02.04 Virus.Win32.DNSChanger.VJ
K7AntiVirus 9.81.3737 2011.02.03 Riskware
Kaspersky 7.0.0.125 2011.02.04 Trojan-Downloader.Win32.Agent.exgl
McAfee-GW-Edition 2010.1C 2011.02.03 Heuristic.BehavesLike.Win32.Spyware.J
Microsoft 1.6502 2011.02.03 Trojan:Win32/Alureon.DY
NOD32 5844 2011.02.03 Win32/Olmarik.ADZ
Norman 6.07.03 2011.02.03 W32/Suspicious_Gen2.EIISB
nProtect 2011-01-27.01 2011.02.02 Trojan-Downloader/W32.Agent.73728.JD
Panda 10.0.3.5 2011.02.03 Trj/CI.AS
PCTools 7.0.3.5 2011.02.04 Trojan.Gen
Prevx 3.0 2011.02.04 Medium Risk Malware
Sophos 4.61.0 2011.02.04 Mal/Emogen-Y
Symantec 20101.3.0.103 2011.02.04 Trojan.Gen
TheHacker 6.7.0.1.123 2011.02.02 Trojan/Olmarik.adz
TrendMicro 9.200.0.1012 2011.02.04 Mal_TDSS-16
TrendMicro-HouseCall 9.200.0.1012 2011.02.04 Mal_TDSS-16
VBA32 3.12.14.3 2011.02.02 TrojanDownloader.Agent.exgl
VIPRE 8301 2011.02.04 Trojan.Win32.Alureon.DY (v)
VirusBuster 13.6.180.0 2011.02.03 Trojan.DL.Agent!zPxnel7NLbo

Additional information

Show all

MD5 : 03b82be24271737cc0da6c83cbb5a24f

cmd64.dll

[http://www.virustotal.com/file-scan/report.html?](http://www.virustotal.com/file-scan/report.html?id=faff9cb858fcd5560c747f29c3e70e248c37d7e4efb6e6c4977d6d3a11ba1ec-1294575619)

[id=faff9cb858fcd5560c747f29c3e70e248c37d7e4efb6e6c4977d6d3a11ba1ec-1294575619](http://www.virustotal.com/file-scan/report.html?id=faff9cb858fcd5560c747f29c3e70e248c37d7e4efb6e6c4977d6d3a11ba1ec-1294575619)

Submission date:2011-02-04 04:14:58 (UTC)

Result:31/ 43 (72.1%)

AhnLab-V3 2011.01.27.01 2011.01.27 Trojan/Win64.TDSS
Avast 4.8.1351.0 2011.02.03 Win32:Malware-gen
Avast5 5.0.677.0 2011.02.03 Win32:Malware-gen
AVG 10.0.0.1190 2011.02.04 Generic18.CFVM
BitDefender 7.2 2011.02.04 Trojan.Generic.4667917

Comodo 7584 2011.02.03 UnclassifiedMalware
DrWeb 5.0.2.03300 2011.02.04 BackDoor.Tdss.4005
Emsisoft 5.1.0.2 2011.02.04 Trojan.Win64!IK
eTrust-Vet 36.1.8139 2011.02.03 Win64/Alureon.A
F-Secure 9.0.16160.0 2011.02.04 Trojan.Generic.4667917
GData 21 2011.02.04 Trojan.Generic.4667917
Ikarus T3.1.1.97.0 2011.02.04 Trojan.Win64
Jiangmin 13.0.900 2011.02.03 Trojan/Win64.j
K7AntiVirus 9.81.3737 2011.02.03 Trojan
Kaspersky 7.0.0.125 2011.02.04 Trojan.Win64.TDSS.b
McAfee 5.400.0.1158 2011.02.04 Generic.dx!tpx
McAfee-GW-Edition 2010.1C 2011.02.03 Generic.dx!tpx
Microsoft 1.6502 2011.02.03 Trojan:Win64/Alureon.gen!A
NOD32 5844 2011.02.03 Win64/Olmarik.D
Norman 6.07.03 2011.02.03 Suspicious_Gen2.ESEQG
nProtect 2011-01-27.01 2011.02.02 -
Panda 10.0.3.5 2011.02.03 Trj/CI.A
PCTools 7.0.3.5 2011.02.04 Backdoor.Tidserv
Prevx 3.0 2011.02.04 Medium Risk Malware
Symantec 20101.3.0.103 2011.02.04 Backdoor.Tidserv.L
TheHacker 6.7.0.1.123 2011.02.02 Trojan/Tdss.a
TrendMicro 9.200.0.1012 2011.02.04 TROJ_ALUREON.WVM
TrendMicro-HouseCall 9.200.0.1012 2011.02.04 TROJ_ALUREON.WVM
VBA32 3.12.14.3 2011.02.02 Trojan.Win64.TDSS.a
VIPRE 8301 2011.02.04 Trojan.Win32.Generic!BT
ViRobot 2011.2.4.4291 2011.02.04 Trojan.Win32.S.Alureon.45056
VirusBuster 13.6.180.0 2011.02.03 Trojan.Win64.TDSS.ACPV
MD5 : e6b9f8c6726fa44dd833992a9a908907

drv32

Submission date:2011-02-04 04:28:15 (UTC)

Result:37/ 43 (86.0%)

<http://www.virustotal.com/file-scan/report.html?>

[id=1434cac829f1e962f3784d788492626846952c3479530ee57f503ed17e92f71e-1296793695](http://www.virustotal.com/file-scan/report.html?id=1434cac829f1e962f3784d788492626846952c3479530ee57f503ed17e92f71e-1296793695)

AntiVir 7.11.2.50 2011.02.01 TR/TDss.X
Antiy-AVL 2.0.3.7 2011.01.28 Trojan/Win32.TDSS.gen
Avast 4.8.1351.0 2011.02.01 Win32:Alureon-NH
Avast5 5.0.677.0 2011.02.01 Win32:Alureon-NH
AVG 10.0.0.1190 2011.02.02 Cryptic.BLS
BitDefender 7.2 2011.02.02 Trojan.Tdss.4951
CAT-QuickHeal 11.00 2011.02.02 Trojan.Rootkit.gen

Commtouch 5.2.11.5 2011.02.02 W32/MalwareF.TLBA
Comodo 7562 2011.02.02 UnclassifiedMalware
Emsisoft 5.1.0.2 2011.02.02 Trojan.TDss!IK
eSafe 7.0.17.0 2011.02.01 Win32.TRTDss.X
eTrust-Vet 36.1.8135 2011.02.01 Win32/Tnega.VNH
F-Prot 4.6.2.117 2011.02.01 W32/MalwareF.TLBA
F-Secure 9.0.16160.0 2011.02.02 Trojan.Tdss.4951
GData 21 2011.02.02 Trojan.Tdss.4951
Ikarus T3.1.1.97.0 2011.02.02 Trojan.TDss
Jiangmin 13.0.900 2011.02.01 Rootkit.TDSS.esm
K7AntiVirus 9.80.3713 2011.02.01 RootKit
Kaspersky 7.0.0.125 2011.02.02 Rootkit.Win32.TDSS.wia
McAfee 5.400.0.1158 2011.02.02 Generic Dropper.va.gen.e
McAfee-GW-Edition 2010.1C 2011.02.02 Generic Dropper.va.gen.e
Microsoft 1.6502 2011.02.01 Trojan:WinNT/Alureon.L
NOD32 5838 2011.02.01 a variant of Win32/Olmarik.AJN
Norman 6.06.12 2011.02.01 W32/Suspicious_Gen2.GSVJS
Panda 10.0.3.5 2011.02.01 Generic Trojan-BOUNDARY
PCTools 7.0.3.5 2011.01.31 SecurityRisk.ADH
Prevx 3.0 2011.02.04 Medium Risk Malware
Rising 23.43.02.02 2011.02.02 Trojan.Win32.Generic.12621AC5
Sophos 4.61.0 2011.02.02 Mal/TDSSPk-AF
SUPERAntiSpyware 4.40.0.1006 2011.02.02 Trojan.Agent/Gen-FakeAlert
Symantec 20101.3.0.103 2011.02.02 SecurityRisk.ADH
TheHacker 6.7.0.1.122 2011.01.30 Trojan/TDSS.wia
TrendMicro 9.120.0.1004 2011.02.02 TROJ_GEN.R47C2LJ
TrendMicro-HouseCall 9.120.0.1004 2011.02.02 TROJ_GEN.R47C2LJ
VBA32 3.12.14.3 2011.02.01 Rootkit.TDSS.wik
VIPRE 8282 2011.02.02 Trojan.Win32.Generic!BT
VirusBuster 13.6.176.0 2011.02.01 Rootkit.TDSS!FdSt/2yWsyY

Additional information

Show all

MD5 : 528c67f455234cd413335246ebc136b7

drv64

<http://www.virustotal.com/file-scan/report.html?id=231e95dc2ad1c2e2325ebcd2f75b2d2569a952e138226b71ee8420ee5a639ef1-1296795040>

Submission date:2011-02-04 04:50:40 (UTC)

Result:28/ 42 (66.7%)

AhnLab-V3 2011.01.27.01 2011.01.27 Backdoor/Win64.Tidserv

AntiVir 7.11.2.68 2011.02.03 RKit/TDss.A

Avast 4.8.1351.0 2011.02.03 Win64:Alureon

Avast5 5.0.677.0 2011.02.03 Win64:Alureon
AVG 10.0.0.1190 2011.02.04 Cryptic.BMW
BitDefender 7.2 2011.02.04 Rootkit.TDSS.BH
CAT-QuickHeal 11.00 2011.02.04 Trojan.Alureon.Gen
Comodo 7584 2011.02.03 UnclassifiedMalware
DrWeb 5.0.2.03300 2011.02.04 BackDoor.Tdss.4688
Emsisoft 5.1.0.2 2011.02.04 Rootkit.TDss!IK
eTrust-Vet 36.1.8139 2011.02.03 Win64/Alureon.A
F-Secure 9.0.16160.0 2011.02.04 Rootkit.TDSS.BH
GData 21 2011.02.04 Rootkit.TDSS.BH
Ikarus T3.1.1.97.0 2011.02.04 Rootkit.TDss
K7AntiVirus 9.81.3737 2011.02.03 Riskware
McAfee 5.400.0.1158 2011.02.04 Generic.dx!vfe
McAfee-GW-Edition 2010.1C 2011.02.03 Generic.dx!vfe
NOD32 5844 2011.02.03 Win64/Olmarik.H
Norman 6.07.03 2011.02.03 Suspicious_Gen2.GQURM
nProtect 2011-01-27.01 2011.02.02 -
Panda 10.0.3.5 2011.02.03 Generic MalwareBOUNDARY
PCTools 7.0.3.5 2011.02.04 Backdoor.Tidserv
Sophos 4.61.0 2011.02.04 Troj/TDL3-Fam
SUPERAntiSpyware 4.40.0.1006 2011.02.04 -
Symantec 20101.3.0.103 2011.02.04 Backdoor.Tidserv.L
TheHacker 6.7.0.1.123 2011.02.02 Trojan/Olmarik.g
TrendMicro 9.200.0.1012 2011.02.04 BKDR_TDSS.ANU
TrendMicro-HouseCall 9.200.0.1012 2011.02.04 TROJ_GEN.R47C3AA
VIPRE 8301 2011.02.04 Trojan.Win32.Generic!BT
VirusBuster 13.6.180.0 2011.02.03 Rootkit.TDss!DMEmZtR66Yk
Show all
MD5 : f7e79b727d9eb24eb522204182d47fdd

ldr16

<http://www.virustotal.com/file-scan/report.html?id=964fec64fb8b03d387fae132e206f0b7e4c3fe5e7aa1f5d12fbe765f7da2c66a-1296795255>

Submission date:2011-02-04 04:54:15 (UTC)

Result:8/ 43 (18.6%)

Avast 4.8.1351.0 2011.02.03 Alureon-B@mbr
Avast5 5.0.677.0 2011.02.03 Alureon-B@mbr
BitDefender 7.2 2011.02.04 Rootkit.TDSS.BH
DrWeb 5.0.2.03300 2011.02.04 BackDoor.Tdss.4724
eTrust-Vet 36.1.8139 2011.02.03 Dos/Alureon
F-Secure 9.0.16160.0 2011.02.04 Rootkit.TDSS.BH
GData 21 2011.02.04 Rootkit.TDSS.BH

VIPRE 8301 2011.02.04 Trojan.DOS.Alureon.a (v)

MD5 : f4cbf6bef6df44213cff3332422a0b78

Idr32

[http://www.virustotal.com/file-scan/report.html?](http://www.virustotal.com/file-scan/report.html?id=857df0c9d476fa9fbaa96bc07aeb94466172fa0820c3625a04b1f87f3d94731a-1296795535)

[id=857df0c9d476fa9fbaa96bc07aeb94466172fa0820c3625a04b1f87f3d94731a-1296795535](http://www.virustotal.com/file-scan/report.html?id=857df0c9d476fa9fbaa96bc07aeb94466172fa0820c3625a04b1f87f3d94731a-1296795535)

Submission date:2011-02-04 04:58:55 (UTC)

Result:34/ 43 (79.1%)

Antivirus	Version	Last Update	Result
-----------	---------	-------------	--------

AhnLab-V3	2011.01.27.01	2011.01.27	Backdoor/Win32.Tidserv
-----------	---------------	------------	------------------------

AntiVir	7.11.2.50	2011.02.01	TR/Alureon.3134.X.2
---------	-----------	------------	---------------------

Avast	4.8.1351.0	2011.02.01	Win32:Alureon-MJ@mbr
-------	------------	------------	----------------------

Avast5	5.0.677.0	2011.02.01	Win32:Alureon-MJ@mbr
--------	-----------	------------	----------------------

AVG	10.0.0.1190	2011.02.02	Generic20.AFVG
-----	-------------	------------	----------------

BitDefender	7.2	2011.02.02	Rootkit.TDSS.BH
-------------	-----	------------	-----------------

CAT-QuickHeal	11.00	2011.02.02	Trojan.Alureon.gen
---------------	-------	------------	--------------------

ClamAV	0.96.4.0	2011.02.02	BC.Heuristics.Rootkit.B-9.SL5IT
--------	----------	------------	---------------------------------

Commtouch	5.2.11.5	2011.02.02	W32/MalwareF.UGCX
-----------	----------	------------	-------------------

Comodo	7562	2011.02.02	UnclassifiedMalware
--------	------	------------	---------------------

DrWeb	5.0.2.03300	2011.02.01	BackDoor.Tdss.4688
-------	-------------	------------	--------------------

Emsisoft	5.1.0.2	2011.02.02	Trojan.Win32.Alureon!IK
----------	---------	------------	-------------------------

eSafe	7.0.17.0	2011.02.01	Win32.TRALureon.X
-------	----------	------------	-------------------

eTrust-Vet	36.1.8135	2011.02.01	Win32/Alureon.CFS
------------	-----------	------------	-------------------

F-Prot	4.6.2.117	2011.02.01	W32/MalwareF.UGCX
--------	-----------	------------	-------------------

F-Secure	9.0.16160.0	2011.02.02	Rootkit.TDSS.BH
----------	-------------	------------	-----------------

Fortinet	4.2.254.0	2011.02.02	W32/DNSChanger.EP!tr
----------	-----------	------------	----------------------

GData	21	2011.02.02	Rootkit.TDSS.BH
-------	----	------------	-----------------

Ikarus	T3.1.1.97.0	2011.02.02	Trojan.Win32.Alureon
--------	-------------	------------	----------------------

K7AntiVirus	9.80.3713	2011.02.01	Riskware
-------------	-----------	------------	----------

McAfee	5.400.0.1158	2011.02.02	DNSChanger!ep
--------	--------------	------------	---------------

McAfee-GW-Edition	2010.1C	2011.02.02	DNSChanger!ep
-------------------	---------	------------	---------------

Microsoft	1.6502	2011.02.01	Trojan:Win32/Alureon.gen!X
-----------	--------	------------	----------------------------

NOD32	5838	2011.02.01	Win32/Olmarik.AFK
-------	------	------------	-------------------

Norman	6.06.12	2011.02.01	W32/Suspicious_Gen2.GSECX
--------	---------	------------	---------------------------

Panda	10.0.3.5	2011.02.01	Trj/CI.A
-------	----------	------------	----------

PCTools	7.0.3.5	2011.01.31	Backdoor.Tidserv
---------	---------	------------	------------------

Rising	23.43.02.02	2011.02.02	Trojan.Win32.Generic.126012F5
--------	-------------	------------	-------------------------------

Sophos	4.61.0	2011.02.02	Mal/Generic-L
--------	--------	------------	---------------

Symantec	20101.3.0.103	2011.02.02	Backdoor.Tidserv.L
----------	---------------	------------	--------------------

TheHacker	6.7.0.1.122	2011.01.30	W32/Behav-Heuristic-068
-----------	-------------	------------	-------------------------

TrendMicro	9.120.0.1004	2011.02.02	TROJ_GEN.R47C2LB
------------	--------------	------------	------------------

TrendMicro-HouseCall	9.120.0.1004	2011.02.02	TROJ_GEN.R47C2LB
----------------------	--------------	------------	------------------

VIPRE 8282 2011.02.02 Trojan.Win32.Generic!BT

MD5 : 8b0b9acea732b91bc2305162c06ed8fc

ldr64

[http://www.virustotal.com/file-scan/report.html?](http://www.virustotal.com/file-scan/report.html?id=215e7f87c18525fc842c155278a0a49d5075c35ffac1d4f1580e1fc92d4cc52c-1296797566)

[id=215e7f87c18525fc842c155278a0a49d5075c35ffac1d4f1580e1fc92d4cc52c-1296797566](http://www.virustotal.com/file-scan/report.html?id=215e7f87c18525fc842c155278a0a49d5075c35ffac1d4f1580e1fc92d4cc52c-1296797566)

Submission date:2011-02-04 05:32:46 (UTC)

Result:20/ 43 (46.5%)

Antivirus	Version	Last Update	Result
-----------	---------	-------------	--------

AhnLab-V3	2011.01.27.01	2011.01.27	Malware/Win64.Generic
-----------	---------------	------------	-----------------------

AntiVir	7.11.2.68	2011.02.03	RKit/TDss.CC
---------	-----------	------------	--------------

Avast	4.8.1351.0	2011.02.03	Win64:Alureon-B@mbr
-------	------------	------------	---------------------

Avast5	5.0.677.0	2011.02.03	Win64:Alureon-B@mbr
--------	-----------	------------	---------------------

AVG	10.0.0.1190	2011.02.04	Cryptic.BUA
-----	-------------	------------	-------------

BitDefender	7.2	2011.02.04	Rootkit.TDSS.BH
-------------	-----	------------	-----------------

Comodo	7586	2011.02.04	UnclassifiedMalware
--------	------	------------	---------------------

DrWeb	5.0.2.03300	2011.02.04	BackDoor.Tdss.4688
-------	-------------	------------	--------------------

Emsisoft	5.1.0.2	2011.02.04	Rootkit.TDss!IK
----------	---------	------------	-----------------

eSafe	7.0.17.0	2011.02.03	Win32.Rootkit.TDSS.B
-------	----------	------------	----------------------

eTrust-Vet	36.1.8139	2011.02.03	Win64/Alureon.A
------------	-----------	------------	-----------------

F-Secure	9.0.16160.0	2011.02.04	Rootkit.TDSS.BH
----------	-------------	------------	-----------------

GData	21	2011.02.04	Rootkit.TDSS.BH
-------	----	------------	-----------------

Ikarus	T3.1.1.97.0	2011.02.04	Rootkit.TDss
--------	-------------	------------	--------------

K7AntiVirus	9.81.3737	2011.02.03	Riskware
-------------	-----------	------------	----------

NOD32	5844	2011.02.03	Win64/Olmarik.G
-------	------	------------	-----------------

Norman	6.07.03	2011.02.03	Suspicious_Gen2.GVBYR
--------	---------	------------	-----------------------

Panda	10.0.3.5	2011.02.03	Trj/Cl.A
-------	----------	------------	----------

TheHacker	6.7.0.1.123	2011.02.02	Trojan/Olmarik.g
-----------	-------------	------------	------------------

VIPRE 8302 2011.02.04 Trojan.Win32.Generic!BT

MD5 : 3edd490066ea4a312e6fa6dc420af6c6

