virustotal

SHA256: 7d83ba11047bfacc978d96bc13ab5209beee77e72c54f1d8252f2e6372f82351

File name: fawi.exe

Detection ratio: 30 / 43

Analysis date: 2012-02-26 03:50:29 UTC (0 minutes ago)

Antivirus	Result	Update
AhnLab-V3	Win-Trojan/Agent.200272	20120225
AntiVir	TR/Fakealert.CSQ	None
Antiy-AVL	-	20120226
Avast	Win32:Malware-gen	20120225
AVG	Pakes.LBY	20120226
BitDefender	Trojan.FakeAlert.CSQ	20120226
ByteHero	-	None
CAT-QuickHeal	-	20120225
ClamAV	Trojan.Zbot-16626	20120226
Commtouch	-	20120225
Comodo	TrojWare.Win32.Kryptik.CSQ	20120226
DrWeb	Trojan.PWS.Panda.655	20120226
Emsisoft	Trojan.Win32.Reveton!IK	20120226
eSafe	-	None
eTrust-Vet	Win32/Kollah.NBP	20120225
F-Prot	-	20120225
F-Secure	Trojan.FakeAlert.CSQ	20120226
Fortinet	-	20120226
GData	Trojan.FakeAlert.CSQ	20120226
Ikarus	Trojan.Win32.Reveton	20120225
Jiangmin	TrojanDropper.Injector.kwd	20120225
K7AntiVirus	Riskware	20120225
Kaspersky	HEUR:Trojan.Win32.Generic	20120226
McAfee	PWS-Zbot.gen.qp	20120226
McAfee-GW-Edition	PWS-Zbot.gen.qp	20120225

Microsoft	PWS:Win32/Zbot	20120225
NOD32	Win32/Spy.Zbot.YW	20120226
Norman	Zbot.dam	20120225
nProtect	Trojan-Dropper/W32.Injector.200272	20120225
Panda	Suspicious file	20120225
PCTools	-	None
Prevx	-	20120226
Rising	-	20120224
Sophos	Mal/Zbot-EZ	20120225
SUPERAntiSpyware	Trojan.Agent/Gen-Faldesc[Cont]	None
Symantec	Trojan.Gen	20120226
TheHacker	Trojan/Spy.Zbot.yw	20120225
TrendMicro	-	20120226
TrendMicro-HouseCall	-	20120226
VBA32	TrojanDropper.Injector.cnch	20120224
VIPRE	Trojan.Win32.Generic!BT	20120225
ViRobot	-	20120225
VirusBuster	TrojanSpy.Zbot!YiyOxCGYLXo	20120225

Comments | Additional information

ssdeep

6144:vIT4RK91lPQtCbb8/gVJYnKjw0hQ3BYfoSYy:wT4w9Pu/grxQGoSYy

TrID

UPX compressed Win32 Executable (39.5%)
Win32 EXE Yoda's Crypter (34.3%)
Win32 Executable Generic (11.0%)
Win32 Dynamic Link Library (generic) (9.8%)
Generic Win/DOS Executable (2.5%)

ExifTool

```
UninitializedDataSize....: 143360
InitializedDataSize......: 4096
ImageVersion.............: 10.2
ProductName..............: Duet
FileVersionNumber........: 8.3.0.0
LanguageCode.............: English (U.S.)
FileFlagsMask............: 0x003f
FileDescription..........: Glows Anger Hebrew
CharacterSet.............: Unicode
LinkerVersion............: 9.0
FileOS...................: Windows NT 32-bit
MIMEType.................: application/octet-stream
Subsystem................: Windows GUI
FileVersion..............: 8.3
```

```
PEType...................: PE32
InternalName.............: Source Smith Tried
ProductVersion...........: 8.3
SubsystemVersion.........: 4.0
OSVersion................: 10.4
OriginalFilename.........: Oho.exe
LegalCopyright...........: Vulcan 2003-2007
MachineType..............: Intel 386 or later, and compatibles
CompanyName..............: Orb Networks
CodeSize.................: 196608
FileSubtype..............: 0
ProductVersionNumber.....: 8.3.0.0
EntryPoint...............: 0x52550
ObjectFileType...........: Executable application
```

Sigcheck

```
publisher................: Orb Networks
product..................: Duet
internal name............: Source Smith Tried
copyright................: Vulcan 2003-2007
original name............: Oho.exe
file version.............: 8.3
description..............: Glows Anger Hebrew
```

Portable Executable structural information

```
PE Sections...................:

Name        Virtual Address  Virtual Size  Raw Size  Entropy  MD5
UPX0                   4096        143360         0     0.00  d41d8cd98f00b204e9800998ecf8427e
UPX1                 147456        196608    193024     8.00  900641794a865f854bf0aa672e823e89
.rsrc                344064          4096      2560     3.26  e1d8e007e0a09da9bd00e852b0b6686b

PE Imports....................:

comdlg32.dll
        ChooseFontA

gdi32.dll
        EndPath

KERNEL32.DLL
        LoadLibraryA, GetProcAddress, VirtualProtect, VirtualAlloc, VirtualFree, ExitProcess

netapi32.dll
        NetGroupAdd

rpcrt4.dll
        RpcEpUnregister

imm32.dll
        ImmDisableIME

user32.dll
        DrawAnimatedRects

userenv.dll
        FreeGPOListW
```

First seen by VirusTotal

2012-02-26 03:50:29 UTC (28 minutes ago)

2012-02-26 03:50:29 UTC (28 minutes ago)

File names (max. 25)

1. fawi.exe