Datei shell.fne empfangen 2009.09.30 19:43:04 (UTC)			
Antivirus	Version	letzte aktualisierung	Ergebnis
a-squared	4.5.0.24	2009.09.30	Trojan.Peed!IK
AhnLab-V3	5.0.0.2	2009.09.30	Win-Trojan/Peed.40960.ES
AntiVir	7.9.1.27	2009.09.30	TR/Peed.A.1052
Antiy-AVL	2.0.3.7	2009.09.30	-
Authentium	5.1.2.4	2009.09.30	W32/Autorun.NG
Avast	4.8.1351.0	2009.09.29	Win32:Trojan-gen {Other}
AVG	8.5.0.412	2009.09.30	Crypt.FQT
BitDefender	7.2	2009.09.30	-
CAT-QuickHeal	10.00	2009.09.30	Trojan.Agent.gen
ClamAV	0.94.1	2009.09.30	-
Comodo	2474	2009.09.30	UnclassifiedMalware
DrWeb	5.0.0.12182	2009.09.30	-
eSafe	7.0.17.0	2009.09.30	Win32.TRPeed.a
eTrust-Vet	None	2009.09.30	-
F-Prot	4.5.1.85	2009.09.30	W32/Autorun.NG
F-Secure	8.0.14470.0	2009.09.30	-
Fortinet	3.120.0.0	2009.09.30	-
GData	19	2009.09.30	Win32:Trojan-gen {Other}
Ikarus	T3.1.1.72.0	2009.09.30	Trojan.Peed
Jiangmin	11.0.800	2009.09.27	-
K7AntiVirus	7.10.857	2009.09.30	Trojan.Win32.Malware
Kaspersky	7.0.0.125	2009.09.30	-
McAfee	5757	2009.09.30	Generic.dx
McAfee+Artemis	5757	2009.09.30	Generic.dx
McAfee-GW-Edition	6.8.5	2009.09.30	Heuristic.LooksLike.Win32.Peed.H
Microsoft	1.5005	2009.09.23	Trojan:Win32/Bumat!rts
NOD32	4471	2009.09.30	probably a variant of Win32/Agent
Norman	6.01.09	2009.09.30	Smalltroj.ITDL
nProtect	2009.1.8.0	2009.09.30	-
Panda	10.0.2.2	2009.09.30	Generic Trojan
PCTools	4.4.2.0	2009.09.30	Trojan.Agent.ADMK
Prevx	3.0	2009.09.30	-
Rising	21.49.22.00	2009.09.30	-
Sophos	4.45.0	2009.09.30	Mal/EncPk-GF
Sunbelt	3.2.1858.2	2009.09.30	Trojan.Peed.Gen
Symantec	1.4.4.12	2009.09.30	Trojan Horse

TheHacker	6.5.0.2.023	2009.09.30	-
TrendMicro	8.950.0.1094	2009.09.30	-
VBA32	3.12.10.11	2009.09.30	-
ViRobot	2009.9.30.1965	2009.09.30	-
VirusBuster	4.6.5.0	2009.09.30	-

weitere Informationen

File size: 40960 bytes

MD5...: 1fb1d0b167dd9850ced0eacbbaa5602f

SHA1..: a1d50e9e984a8a2bddf018b19d48279f2230b791

SHA256: 95bb9d1d2f6bb51dab10403fcb83616493516ff3b3f923eb3c9f4868475d1cb3

ssdeep: 768:ct0zTV6aYEreHAke33GNYB5SYO6W3FjLoLm66tlk0tARkI1LceW:ctSYaYEf
331BZO6WxoUkjG4O

PEiD..: -

PEInfo: PE Structure information

(base data)
entrypointaddress.: 0x5e65
timedatestamp.....: 0x4837a56f (Sat May 24 05:19:43 2008)
machinetype.......: 0x14c (I386)

(4 sections)
name viradd virsiz rawdsiz ntrpy md5
.text 0x1000 0x5000 0x5000 7.49 3a044f3b9020fe9b7cc370ef66797503
.rdata 0x6000 0xd86 0x1000 4.64 da39373d7ecbc259d88551f58fd8cb5d
.data 0x7000 0x81e0 0x2000 6.24 406a7b73a2b3a7e1a8a3a8b7d3fc6894
.data 0x10000 0x7a2 0x1000 3.54 00cc6b990a8291e55324c9879e589988

(5 imports)
> KERNEL32.dll: lstrlenA, GetTempPathA, GetSystemDirectoryA, GetWindowsDirectoryA, GetLastError, GetCurrentProcess, GetVersionExA, SetSystemPowerState, MultiByteToWideChar, WideCharToMultiByte, HeapFree, GetStringTypeA, LCMapStringW, LCMapStringA, LoadLibraryA, GetProcAddress, VirtualAlloc, GetOEMCP, GetACP, GetCPInfo, HeapReAlloc, GetProcessHeap, HeapAlloc, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, IsBadCodePtr, IsBadWritePtr, IsBadReadPtr, SetUnhandledExceptionFilter, WriteFile, RtlUnwind, GetCommandLineA, GetVersion, GetCurrentThreadId, TlsSetValue, TlsAlloc, TlsFree, SetLastError, TlsGetValue, ExitProcess, TerminateProcess, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, DeleteCriticalSection, GetModuleFileNameA, FreeEnvironmentStringsA, FreeEnvironmentStringsW, GetEnvironmentStrings, GetEnvironmentStringsW, HeapDestroy, HeapCreate, VirtualFree, GetStringTypeW
> USER32.dll: EnableWindow, ExitWindowsEx, SetForegroundWindow, SetActiveWindow, GetActiveWindow, IsWindow, GetForegroundWindow, IsWindowEnabled, GetParent
> ADVAPI32.dll: LookupPrivilegeValueA, AdjustTokenPrivileges, OpenProcessToken
> SHELL32.dll: SHGetMalloc, SHFileOperationA, SHGetSpecialFolderPathA, ShellExecuteA, SHBrowseForFolderA, SHGetPathFromIDListA, SHGetFileInfoA
> ole32.dll: CoCreateInstance

(0 exports)

RDS...: NSRL Reference Data Set
-

pdfid.: -

trid..: Win32 Executable MS Visual C++ (generic) (65.2%)
Win32 Executable Generic (14.7%)
Win32 Dynamic Link Library (generic) (13.1%)
Generic Win/DOS Executable (3.4%)
DOS Executable Generic (3.4%)

ThreatExpert info: http://www.threatexpert.com/report.aspx?md5=1fb1d0b167dd9850ced0eacbbaa5602f

sigcheck:
publisher....: n/a
copyright....: n/a
product.....: n/a
description..: n/a
original name: n/a
internal name: n/a
file version.: n/a
comments.....: n/a
signers.....: -
signing date.: -
verified.....: Unsigned

packers (Kaspersky): PE-Crypt.CF