Anti-Malware
Testing Laboratory

Anti-rootkit software testing on the detection and removal of malware (03.2007)

www.anti-malware-test.com

Table 2: Detailed results of testing for malicious program detection and removal by anti-rootkit solutions

Anti-rootkit \ Malware *	Backdoor.Win32. Haxdoor.fd	Backdoor.Win32. Padodor.ax	Monitor.Win32.Elite Keylogger.21	Monitor.Win32. SpyLantern.530	Trojan-Clicker.Win32. Costrat.af	Trojan-Spy.Win32. Goldun.np	Worm.Win32. Feebs.gt	Trojan-Proxy.Win32. Agent.lb	Trojan.Win32.DNSChanger.ih
Antivir Rootkit 1.0.1.12 Beta3	Successfully detected and removed all files	Detected and removed Daqjjn32.exe	Successfully detected and removed all files	Successfully detected and removed all files	Successfully detected and removed the file	Detected and removed MemMan.dll	Successfully detected and removed all files (including malware copies)	Successfully detected and removed malware file	Successfully detected and removed the file
AVG Antirootkit 1.1.0.29 Beta	Successfully detected and removed all files	Detected and renamed Daqjjn32.exe	Detected and renamed fltMgrnt.sys, mf2k.sys	Successfully detected and renamed all files	Successfully detected and removed the file	Detected and renamed MemMan.dll	Successfully detected and removed all files (including malware copies)	Successfully detected and renamed the file	Successfully detected and renamed the file
AVZ 4.23	Detected and removed tcpq32.dll, tcpq64.sys	Detected and removed Daqjjn32.exe, Opknnaei.dll	Detected and removed fltMgrnt.sys, mf2k.sys, tdiex.sys	Detected and removed cyfyweb.exe, cyfyweb.sys, cyfyweba.dll, cyfywebh.dll, cyfywebl.exe	Successfully detected and removed the file	Successfully detected and removed all files	Died when scanning had been started but detected and removed mswm32.dll when AVZ process had been renamed and AVZGuard turned on.	Successfully detected and removed the file	Detected the intercepts only
Bitdefender Antirootkit 1.2.0.0 Beta2	Detected and removed all files except of tcpq32.dll (couldn't remove)	Detected and renamed Daqjjn32.exe	Detected and removed all files but mslcache.dll (couldn't remove)	Detected and rename cyfywebl.exe, cyfyweb.exe, but the intercepts in user and kernel mode still took place.	Didn't detect the malware	Detected and renamed MemMan.dll	Successfully detected and removed all files (including malware copies)	Didn't detect the malware	Detected the file but couldn't rename or remove it.
F-Secure BlackLight 2.2.1055 Beta	Successfully detected and removed all files	Detected and renamed Daqjjn32.exe	Successfully detected and removed all files	Successfully detected and removed all files	Didn't detect the malware	Detected and renamed MemMan.dll	Successfully detected and removed all files	Successfully detected and renamed the file	Successfully detected and renamed the file

Anti-rootkit \ Malware *	Backdoor.Win32.Haxdoor.fd	Backdoor.Win32.Padodor.ax	Monitor.Win32.EliteKeylogger.21	Monitor.Win32.SpyLantern.530	Trojan-Clicker.Win32.Costrat.af	Trojan-Spy.Win32.Goldun.np	Worm.Win32.Feebs.gt	Trojan-Proxy.Win32.Agent.lb	Trojan.Win32.DNSChanger.ih
Gmer 1.0.12.12027	Detected and removed all files except of tcpq32.dll (couldn't remove)	Detected and renamed Daqjjn32.exe	Successfully removed the drivers registry keys but all malware files could be removed only manually.	Removed the registry keys for cyfyweb.exe, cyfyweb.sys	Successfully removed the registry keys but not active file remain in the stream.	Detected all files but was removed CsdDriver.sys only. The malware was active after system reboot.	Died after starting the scanning process	Detected the file but couldn't remove it	Detected the file, removed the intercepts and registry key (through registry editor). The file can be removed manually after system reboot.
McAfee Rootkit Detective 1.0.0.41 Beta	Successfully detected and removed all files	Detected and removed Daqjjn32.exe and registry key for running Opknnaei.dll	Detected and renamed dmdsk32.dll, mslcache.dll, verifsvr.exe. Renamed registry keys for fltMgrnt.sys, mf2k.sys, tdiex.sys drivers.	Successfully detected and renamed all files	Successfully renamed autorun keys but they were restored again after system reboot and the malware were active.	Successfully detected and renamed all files. Renamed MemMan.dll and its autorun registry key.	Detected and removed all files (including all malware copies) and autorun key for mswm32.dll (ShellServiceObjectDelayLoad)	Successfully detected and removed the file	Successfully detected and removed the file
Rootkit Unhooker 3.20.130.388	Successfully detected and removed all files	Detected and renamed Daqjjn32.exe	Successfully detected and removed all files	Successfully detected and removed all files	Successfully detected and removed the file	Successfully detected and removed all files	Detected the intercepts from mswm32.dll after that the file was removed using the Rku features	Detected the intercepts from msvcrt64.dll after that the file was removed using the Rku features	Detected the intercepts only
Sophos Anti-Rootkit 1.2.2	Successfully detected and removed all files	Detected and renamed Daqjjn32.exe	Successfully detected and removed all files	Successfully detected and removed all PE-files	Successfully detected and removed the file	Detected and removed MemMan.dll	Didn't detect the malware	Successfully detected and removed the file	Successfully detected and removed the file

Anti-rootkit \ Malware *	Backdoor.Win32.Haxdoor.fd	Backdoor.Win32.Padodor.ax	Monitor.Win32.EliteKeylogger.21	Monitor.Win32.SpyLantern.530	Trojan-Clicker.Win32.Costrat.af	Trojan-Spy.Win32.Goldun.np	Worm.Win32.Feebs.gt	Trojan-Proxy.Win32.Agent.lb	Trojan.Win32.DNSChanger.ih
Trend Micro RootkitBuster 1.6.0.1055 Beta	Detected and removed all files except of tcpq32.dll (couldn't remove)	Detected and removed Daqjjn32.exe and registry key for running Opknnaei.dll	Removed the registry keys for fltMgrnt.sys, mf2k.sys, tdiex.sys	Successfully detected and removed all files	Successfully removed the registry keys but not active file remain in the stream.	Detected and removed MemMan.dll and its autorun registry key	Detected and removed all files and autorun key for mswm32.dll (ShellServiceObjectDelayLoad)	Successfully detected and removed the file	Successfully detected and removed the file
UnHackMe 4.0	Detected autorun keys for tcpq64.sys but couldn't remove it. The malware ware active after system reboot.	Detected hidden Daqjjn32.exe process but couldn't removed the file. The malware ware active after system reboot.	Removed the registry keys for fltMgrnt.sys, mf2k.sys, tdiex.sys	Detected and removed cyfyweb.exe	Didn't detect the malware	Didn't detect the malware	Died during scanning process	Didn't detect the malware	Didn't detect the malware

* - malware names are specified in accordance with the Kaspersky Lab classification
Malware names in classifications of the leading anti-virus vendors

- completely detected and removed the rootkit
- the rootkit was successfully detected and removed, but insignificant traces of its presence in the system remain
- rootkit not detected or removal failed

Table 3: Malware names in classifications of leading antivirus vendors

Kaspersky Lab	Symantec	Trend Micro	McAfee	BitDefender	DrWeb
Backdoor.Win32.Haxdoor.fd	Backdoor.Haxdoor.E	BKDR_Generic	BackDoor-BAC.gen.e	Backdoor.Haxdoor.FA	BackDoor.Haxdoor.173
Backdoor.Win32.Padodor.ax	Backdoor.Berbew.T	BKDR_BERBEW.AA	BackDoor-AXJ	Backdoor.Padodor.AX	BackDoor.HangUp.27
Trojan-Clicker.Win32.Costrat.af	Backdoor.Rustock.B	TROJ_RUSTOCK.NBJ	Spam-Mailbot.c	Backdoor.Rustock.S	Trojan.Spambot
Monitor.Win32.EliteKeylogger.21	-	TROJ_Generic.ZA	-	-	-
Monitor.Win32.SpyLantern.530	Spyware.SpyLantern	-	-	-	-
Trojan-Proxy.Win32.Agent.lb	Backdoor.Trojan	TROJ_AGENT.HQY	Proxy-Agent.ba	Backdoor.ShellBot.C	BackDoor.Shellbot
Trojan-Spy.Win32.Goldun.np	Trojan.Goldun	TROJ_Generic	-	Trojan.Spy.Goldun.BP	Trojan.PWS.GoldSpy
Trojan.Win32.DNSChanger.ih	-	-	-	-	-
Worm.Win32.Feebs.gt	W32.Feebs	WORM_FEEBS.AZ	W32/Feebs.gen@MM	Win32.Worm.Feebs.CF	Win32.HLLM.Graz.based

Table 4: Description of the malware used in the test

Malware name *	Files of malware	Processes of malware	Comments
Backdoor.Win32.Haxdoor.fd	c:\windows\system32\klgcptini.dat c:\windows\system32\qz.dll c:\windows\system32\qz.sys c:\windows\system32\stt82.ini c:\windows\system32\tcpq32.dll c:\windows\system32\tcpq64.sys	System process winlogon.exe explorer.exe	All files, Windows registry keys for running tcpq32.dll, tcpq64.sys and system processes winlogon.exe, explorer.exe are hidden.
Backdoor.Win32.Padodor.ax	C:\WINDOWS\system32\Daqjjn32.exe C:\WINDOWS\system32\Opknnaei.dll	Daqjjn32.exe	Hidden file Daqjjn32.exe, processesDaqjjn32.exe and registry key for running Opknnaei.dll (ShellServiceObjectDelayLoad)
Monitor.Win32.EliteKeylogger.21	C:\WINDOWS\system32\dmdsk32.dll C:\WINDOWS\system32\drivers\fltMgrnt.sys C:\WINDOWS\system32\drivers\mf2k.sys C:\WINDOWS\system32\drivers\tdiex.sys C:\WINDOWS\system32\mslcache.dll C:\WINDOWS\system32\verifsvr.exe		Hide all files and autorun keys for fltMgrnt.sys, mf2k.sys, tdiex.sys
Monitor.Win32.SpyLantern.530	c:\windows\system32\cyfyweb.cfg c:\windows\system32\cyfyweb.chm c:\windows\system32\cyfyweb.exe c:\windows\system32\cyfyweb.sys c:\windows\system32\cyfyweba.dll c:\windows\system32\cyfywebcc.exe c:\windows\system32\cyfywebh.dll c:\windows\system32\cyfyweb	cyfyweb.exe cyfywebl.exe	Hide all files, directories and process.
Trojan-Clicker.Win32.Costrat.af	C:\WINDOWS\system32:huy32.sys:$DATA		Hidden huy32.sys file and its autorun key
Trojan-Spy.Win32.Goldun.np	C:\WINDOWS\system32\CsdDriver.sys C:\WINDOWS\system32\MemMan.dll		Hidden MemMan.dll file and its registry key (ShellServiceObjectDelayLoad)
Worm.Win32.Feebs.gt	c:\WINDOWS\system32\msvx.exe c:\WINDOWS\system32\mswm32.dll c:\WINDOWS\system32\msdi + many own copies throughout the system disk	System process svchost.exe	Hide all files and the autorun key for mswm32.dll (ShellServiceObjectDelayLoad)
Trojan-Proxy.Win32.Agent.lb	c:\windows\system32\msvcrt64.dll		Hide own file and the autorun key (ShellServiceObjectDelayLoad)
Trojan.Win32.DNSChanger.ih	C:\WINDOWS\system32\kdaup.exe		Hidden file, no active prosesses, the registry key for Winlogon with parameter System = kdeiy.exe don't hide

* - malware names are specified in accordance with the Kaspersky Lab classification

Table 5: Malware disguise method (intercepted API)

Malware name *	Disguise method (intercepted API)
Backdoor.Win32.Haxdoor.fd	NtCreateProcess NtCreateProcessEx NtOpenProcess NtOpenThread NtQueryDirectoryFile NtQuerySystemInformation
Backdoor.Win32.Padodor.ax	ntdll.dll:NtQuerySystemInformation ntdll.dll:RtlGetNativeSystemInformation ntdll.dll:ZwQuerySystemInformation kernel32.dll:FindNextFileW kernel32.dll:Process32Next advapi32.dll:RegEnumKeyA advapi32.dll:RegEnumKeyExA advapi32.dll:RegEnumKeyExW advapi32.dll:RegEnumKeyW advapi32.dll:RegEnumValueA advapi32.dll:RegEnumValueW
Monitor.Win32.EliteKeylogger.21	NtCreateKey NtEnumerateKey NtOpenKey Driver-filter of file system
Monitor.Win32.SpyLantern.530	advapi32.dll:EnumServicesStatusA advapi32.dll:EnumServicesStatusW NtQueryDirectoryFile NtQuerySystemInformation
Trojan-Clicker.Win32.Costrat.af	Driver-filter of file system SYSENTER/Int 2E
Trojan-Spy.Win32.Goldun.np	NtEnumerateKey NtEnumerateValueKey NtQueryDirectoryFile
Worm.Win32.Feebs.gt	kernel32.dll:FindFirstFileA kernel32.dll:FindFirstFileW kernel32.dll:FindNextFileA kernel32.dll:FindNextFileW kernel32.dll:OpenProcess ntdll.dll:NtQuerySystemInformation ntdll.dll:RtlGetNativeSystemInformation ntdll.dll:ZwQuerySystemInformation advapi32.dll:RegEnumKeyA advapi32.dll:RegEnumKeyExA advapi32.dll:RegEnumKeyExW advapi32.dll:RegEnumKeyW advapi32.dll:RegEnumValueA advapi32.dll:RegEnumValueW
Trojan-Proxy.Win32.Agent.lb	kernel32.dll:FindFirstFileA kernel32.dll:FindFirstFileW kernel32.dll:FindNextFileA kernel32.dll:FindNextFileW kernel32.dll:Module32First kernel32.dll:Module32FirstW kernel32.dll:Module32Next kernel32.dll:Module32NextW advapi32.dll:RegEnumValueA advapi32.dll:RegEnumValueW
Trojan.Win32.DNSChanger.ih	ntdll.dll:NtCreateThread ntdll.dll:NtQueryDirectoryFile ntdll.dll:ZwCreateThread ntdll.dll:ZwQueryDirectoryFile

* - malware names are specified in accordance with the Kaspersky Lab classification