


**Test results for detection and removal of rootkits by  
antivirus/anti-rootkit software  
(Test#2 - 01.2008)**

**Table 1a: Test results for antivirus/anti-rootkit products**

Antivirus / Anti-rootkit	Award	Total points		
		Malware (6 max)	Proof-of-concept (2 max)	Total (max 8)
Rootkit Unhooker 3.7.300	 <b>Gold Anti-Rootkit Protection Award</b>	5.5	2	7.5
GMER 1.0.13		5.5	1.5	7
Kaspersky Anti-Virus 7.0		4.5	2	6.5
Avira Rootkit Detection 1.0		5	1.5	6.5
AVG Anti-Rootkit 1.1	 <b>Silver Anti-Rootkit Protection Award</b>	4	1.5	5.5
Panda AntiRootkit version 1.08		4	1.5	5.5
Sophos Anti-Rootkit 1.3.1		4.5	1	5.5
Dr.Web 4.44		5	0	5
Trend Micro RootkitBuster 1.6		4	1	5
Symantec Anti-Virus 2008	 <b>Bronze Anti-Rootkit Protection Award</b>	4	0.5	4.5
F-Secure Anti-Virus 2008		2.5	1.5	4
McAfee Rootkit Detective 1.1		3	0.5	3.5
BitDefender Antivirus 2008	<b>Failed</b>	3	0	3
McAfee VirusScan Plus 2008		1.5	0	1.5
Eset Nod32 Anti-Virus 3.0		1	0	1
Trend Micro Antivirus plus Antispyware 2008		1	0	1

**Table 1b: Test results for antivirus products**

Antivirus	Malware (6 max)	Proof-of-concept rootkits (2 max)	Total points
Kaspersky Anti-Virus 7.0	4.5	2	6.5
Dr.Web 4.44	5	0	5
Symantec Anti-Virus 2008	4	0.5	4.5
F-Secure Anti-Virus 2008	2.5	1.5	4
BitDefender Antivirus 2008	3	0	3
McAfee VirusScan Plus 2008	1.5	0	1.5
Eset Nod32 Anti-Virus 3.0	1	0	1
Trend Micro Antivirus plus Antispyware 2008	1	0	1

**Table 1c: Test results for Anti-rootkit products**

Anti-rootkit	Malware (6 max)	Proof-of-concept rootkits (2 max)	Total points
Rootkit Unhooker 3.7.300	5.5	2	7.5
GMER 1.0.13	5.5	1.5	7
Avira Rootkit Detection 1.0	5	1.5	6.5
AVG Anti-Rootkit 1.1	4	1.5	5.5
Panda AntiRootkit version 1.08	4	1.5	5.5
Sophos Anti-Rootkit 1.3.1	4.5	1	5.5
Trend Micro RootkitBuster 1.6	4	1	5
McAfee Rootkit Detective 1.1	3	0.5	3.5

[Detailed results for any antivirus and anti-rootkit](#)

[Description of the malicious programs and proof-of-concept rootkits used in the test](#)

[Malware disguise method \(intercepted API\)](#)

[Malware names in classifications of leading antivirus vendors](#)

**Table 2: Test results for the detection and removal of malware with rootkit technologies by antivirus/anti-rootkit software**

Antivirus / Malware	Trojan-Spy.Win32. Goldun.hn	Trojan-Proxy. Win32.Wopla.ag	SpamTool. Win32.Mailbot.bd	Monitor.Win32. EliteKeylogger.21	Rootkit.Win32. Agent.ea	Rootkit.Win32. Podnuha.a	Total points
BitDefender Antivirus 2008	++	++	-/-	++	-/-	-/-	3
Dr.Web 4.44	++	++	++	-/-	++	++	5
F-Secure Anti-Virus 2008	++	+/-	+/-	+/-	-/-	-/-	2.5
Kaspersky Anti-Virus 7.0	++	++	++	++	+/-	-/-	4.5
Eset Nod32 Anti-Virus 3.0	++	-/-	-/-	-/-	-/-	-/-	1
McAfee VirusScan Plus 2008	++	-/-	+/-	-/-	-/-	-/-	1.5
Symantec Anti-Virus 2008	++	++	++	++	-/-	-/-	4
Trend Micro Antivirus plus Antispyware 2008	++	-/-	-/-	-/-	-/-	-/-	1
<b>Anti-rootkit</b>							
AVG Anti-Rootkit 1.1	++	++	++	++	-/-	-/-	4
Avira Rootkit Detection 1.0	++	++	++	++	++	-/-	5
GMER 1.0.13	+/-	++	++	++	++	++	5.5
McAfee Rootkit Detective 1.1	++	++	+/-	+/-	-/-	-/-	3
Panda AntiRootkit version 1.08	++	++	+/-	++	+/-	-/-	4
Rootkit Unhooker 3.7.300	++	++	++	++	++	+/-	5.5
Sophos Anti-Rootkit 1.3.1	++	++	++	++	+/-	-/-	4.5
TrendMicro RootkitBuster 1.6	++	+/-	++	++	+/-	-/-	4

**Table 3: Test results for the detection and removal of proof-of-concept rootkits by antivirus/anti-rootkit software**

Antivirus / Proof-of-concept rootkit	Unreal A 1.0.1	RkDemo v1.2	FuTo	HideToolz	Total points
BitDefender Antivirus 2008	-	-	-	-	0
Dr.Web 4.44	-	-	-	-	0
F-Secure Anti-Virus 2008	-	+	+	+	1.5
Kaspersky Anti-Virus 7.0	+	+	+	+	2
Eset Nod32 Anti-Virus 3.0	-	-	-	-	0
McAfee VirusScan Plus 2008	-	-	-	-	0
Symantec Anti-Virus 2008	+	-	-	-	0.5
Trend Micro Antivirus plus Antispyware 2008	-	-	-	-	0
<b>Anti-rootkit</b>					
AVG Anti-Rootkit 1.1	-	+	+	+	1.5
Avira Rootkit Detection 1.0	-	+	+	+	1.5
GMER 1.0.13	-	+	+	+	1.5
McAfee Rootkit Detective 1.1	-	-	-	+	0.5
Panda AntiRootkit version 1.08	+	+	-	+	1.5
Rootkit Unhooker 3.7.300	+	+	+	+	2
Sophos Anti-Rootkit 1.3.1	-	-	+	+	1
TrendMicro RootkitBuster 1.6	-	-	+	+	1

+ / +	- rootkit was successfully detected on the system (file, process or function hook) and deleted (1 point)
+ / -	- rootkit was successfully detected on the system, but couldn't be deleted (0.5 points)
-	- rootkit was not detected on the system (0 points)