



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

www.anti-malware-test.com

Table 1a: Summary of anti-rootkit testing results

Anti-rootkit solution	Successfully removed	Rank
Antivir Rootkit 1.0.1.12 Beta3	9 from 9	Excellent
AVG Antirootkit 1.1.0.29 Beta		
Trend Micro RootkitBuster 1.6.0.1055 Beta		
McAfee Rootkit Detective 1.0.0.41 Beta	8 from 9	Good
Rootkit Unhooker 3.20.130.388		
F-Secure BlackLight 2.2.1055 Beta		
Sophos Anti-Rootkit 1.2.2		
AVZ 4.23	6 from 9	
Gmer 1.0.12.12027		
Bitdefender Antirootkit 1.2.0.0 Beta2		
UnHackMe 4.0	2 from 9	

Table 1b: Summary of anti-rootkit testing results

Anti-rootkit solution	Successfully detected and removed		Rootkit not detected or removal failed
	Successfully detected and removed	Traces of infection remaining*	
Antivir Rootkit 1.0.1.12 Beta3	7	2	0
AVG Antirootkit 1.1.0.29 Beta	6	3	0
AVZ 4.23	4	4	1
Bitdefender Antirootkit 1.2.0.0 Beta2	1	5	3
F-Secure BlackLight 2.2.1055 Beta	6	2	1
Gmer 1.0.12.12027	1	5	3
McAfee Rootkit Detective 1.0.0.41 Beta	7	1	1
Rootkit Unhooker 3.20.130.388	7	1	1
Sophos Anti-Rootkit 1.2.2	6	2	1
Trend Micro RootkitBuster 1.6.0.1055 Beta	5	4	0
UnHackMe 4.0	0	2	7

[Detailed results for any malicious program using in the test](#)

[Description of the malicious programs used in the test](#)

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

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