FEATURE

ANTI-STEALTH FIGHTERS: TESTING FOR ROOTKIT DETECTION AND REMOVAL

Andreas Marx & Maik Morgenstern
AV-Test.org, Germany

'Most people don't even know what a rootkit is, so why should they care about it?' (Thomas Hesse, President, Global Digital Business, Sony BMG [2005])

Malware is becoming more and more complex every day. The number of newly discovered malware samples is skyrocketing, but that's not the only challenge for the AV industry. In most cases, we're looking at malware that is built in a modular way, with plug-ins that support new features such as hiding the malware's presence from the user and from AV products. While it is easy for a good signature-driven product to find a known sample that has not yet been activated, it is becoming increasingly challenging to detect the sample once it is running and trying to hide itself and other malicious components. On the *Windows* platform the hidden objects usually include services and processes, registry keys and values, as well as directories and files.

Shortly after the infamous '*Sony* rootkit' was released in 2005 [1], *AV-Test.org* started testing for rootkit detection. At that time, most AV programs could easily be fooled. As soon as the rootkit was running, the system was reported to be clean – even if a hidden piece of malware was running in the background, sending out junk emails and attempting to infect further computers. Until now, our anti-rootkit test results have only been published in certain hard copy magazines and in German. In an attempt to close this information gap we have decided to present the results of two recent tests here in *VB*.

The first part of our research, a dedicated anti-rootkit test covering 27 products on *Windows XP* (32-bit, SP2) and *Vista* (32-bit, RTM), was published in the German *ComputerBild* magazine [2]. The second part, a small-scale anti-rootkit review as part of a comprehensive AV test of 17 tools on *Windows Vista* (32-bit, RTM), was performed for the German *c't* magazine [3].

STEP 1: SELECTING THE SAMPLES

Before a review can start, samples of standalone rootkits and malware using rootkit technologies must be selected to test against. The manual and automated analysis of such samples is tricky and good reverse-engineering skills are required. For a less comprehensive basic check it might be sufficient just to compare the system in a clean state (without any malware), in an infected state (with the activated rootkit running on the system) and in the state in which the malware-infected system has been booted from a known clean installation (so no files and registry entries are hidden, as the rootkit is not active). For a good review, further analysis needs to be performed to check for other hidden objects on the infected system. This might take several hours per sample.

For the part of the *ComputerBild* review that focused on *Windows XP*, we used a total of 60 samples, including two versions of the *Sony* rootkit (XCP/First4Internet rootkit) found on CDs and one copy of the Alpha DVD (Settec) rootkit used on the German DVD *Mr. and Mrs. Smith* [4]. Malware samples included several variants of Agent, Delf, Dragonbot, Feebs, Fuzen, Graybird, Hacker Defender, Haxdoor, Hider, Hupigon, iBill, Kenfa, Klone, Madtol, Maslan, NsAnti, NT Illusion, NT Rootkit, Nuwar, Pakes, PC Client, QQPass, Rontokbro, Small, Tibs, Wopla and X-Shadow. Some of the malware listed is included on the WildList. The exact samples used for the test have already been shared with the tested AV companies. The *Windows Vista* test for *ComputerBild* was performed with a much smaller set of samples and will not be discussed in detail.

The *c't* review on *Windows Vista* included just six samples which run well on *Vista*, covering the two aforementioned CD rootkits, two versions of Hacker Defender, as well as one copy of NT-Illusion and a copy of Vanquish. These rootkits are a little older, but still work well on *Vista* as long as User Account Control (UAC) has been switched off (a step that was performed prior to testing).

We only used 'real' PCs (equipped with a Core 2 Duo 6600 processor, 2 GB RAM and a 400 GB NTFS-formatted hard disk) for the tests. The reason for this is that a lot of malware checks for the presence of virtualization products such as *VMware* or *Virtual PC*, and in such cases the malicious software might behave differently. Besides this, the helper tools installed on a guest operating system might be incompatible or cause problems with the rootkits, as they also try to hook critical system functions.

STEP 2: TESTING FOR DETECTION OF INACTIVE ROOTKITS

It is important to check whether the AV products are able to detect the rootkits before installation when they are easy to identify using standard AV techniques such as signature scanning. This will demonstrate the products' ability to block the malware before it can harm the system. This test should be performed both with the on-demand scanner and especially using the on-access guard. If the guard cannot

prevent the download and installation of the rootkit, a proper detection will be much more difficult.

Preparation for this test is straightforward and does not differ from any other tests: one only needs to install the test product on a known clean system (e.g. from a *Windows XP SP2* image file), update the product to the latest available version (this might involve a few reboots), and create an image of this system. Once this has been done, the PC will not need to be connected to the Internet again, and will only be used in a secure test lab environment. The selected samples will then be used to test the products. This only takes a few minutes per tool, including proper documentation and the creation of report files.

Testing web-based online scanners (usually implemented as ActiveX controls or Java applets) is a bit trickier, as these tools require a working Internet connection and update themselves regularly. Special precautions must be taken, such as limiting the Internet connection (so that only the required IP addresses from the AV company's servers and ports can be accessed). Furthermore, the tests of online scanners have to be performed at almost the same time, in order for the products to be in a comparable state. In order to be able to reproduce the test results at a later time, it is a good idea not only to create image files of the system, but also to capture all the Internet traffic and to create screenshots or videos of the entire test, showing each detection and miss in detail.

STEP 3: TESTING FOR DETECTION AND REPAIR OF ACTIVELY RUNNING ROOTKITS

The testing of products against active rootkit samples is actually the 'real' rootkit test, showing how well the products handle hidden objects, not only regarding detection but also with regard to disabling the rootkit and removing all of its components.

There are many different possible scenarios in which a rootkit could enter a system. One is that the computer is not running an AV solution, and another is that the AV product on the system is outdated or doesn't have signatures for the specific version of the rootkit in its database. For our testing, we used the scenario that the AV product is up to date and working, but the on-access protection is turned off, so the rootkit can be installed without any warning messages from the guard. This way, we do not need to install and update the product again and again, which saves a lot of time. Besides this, we can use images of the products for testing, thus making the reproduction of the results (when required) a lot easier, as the same version is used in all cases.

After the malware is executed on the test system, it is important to check whether the rootkit has installed properly and is running. This includes checking that all the files and registry entries that should be present according to our previous analysis are actually present, and that the objects that should be hidden are hidden.

We then turn the guard back on and if anything is detected we let the product perform its cleaning routine (if any). We then perform an on-demand scan using the default settings of the product. Again, if anything is detected we let the product perform the suggested repair routine (if any). The system is rebooted if the tool prompts for this to complete the cleaning operation.

Straight after this, we need to determine whether the rootkit (and the related malware) is still active and find out which components have been removed (or renamed) and which have not been handled. Of course, the job of the AV tool should include the removal of all active traces of the malware, but it should not be considered a fault if some inactive traces, such as harmless text files, are left on the system. Scanner report files and snapshots created before and after the malware execution and cleaning are a good way of documenting the actions of the tool, but we have to be sure that these tools deal properly with the rootkits used during the testing.

For every test run, only one product should be checked against a single rootkit, and afterwards the system must be restored from a clean image file before the next test can start. Testing against active samples usually requires around 20 to 30 minutes per sample, depending on the documentation and quality requirements of the test. So the test of a single product against 60 samples can easily take 20 to 30 hours. As performing such tests requires quite a lot of knowledge and experience, they cannot easily be automated. However, the tasks of the tester can be supported by various self-developed helper tools to make the work easier to perform.

As with the test against inactive rootkits, the testing of online scanners against active samples is more problematic than testing standalone AV products. Once again, the problems include the reproducibility of the results and the fact that a system with actively running malware needs to be connected to the Internet for a short amount of time.

LOOKING AT THE RESULTS

In the case of the *ComputerBild* review on *Windows XP*, all products (in their most current versions) were updated and then frozen on 25 October 2007. The only exceptions were the online scanners, which were tested on 25 October and 2 November 2007.

ComputerBild review (Windows XP Home Edition, 32-bit, SP2) [1]							
Product	**Version**	**Detection of inactive samples**	**Detection of actively running rootkits**	**Detection of malware hidden by rootkits**	**Removal of inactive samples**	**Removal of actively running rootkits**	**Removal of malware hidden by rootkits**
	Reference (max) ->	30	30	30	27	30	30
INTERNET SECURITY SUITES							
Avira AntiVir Premium Security Suite	7.06.00.168	28	29	30	25	7	7
BitDefender Internet Security 2008	11.0.13	30	28	29	27	23	27
Bullguard Internet Security Suite	7.0.0.27	30	7	10	27	4	0
G DATA InternetSecurity 2008	18.0.7227.533	30	9	4	27	7	0
Kaspersky Internet Security 7.0	7.0.0.119	28	24	28	25	22	25
Kaspersky Personal Security Suite V	6.0.2.621	28	21	27	25	19	17
Norton Internet Security 2008	15.0.0.60	25	18	25	25	18	25
WEB-BASED ONLINE SCANNER							
BitDefender Online Scanner	1.0 Build 2422	30	5	3	27	2	0
F-Secure Online Virus Scanner	3.2 Beta (1.0.64)	24	27	26	24	23	23
Kaspersky Online Scanner	5.0.98.1	28	6	21	25	0	0
Microsoft Windows Live Safety Scanner	1.1.3007.0	20	17	25	19	10	8
Panda Security ActiveScan	5.54.01	28	25	26	27	15	26
Trend Micro HouseCall	6.6 (1103-1060)	27	8	5	27	7	1
SPECIALIZED ANTI-ROOTKIT TOOLS							
AVG Anti-Rootkit Free	1.1.0.42	n/a	30	29	n/a	26	27
Avira RootKit Detection	1.0.1.17 Beta	n/a	28	30	n/a	23	28
BitDefender RootKit Uncover	1.0 Beta 2	n/a	24	28	n/a	16	12
F-Secure Blacklight	2.2.1064.0 Beta	n/a	28	28	n/a	20	27
GMER	1.0.13.12551	n/a	30	28	n/a	19	26
IceSword	1.2.2.0	n/a	25	26	n/a	10	6
McAfee Rootkit Detective	1.1.0.0	n/a	26	29	n/a	21	28
Microsoft Rootkit Revealer	1.71.0.0	n/a	15	14	n/a	n/a	n/a
Panda Security Anti-Rootkit	1.07.00	n/a	24	28	n/a	22	27
Rootkit Unhooker LE	3.7.300.509	n/a	30	30	n/a	22	28
Safe'n'Sec Pro	3.0.0.4104	n/a	18	9	n/a	7	3
Sophos Anti-Rootkit	1.3.1 (1.07)	n/a	26	26	n/a	17	24
System Virginity Verifier	2.3	n/a	15	3	n/a	10	3
Trend Micro Rootkit Buster	1.6 Beta	n/a	30	29	n/a	20	24

We first checked the products' on-demand detection and removal of inactive samples. This already revealed some missing signatures in the scanners' databases. The results of the on-access scanning were identical to the on-demand results, so they are not listed separately in the results table. None of the dedicated anti-rootkit tools we tested had an integrated on-demand scanner, so no results are available in this category. The maximum number of samples the tools could detect was 30 dedicated rootkits, and no more than 27 rootkits could be removed because we used the original (and thus, write-protected) CD and DVD media with the three 'commercial' rootkits.

The test with 30 active rootkits and 30 items of other malware using rootkit technologies was a lot more challenging both for the testers and the products. On average, the specialized anti-rootkit utilities were able to detect around 80% of the test samples. The security suites detected a little more than 66% of the rootkit infections and the online scanners performed the worst, with a detection rate of just 53%. We encountered significant problems in several cases in which the tools either crashed or hung during or after finishing a scan (in these cases we counted the rootkit as not detected).

Rootkit removal proved even more problematic. Once again the specialized tools performed the best on average, with a disinfection score of a little below 66% of the samples. However, the security suites were not able to clean more than 50% of the infections and the online scanners were almost useless, with a disinfection rate of only around 32%.

We also saw a good number of crashes and related problems in this section, but sometimes the rootkit was gone after a bluescreen and one or two reboots. Tools like *Avira RootKit Detection* sometimes removed the *Windows* explorer.exe file, so the system could not be started after a 'successful' disinfection run. *McAfee Rootkit Detective* renamed the original *Internet Explorer* iexplore.exe file in two cases. Sporadically, *AVG Anti-Rootkit Free* also tried to remove some system files, leaving the system in an unbootable state. (Note: this list of problems is not comprehensive.)

The *c't* magazine review on *Windows Vista* only included 'pure' anti-virus programs. The tools were last updated and frozen on 2 October 2007. To our surprise, the detection rate of inactive samples reached just 90% on average, even though most of the rootkits used were

c't review (Windows Vista Ultimate Edition, 32-bit, RTM) [2]				
Product	**Version**	**Detection of inactive samples**	**Detection of actively running rootkits**	**Removal of actively running rootkits**
	Reference (max) ->	6	6	6
Avast! Antivirus Professional Edition	4.7.1043 (000778-1)	6	3	3
AVG Anti-Malware	7.5.488 (269.13.37 / 1042)	6	0	0
Avira Antivir PersonalEdition Premium	7 Build 308 (7.06.00.18)	4	6	3
G Data AntiVirus 2008	18.0.7227.533 (8434 / 393)	6	3	3
BitDefender Antivirus 2008	11.0.0.25 (7.15077)	6	5	5
CA Anti-Virus Plus 2008	4.0.0.130 (31.1.0 / 5178)	6	6	4
ClamWin Free Antivirus	0.91.2 (4 / 4452)	3	3	1
Dr Web Antivirus für Windows	4.44.0.09170	2	2	2
F-Secure Anti-Virus 2008	6.80.2610.0 (2007-10-02_01)	6	6	6
Ikarus virus.utilities	1.0.60 (1.1.13)	6	2	1
Kaspersky Anti-Virus	7.0.0.119	6	6	2
McAfee VirusScan 2008	11.2.121 (5100-5131)	6	2	2
Microsoft Windows Live OneCare	1.6.2111.32 (1.1.2803.0)	5	1	1
Eset Nod32 Antivirus	2.70.39.0 (10902)	5	5	5
Norton Antivirus 2008	15.0.0.58	6	6	6
Panda Security Antivirus 2008	3.00.00 (2.1.29.0)	6	6	6
Trend Micro Antivirus + Antispyware 2008	16.00.1413 (8.500-4.752.90)	6	5	5

released during 2005 and 2006. Only four of the six installed rootkits could be detected by an average tool and the cleaning rate was even lower with 54%. *AVG* (with one of the best standalone tools on *Windows XP*) performed poorly with no detection or cleaning of running rootkits on *Vista*. Tools from *Microsoft*, *Ikarus* and *Doctor Web* also demonstrated the need for some significant improvements on this platform.

CONCLUSION

Tests of the active rootkit detection and cleaning features of anti-malware products are rather time consuming and require a lot of resources to perform. However, programmers and testers should dedicate more attention to these features, as most AV tools still perform poorly in this area. Without proper anti-rootkit features a protection program may give the user the wrong impression about the status of his PC.

A step in the right direction could be to focus on providing bootable rescue media, too: this might be the product installation CD or a CD or disk that a user can create and update himself [5, 6]. When the system is started from this media, the rootkit cannot be activated on the system, so a scanner would be able to see all files and registry entries which would usually be hidden. This way, the scanner could detect and delete all rootkit and malware components as long as the signature database is up to date and comprehensive.

REFERENCES

[1] Russinovich, M. Inside Sony's rootkit. Virus Bulletin, December 2005, p.11. http://www.virusbtn.com/virusbulletin/archive/2005/12/vb200512-sonys-rootkit.

[2] Melfsen, T.; Badenius, F.; Pursche, O. Wurzelbehandlung (Root Treatment). ComputerBild 26/2007, pp.74–95, Axel Springer Verlag, Hamburg, Germany. http://www.computerbild.de/.

[3] Knop, D.; Schmidt, J. Auf der Pirsch: 17 Antivirenlösungen unter Windows Vista und XP. (Going Hunting: 17 AV solutions for XP and Vista). c't 01/2008, pp.92–103, Verlag Heinz Heise, Hanover, Germany. http://www.heise.de/.

[4] Florio, E. Stories from the DRM world: the Settec case. Virus Bulletin, April 2006, p.10. http://www.virusbtn.com/virusbulletin/archive/2006/04/vb200604-smith.

[5] Marx, A. Rescue Me: Updating Anti-Virus Rescue Systems. Virus Bulletin May 2002, pp.10–12. http://www.virusbtn.com/pdf/magazine/2002/200205.pdf.

[6] Marx, A. Rescue Me 2: Disinfection With Bootable Rescue Media. Virus Bulletin March 2004, pp.14–16. http://www.virusbtn.com/pdf/magazine/2004/200403.pdf.