In-the-wild Rootkit Remediation Comparative Analysis 2015 Q3

Table of Contents

1 Introduction

"A rootkit is a stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer."[1] If a computer is already infected, it is not an easy task to detect and remove the rootkit. As per the definition, rootkit detection is difficult; sometimes rootkits bury themselves so deep in the system that removal is anything but trivial. Not all malware has rootkit functionalities, but it is common practice among malware distributors that first a rootkit component is installed on the infected system, to provide long persistence on the system, and this rootkit installs other components (sometimes simple user-mode malware) so criminals can profit. And even if the user-mode malware is detected and removed, the rootkit operators can drop other fresh malware to the infected system.

Zemana Ltd. commissioned MRG Effitas to conduct a comparative analysis of its Zemana AntiMalware product, and other prevalent rootkit remediation, second-opinion malware scanners and anti-malware system rescue tools.

1.1 Zemana AntiMalware

Zemana AntiMalware is a second-opinion malware scanner designed to rescue a computer from malware that has infected the computer despite all the security measures taken. It uses cloud-based scanning to reduce detection time for new virus outbreaks and to improve scanning performance. The tested version was 2.16.1.886

1.2 Competitor products tested

- TDSS killer 3.0.0.44
- Emsisoft Free Emergency Kit 10.0.0.5488
- MalwareBytes Anti Malware 2.1.8.1057
- HitmanPro 3.7.9 build 242

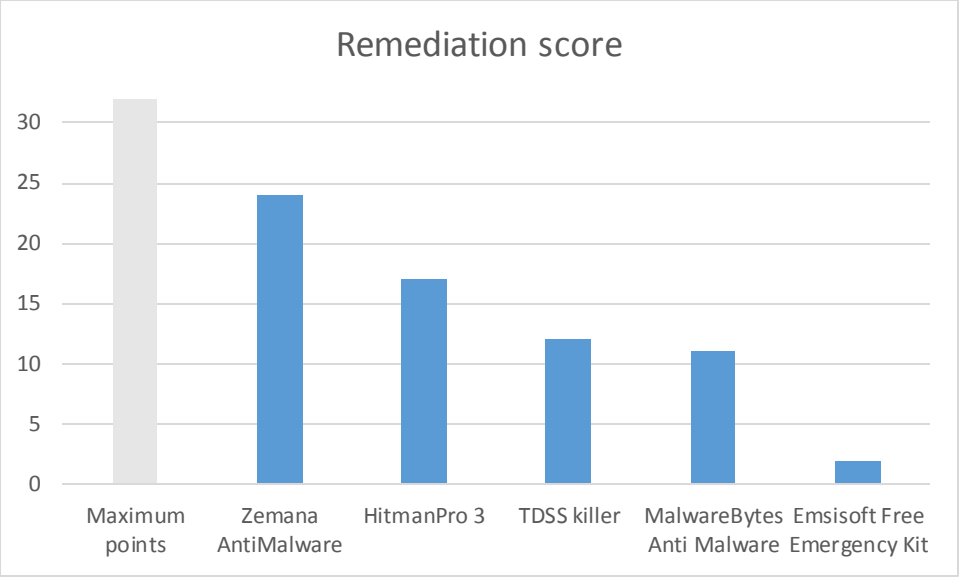
TDSS Killer is declared as a utility with support of specific rootkit removal. Other Kaspersky products like Kaspersky Virus Removal Tool or Kaspersky Antivirus are considered to cover more rootkits (and malware in general), thus comparing against those products one could expect better results. Not all rootkits from the test are declared as supported by the TDSS killer utility, so KVRT would have considered as a more proper product into the test.

1.3 Executive summary

We tested the rootkit remediation, second-opinion malware scanners and anti-malware system rescue tools against eight different rootkits, which have been prevalent in-the-wild over the past 3-4 years. First, the system was infected with the rootkit, and when the rootkit fully installed itself, we scanned the system for the presence of the rootkit, and used the malware removal function in the scanner to remove the rootkit. Then we used forensic tools to evaluate the effectiveness of the remediation process.

[1] https://en.wikipedia.org/wiki/Rootkit

Final results



Based on this report, Zemana AntiMalware proved to be the best rootkit remediator among the tested products during the test.

2 Tests employed and results

This rootkit remediation test was performed as follows: We acquired a dropper for the rootkit, installed the rootkit on a clean system, rebooted the system, scanned the system for rootkit infections, and removed any artifacts found. The scoring is based on the level of detection and remediation.

When conducting these tests, we tried to simulate normal user behaviour. We are aware that a "Real World" test cannot be conducted by a team of professionals inside a lab because we understand how a rootkit works, how it attacks and how such attacks could be prevented. Simulating normal user behaviour means that we paid special attention to all alerts given by security applications.

Cat-and-Mouse Game: It is no secret that when it comes to rootkits, vendors have a lot of work on their hands. Kernel mode rootkits, user-mode rootkits, Master Boot Record infectors (MBR bootkits), Volume Boot Record infectors, file-less malware, WMI based malware, and Powershell malware are just a few examples of techniques used by malware authors to hide their rootkits from Antivirus engines. Rootkits often show the clean, original content to the system when accessed via traditional, high level API-functions.

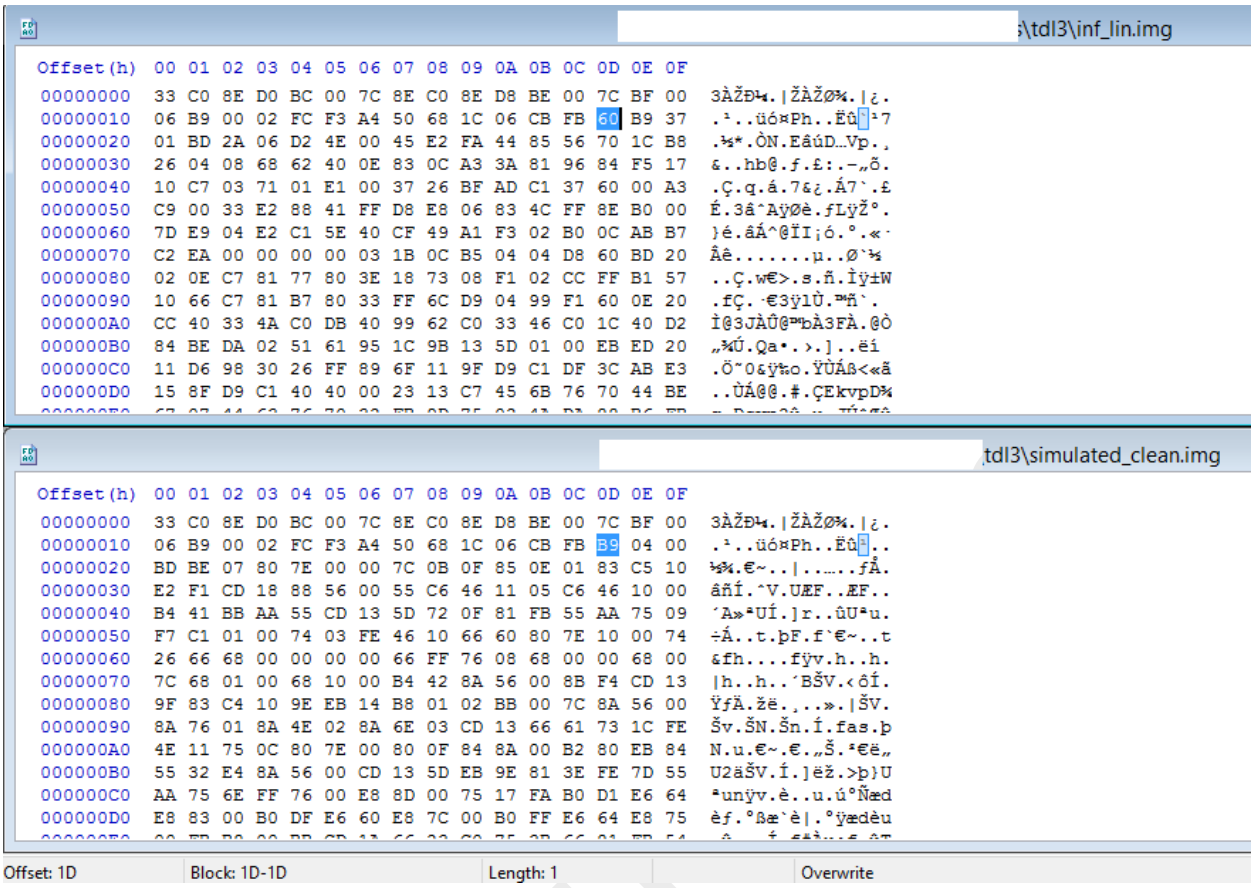


Figure 1 - MBR as seen from infected system and clean system

All tests were carried out in a combination of virtualized and physical hardware environment, on a fully patched Windows 7 32-bit. We used physical hardware where the rootkit dropper was virtualization aware, and refused to install in a virtualized environment. We used 32-bit Windows because not all (but most) rootkits were fully 64-bit compatible.

The test was carried out between June 29 and July 21, 2015.

2.1 High-level overview of the tests

Sample selection is of fundamental importance to this and all similar tests. The type of samples used is selected by MRG Effitas on the basis of a mixture of criteria, centering about key relevancies:

1. Prevalence – they are widespread (among rootkits) and so represent the most common threats.
2. Innovation – they employ innovative techniques to counter security measures.
3. It is malware having rootkit capabilities, by hiding its presence from the user and security software.

During our tests we did not use the latest zero day rootkits, because it is very hard to acquire working recent samples from rootkits. On the other hand, the number of different rootkit techniques is quite limited, and if a rootkit hiding technique is detected, usually it does not matter if the rootkit is zero day, or a two-year old sample. The use of zero day malware is more important when it comes to user-mode malware.

We started the rootkit dropper with administrator level privileges, and allowed the UAC prompt. This was a realistic scenario because most home users and small-business users have administrator level privileges on their computer, and either the user can be socially engineered to allow the execution with elevated privileges, or the

UAC is already turned off, or the dropper can have UAC bypass exploits. As we used a fully patched Windows, the bypass might have failed.

Figure 2 - ZeroAccess bypass UAC method using Flash Player

If the malware was able to install, we waited 6 minutes for the rootkit to reboot. If this did not happen, we rebooted the machine manually. After the reboot, we used forensic techniques to detect the presence of the malware, including:

- Byte comparing the MBR and VBR with a clean copy
- Check for usermode and kernel mode hooks
- Registry entries prevalent to the rootkit (with raw access)
- Files on the filesystem (with direct disk access, bypassing rootkit hiding functions)

After we confirmed that the rootkit was working as expected, we installed the rootkit detector/second opinion malware scanner/rescue kit, updated it to the latest version (both program and signatures), and started the default quick/smart scan. Cloud connectivity was allowed. Whenever the software detected the presence of the rootkit, we executed the default action (quarantine or delete). If the software demanded a computer reboot, we rebooted the computer.

The small number of test cases (8 rootkits) is because rootkit remediation tests cannot be done automatically, and all remediation has to be followed by a forensics analysis, which is time consuming.

2.2 Scoring

As there are different levels of remediation, we came up with the following scoring system. Each software was able to collect points on every test, and the security software received:

- 0 points whenever the infection was not detected. Dropper detection does not count in our methodology.
- 1 point if the infection was detected, but the software was unable to remove the infection.
- 3 points when the software was able to remove the infection so that the rootkit was not functional at all, but some artifacts remained on the infected system, which lowered the overall security level of the system. These artifacts were: main malware executable (directly on the filesystem, or in registry), autorun registry entries, executable files, host file modifications, etc. The following artifacts were not considered harmful: encrypted configuration files, empty directories, any files left in the temp folder, and encrypted Virtual File Systems.

- 4 points when the rootkit was detected, fully removed, and all risky artifacts removed.

It is important to note that after a rootkit is installed, malware operators can change the security level of the system individually (e.g. specific to a computer). These custom modifications cannot be detected by any security software, thus we recommend that all computers be checked manually after any malware infection. For example, malware operators can install new trusted root certificate authorities, disable Windows security options (e.g. Firewall, Malware scanner, UAC), etc.

2.3 Rootkits tested and results

We tested the following rootkits against the rootkit remediation, second-opinion malware scanners and anti-malware system rescue tools.

2.3.1 TDL4/TDSS/Alureon

This rootkit is an MBR infector bootkit; it uses its own Virtual File System to store the configuration files, binaries, etc. For more detailed information about this version, see http://contagiodump.blogspot.gr/2011/02/tdss-tdl-4-alureon-32-bit-and-64-bit.html?m=1

Test results

	Emsisoft Free Emergency Kit	HitmanPro 3	MalwareBytes Anti Malware	TDSS killer	Zemana AntiMalware
Score	**1**	**4**	**0**	**4**	**4**

2.3.2 ZeroAccess/Max++

This rootkit installs its own kernel mode disk driver rootkit to prevent detection of the rootkit binaries, and uses IRP hooking to fool detection attempts.

Test results

	Emsisoft Free Emergency Kit	HitmanPro 3	MalwareBytes Anti Malware	TDSS killer	Zemana AntiMalware
Score	**0**	**4**	**3**	**4**	**3**

2.3.3 Gapz!C

This rootkit is an MBR infector bootkit; it uses its own Virtual File System to store the configuration files, binaries, etc. For code injection, it uses the popular PowerLoader kit. For more information, see http://www.welivesecurity.com/wp-content/uploads/2013/05/gapz-bootkit-whitepaper.pdf

Test results

	Emsisoft Free Emergency Kit	HitmanPro 3	MalwareBytes Anti Malware	TDSS killer	Zemana AntiMalware
Score	**0**	**1**	**0**	**4**	**4**

2.3.4 Rovnix/Cidox

This rootkit is a VBR infector bootkit (it modifies the NTFS bootstrap code), loads its own kernel driver via debug registers, etc. For more information, see:

http://www.welivesecurity.com/2011/08/23/hasta-la-vista-bootkit-exploiting-the-vbr/

Test results

	Emsisoft Free Emergency Kit	HitmanPro 3	MalwareBytes Anti Malware	TDSS killer	Zemana AntiMalware
Score	**0**	**0**	**0**	**0**	**1**

2.3.5 Poweliks/XSwkit/Gootkit

This rootkit is fileless malware. The important code resides in the registry, and persistence is achieved via default software found on Windows installations (rundll, mshta, ActiveX). Based on these features, it can bypass application whitelist protection. For more information, see:

http://www.kernelmode.info/forum/viewtopic.php?f=16&t=3669

Test results

	Emsisoft Free Emergency Kit	HitmanPro 3	MalwareBytes Anti Malware	TDSS killer	Zemana AntiMalware
Score	**0**	**0**	**0**	**0**	**3**

2.3.6 WMIGhost/Syndicasec

This rootkit operates as a WMI script, thus traditional AV software is bypassed. Persistence is achieved via WMI filters, a lesser known but effective technique. For more information, see:

http://www.welivesecurity.com/2013/05/23/syndicasec-in-the-sin-bin/

Test results

	Emsisoft Free Emergency Kit	HitmanPro 3	MalwareBytes Anti Malware	TDSS killer	Zemana AntiMalware
Score	**0**	**0**	**0**	**0**	**4**

2.3.7 Phasebot

This rootkit is similar to the Poweliks rootkit as it employs the same fileless method, but it uses Powershell. We included this rootkit because we believe this fileless malware technique will become more prevalent. For more information, see:

http://www.malwaretech.com/2014/12/phase-bot-fileless-rootkit.html

Test results

	Emsisoft Free Emergency Kit	HitmanPro 3	MalwareBytes Anti Malware	TDSS killer	Zemana AntiMalware
Score	**0**	**4**	**4**	**0**	**1**

2.3.8 Carberp

Carberp is still a prevalent malware, especially because its source code was leaked online in 2013. The tested version used user mode rootkit capabilities to hide the malware binary in the startup folder. For more information, see:

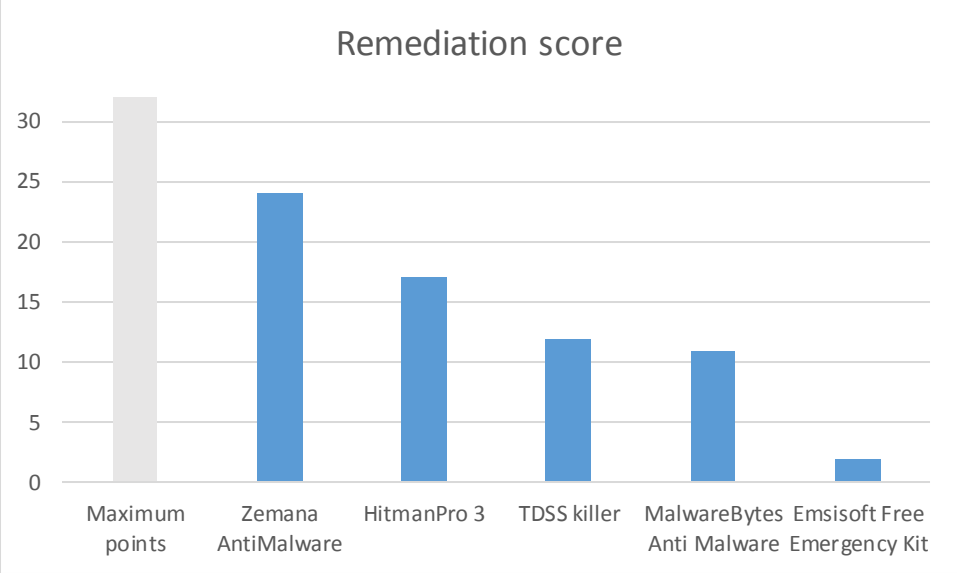
http://pxnow.prevx.com/content/blog/carberp-a_modular_information_stealing_trojan.pdf

Test results

	Emsisoft Free Emergency Kit	HitmanPro 3	MalwareBytes Anti Malware	TDSS killer	Zemana AntiMalware
Score	1	4	4	0	4

3 Final results

	Emsisoft Free Emergency Kit	HitmanPro 3	MalwareBytes Anti Malware	TDSS killer	Zemana AntiMalware	Maximum points (theoretical)
Score	2	17	11	12	24	32



Based on this report, Zemana AntiMalware proved to be the best rootkit remediator among the tested products during the test.

4 Appendix

4.1 Revision history

V 1.0	2015 august 14	Original version
V 1.1	2015 september 7	Added footnote about TDSS killer
V 1.2	2015 september 21	Footnote moved to main document, more information added