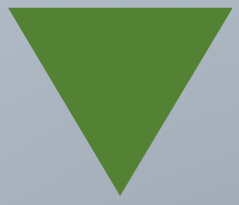
August 2014

PC SECURITY LABS

COMPARATIVE TEST

Remote code execution exploit mitigations for popular applications

Microsoft Office



Flash **Silverlight** **QuickTime**

- Internet Explorer Java Adobe

PCSL
IT CONSULTING INSTITUTE

Content

1. BACKGROUND

Exploit Kits and targeted attacks on home users and companies nowadays focus on exploiting popular applications such as browsers, browser add-ons such as Flash and Silverlight, Java, Acrobat Reader, Microsoft Office Word, Excel, PowerPoint, media players, etc. The objective is to remotely execute code, transparently to the user and without relying on user interaction, in order to infect the machine with undetected malware. This comparative study looks at the effectiveness of different proactive exploit mitigation technologies included in popular security vendors and specialized anti-exploit tools.

There are several methods to block malware infection via utilizing vulnerability exploits, one is to get the freshest patches and the other way is to install security products that include some form of exploit mitigation technologies. In order to test the exploit blocking capabilities, we used a Windows XP SP3 installation with IE8 and popular applications that are vulnerable to a number of exploits. Even though the test was performed under Windows XP SP3 it is worth noting that these tested applications may still be vulnerable to exploitation under more modern Operating Systems such as Windows 7 and Windows 8. In fact most of the exploits tested correspond to recent vulnerabilities from the last two (2) years.

This test is for reviewing exploit blocking capabilities only, and the result does not stand for the overall protection level for tested products.

This test was commissioned by Malwarebytes Corp. to test the exploit blocking capabilities of different products against relevant vulnerabilities (i.e. vulnerable applications which are targeted typically by Exploit Kits and targeted attacks). PCSL made the sole research and methodology decision of which CVEs to test and how to test. No exploit code samples were provided by Malwarebytes.

2. METHODOLOGY

- Most of the exploits are setup on Metasploit and some come from private sources.
- Exploits chosen are relevant in both prevalence as found in Exploit Kits in-the-wild and recent (less than two years old).
- Each exploit will be tested with different payload configurations. Payloads range from execute, download and execute, reverse shells, and other options found in Metasploit.
- We will shut down the on access file detection if the product detects the poc by signature so that the exploit can be launched to test the exploit detection capabilities. As exploits and payloads can be easily modified to bypass signature detection[1] this is a valid methodology to test for exploit blocking capabilities.
- If there is a detection by the product and no payload is executed then this will be counted as successful block. If the security product use some methods to shut down the backdoor connection after the payload is executed, we also count it as a successful block.
- All the tests are executed on Windows XP SP3 Operating System in English, without any other additional patches.
- All the tested security products are download from their official websites.

[1] http://community.rapid7.com/community/metasploit/blog/2014/01/05/a-cat-and-mouse-game-between-exploits-and-antivirus

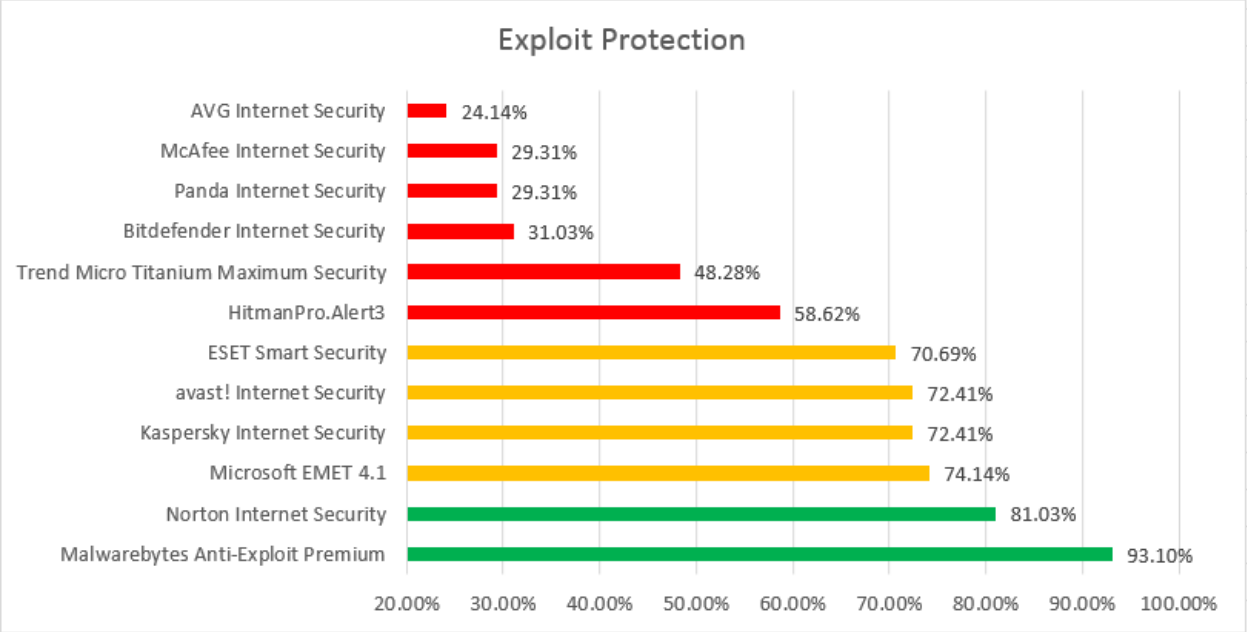
3. PRODUCT INFORMATION

Software	Vendor	Version
avast! Internet Security	AVAST	2014.9.0.2021
AVG Internet Security	AVG	14.0.0.4744
Bitdefender Internet Security	Bitdefender	17.28.0.1191
Enhanced Mitigation Experience Toolkit[2]	Microsoft	4.1.5228.513
ESET Smart Security	ESET	7.0.317.4
HitmanPro.Alert3	SurfRight	3.0.12.73
Kaspersky Internet Security	Kaspersky Lab	14.0.0.4651(g)
Malwarebytes Anti-Exploit Premium	Malwarebytes	1.04.1.1006
McAfee Internet Security	McAfee	12.8.958
Norton Internet Security	Symantec	21.4.0.13
Panda Internet Security	Panda	19.01.01
Trend Micro Titanium Maximum Security	Trend Micro	7.0.1255

[2] EMET 4.1 was used as EMET 5.0 does not support Windows XP.

4. RESULT

We consider products which are only able to block less than 60% of the tested exploits as failed in terms of exploit blocking claims. Products which are able to block between 61% and 80% are considered as insufficient. Finally products which are able to block over 80% of the tests exploits are considered pass.



The following table details the results per product and per exploit and payload option.

Exploits	*Payload*	*Malwarebytes*	*Symantec*	*Bitdefender*	*Kaspersky*	*Panda*	*ESET*
CVE-2012-0663	payload-a	pass	failed	failed	failed	failed	failed
	payload-b	pass	failed	failed	pass	failed	failed
	payload-c	pass	pass	failed	failed	failed	pass
CVE-2013-1017	payload-a	pass	pass	pass	pass	failed	failed
	payload-b	pass	pass	pass	pass	failed	failed
	payload-c	pass	pass	pass	pass	pass	failed
CVE-2012-0158	payload-a	pass	failed	failed	failed	failed	failed
	payload-b	pass	failed	failed	pass	failed	failed
	payload-c	pass	pass	failed	failed	failed	pass
CVE-2012-1856	payload-a	pass	failed	pass	failed	failed	failed
CVE-2013-3897	payload-a	pass	failed	failed	failed	failed	failed
	payload-b	pass	failed	failed	pass	failed	failed
	payload-c	pass	pass	pass	pass	pass	pass
CVE-2013-3163	payload-a	pass	pass	failed	failed	failed	failed
	payload-b	pass	pass	failed	failed	pass	pass
CVE-2013-1347	payload-a	pass	pass	failed	failed	failed	failed
	payload-b	pass	pass	pass	pass	failed	pass
	payload-c	pass	pass	pass	failed	pass	pass
CVE-2012-4969	payload-a	pass	failed	failed	failed	failed	failed
	payload-b	pass	pass	pass	pass	failed	pass
	payload-c	pass	pass	pass	pass	pass	pass
CVE-2012-4792	payload-a	pass	failed	pass	failed	failed	failed
	payload-b	pass	pass	failed	failed	failed	failed
	payload-c	pass	pass	failed	pass	pass	pass
CVE-2013-3346	payload-a	pass	failed	pass	pass	failed	failed
	payload-b	pass	failed	failed	pass	failed	failed
	payload-c	pass	pass	failed	pass	pass	pass

Exploits	*Payload*	*Malwarebytes*	*Symantec*	*Bitdefender*	*Kaspersky*	*Panda*	*ESET*
CVE-2011-2110	payload-a	pass	pass	failed	pass	failed	pass
	payload-b	pass	pass	failed	pass	failed	pass
	payload-c	pass	pass	failed	pass	pass	pass
CVE-2012-1535	payload-a	pass	pass	pass	pass	pass	pass
	payload-b	pass	pass	pass	pass	failed	pass
	payload-c	pass	pass	pass	pass	failed	pass
CVE-2013-0634	payload-a	pass	pass	failed	pass	failed	pass
	payload-b	pass	pass	failed	pass	failed	pass
	payload-c	pass	pass	failed	pass	pass	pass
CVE-2014-0497	payload-a	pass	pass	pass	pass	failed	pass
	payload-b	pass	pass	pass	failed	pass	pass
CVE-2014-0515	payload-a	pass	pass	pass	pass	failed	pass
	payload-b	pass	pass	pass	failed	failed	pass
CVE-2012-0507	payload-a	pass	pass	failed	pass	failed	pass
	payload-b	pass	pass	failed	pass	failed	pass
	payload-c	pass	pass	failed	pass	pass	pass
CVE-2013-1488	payload-a	failed	pass	failed	pass	failed	pass
	payload-b	failed	pass	failed	pass	failed	pass
	payload-c	pass	pass	failed	pass	pass	pass
CVE-2013-2423	payload-a	failed	pass	failed	pass	failed	pass
	payload-b	failed	pass	failed	pass	failed	pass
	payload-c	pass	pass	failed	pass	pass	pass
CVE-2013-2460	payload-a	pass	pass	failed	pass	failed	pass
	payload-b	pass	pass	failed	pass	failed	pass
	payload-c	pass	pass	failed	pass	pass	pass
CVE-2013-2465	payload-a	pass	pass	failed	pass	failed	pass
	payload-b	pass	pass	failed	pass	failed	pass
	payload-c	pass	pass	failed	pass	pass	pass
CVE-2013-0074	payload-a	pass	pass	failed	failed	failed	pass
	payload-b	pass	pass	failed	pass	failed	pass
	payload-c	pass	pass	failed	pass	pass	pass

Exploits	*Payload*	*AVG*	*AVAST*	*Trend Micro*	*McAfee*	*Hitmanpro.Alert3*	*EMET*
CVE-2012-0663	payload-a	failed	failed	failed	failed	failed	pass
	payload-b	failed	failed	failed	failed	failed	pass
	payload-c	failed	failed	failed	failed	failed	pass
CVE-2013-1017	payload-a	failed	failed	failed	failed	pass	pass
	payload-b	failed	failed	failed	failed	pass	pass
	payload-c	failed	failed	failed	pass	pass	pass
CVE-2012-0158	payload-a	failed	failed	failed	failed	pass	pass
	payload-b	failed	failed	failed	failed	pass	pass
	payload-c	failed	failed	failed	failed	pass	pass
CVE-2012-1856	payload-a	failed	failed	failed	failed	pass	pass
CVE-2013-3897	payload-a	failed	pass	failed	failed	pass	pass
	payload-b	failed	failed	failed	failed	pass	pass
	payload-c	failed	pass	failed	pass	pass	pass
CVE-2013-3163	payload-a	failed	pass	failed	failed	failed	pass
	payload-b	failed	pass	failed	pass	pass	pass
CVE-2013-1347	payload-a	failed	failed	pass	failed	failed	pass
	payload-b	pass	pass	pass	failed	pass	pass
	payload-c	pass	pass	pass	pass	pass	pass
CVE-2012-4969	payload-a	failed	pass	failed	failed	pass	pass
	payload-b	pass	pass	pass	failed	pass	pass
	payload-c	pass	pass	failed	pass	pass	pass
CVE-2012-4792	payload-a	pass	pass	pass	failed	pass	pass
	payload-b	failed	failed	pass	failed	failed	pass
	payload-c	failed	pass	pass	pass	pass	pass
CVE-2013-3346	payload-a	failed	pass	failed	failed	pass	pass
	payload-b	failed	pass	failed	failed	pass	pass
	payload-c	failed	pass	failed	pass	pass	pass

Exploits	*Payload*	*AVG*	*AVAST*	*Trend Micro*	*McAfee*	*Hitmanpro.Alert3*	*EMET*
CVE-2011-2110	payload-a	pass	pass	failed	failed	pass	pass
	payload-b	pass	pass	failed	failed	pass	pass
	payload-c	pass	pass	failed	pass	pass	pass
CVE-2012-1535	payload-a	failed	pass	pass	not support	pass	pass
	payload-b	failed	pass	pass	not support	pass	pass
	payload-c	failed	pass	pass	not support	pass	pass
CVE-2013-0634	payload-a	failed	failed	pass	failed	failed	pass
	payload-b	failed	failed	pass	failed	pass	pass
	payload-c	failed	failed	pass	pass	pass	pass
CVE-2014-0497	payload-a	failed	pass	failed	failed	pass	pass
	payload-b	failed	pass	failed	pass	pass	pass
CVE-2014-0515	payload-a	failed	pass	pass	failed	pass	pass
	payload-b	failed	pass	pass	pass	pass	pass
CVE-2012-0507	payload-a	failed	pass	pass	failed	failed	failed
	payload-b	failed	pass	pass	failed	failed	failed
	payload-c	pass	pass	pass	pass	failed	failed
CVE-2013-1488	payload-a	failed	pass	failed	failed	failed	failed
	payload-b	failed	pass	failed	failed	failed	failed
	payload-c	pass	pass	pass	pass	failed	failed
CVE-2013-2423	payload-a	failed	pass	pass	failed	failed	failed
	payload-b	failed	pass	pass	failed	failed	failed
	payload-c	pass	pass	pass	pass	failed	failed
CVE-2013-2460	payload-a	failed	pass	pass	failed	failed	failed
	payload-b	failed	pass	pass	failed	failed	failed
	payload-c	pass	pass	pass	pass	failed	failed
CVE-2013-2465	payload-a	failed	pass	pass	failed	failed	failed
	payload-b	failed	pass	pass	failed	failed	failed
	payload-c	pass	pass	pass	pass	failed	failed
CVE-2013-0074	payload-a	failed	pass	failed	failed	failed	pass
	payload-b	failed	pass	failed	failed	pass	pass
	payload-c	pass	pass	failed	pass	failed	pass

5. SUMMARY

Vendor	*Malwarebytes*	*Symantec*	*EMET*	*AVAST*	*Kaspersky*	*ESET*	*Hitman pro.Alert3*	*Trend Micro*	*Bitdefender*	*Panda*	*McAfee*	*AVG*
Pass	54	47	43	42	42	41	34	28	18	17	17	14
Failed	4	11	15	16	16	17	24	30	40	41	38	44
Not Supported	0	0	0	0	0	0	0	0	0	0	3	0
Score	93.103	81.034	74.138	72.414	72.414	70.690	58.621	48.276	31.034	29.310	29.310	24.138

6. TESTER INTRODUCTION

JIAXING CHENXIANG INFORMATION TECHNOLOGY CO., LTD., is an IT product test and consulting company located in Jiaxing, Zhejiang Province, China. As a professional tester of desktop security products and also mobility security solutions, we are willing to provide references to the endpoint users for choosing security solutions. Not only we test security solutions for different environment and customers, but also we provide test and consulting reports of other IT products, e.g. battery, mobility devices, computer power, etc.

7. RIGHTS STATEMENT

Unless otherwise stated, Jiaxing Chenxiang Information Technology Co., Ltd. (hereinafter referred to as "Chenxiang Information Technology") owns the copyright of this report. Without prior written consent of Chenxiang Information Technology , no other unit or individual shall have the right to alter the contents of this report and use this report for commercial purposes by any means (including but not limited to transmission, dissemination, reproduction, excerpt, etc.).

Unless otherwise stated, Chenxiang Information Technology shall be the rightful owner of the trademarks, service marks of Chenxiang Information Technology used in the report. Any action of infringing upon the legal rights of Chenxiang Information Technology is prohibited, Chenxiang Information Technology shall have the right to pursue the legal liability of the infringer in accordance with the law.

8. DISCLAIMER

Notice that before using the report issued by Jiaxing Chenxiang Information Technology Co. Ltd (hereinafter referred to as"Chenxiang Information Technology") , please carefully read and fully understand the terms and conditions of this disclaimer (hereinafter referred to as"Disclaimer "), including the clauses of exclusion or restriction of the liabilities of Chenxiang Information Technology and the limitation the rights of users. If you have any objection to the terms and conditions of this Disclaimer, you have the right not to use this report, the act of using this report will be regarded as an acceptance and the recognition of the terms and conditions of this Disclaimer, so by using this report, you agree to the following terms and conditions:

1、The report is provided by Chenxiang Information Technology, all the contents contained herein are for reference purpose only, but will not be regarded as the suggestion, invitation or warranty for readers to choose, purchase or use the products mentioned herein. Chenxiang Information Technology will not guarantee the absolute accuracy and completeness of the contents of the report, you should not rely solely on this report or substitute the viewpoints of the report for your independent judgment. If you have any queries, please consult the relevant departments of the State and then choose, purchase or use products by your independent judgment.

2、The contents contained herein is the judgment made by Chenxiang Information Technology to the product characteristics as of the date of the report published, in the future Chenxiang Information Technology will have the right to issue the new reports which contain different contents or draw different conclusions, but Chenxiang Information Technology has no obligation or responsibility to update the original report or inform readers of the update of it, in this case, Chenxiang Information Technology will bear no responsibility for readers' loss of using the original report .

3、The report may contain links to other websites, which are provided solely for readers' convenience to use, the contents of the linked websites are not any part of this report. Readers shall assume the risks and losses or bear the costs when visiting such websites, Chenxiang Information Technology will not guarantee the authenticity, completeness , accuracy and legitimacy of the contents of such websites (including but not limited to advertising, products or other information). Chenxiang Information

Technology does not accept any liability (direct or indirect) for readers' damages or losses arising from their clicking on or viewing such websites to obtain some information, products or service.

4、Chenxiang Information Technology may have or will have a business relationship with the companies which produce the products mentioned in this report, but has no obligation to notify readers about it, no matter there has already been or there will be such business relationship in the future.

5、The act of readers'receiving this report are not regarded as the establishment of the business relationship between readers and Chenxiang Information Technology, so there is no customer relationship existing, Chenxiang Information Technology does not accept any legal liability as the readers' customer .

6、The products which are used to be tested as the samples by Chenxiang Information Technology are bought through official way and legal means, so the report is proper for products bought through official way and legal means, not for products bought through unofficial way and illegal means. Therefore it's the users buying such products who will be responsible for any risk or loss arising therefrom. Chenxiang Information Technology will not have or accept any liability whatsoever for any such risk or loss.

7、Some trademarks, photos or patterns owned by units or individuals will probably be used in this report, if you think your legal right and interests are infringed, please contact Chenxiang Information Technology promptly, Chenxiang Information Technology will handle the matter as quickly as possible.

Chenxiang Information Technology reserves the rights to interpret, modify and update the Disclaimer.