Exploit Protection on Windows XP

A test commissioned by Qihoo 360 and performed by AV-TEST GmbH
Date of the report: April 30th, 2014

Content

Executive Summary

AV-TEST examined 10 anti-virus software solutions in regards to their protection capabilities against exploits targeting vulnerabilities on Windows XP.

Since the support for Windows XP ended in April 2014 and Microsoft will not provide any further updates to the OS, not even for critical security vulnerabilities, it is expected that a lot of attacks to Windows XP will follow. There are different estimations on how many PCs are still running XP but they agree that it is roughly 25% of all Windows PCs worldwide.

All of these PCs are now an easy target as soon as a new vulnerability is detected and can be exploited by malware to infect the system. There are only two solutions:

1. Upgrade to another operating system
2. Protect your system with anti-virus software

Option 1 is often not possible due to hardware constraints and similar problems. So for most users the only option is to rely on a good working anti-virus software.

Since the main problem for Windows XP will be new, currently unknown, exploits it is important that the security solutions provide generic features to block those kinds of attacks. In order to test the exploit blocking capabilities, AV-TEST used a Windows XP installation that was vulnerable to a number of exploits and checked whether the products were able to detect and block these attacks.

Qihoo 360 and Norton were the only products to successfully block all 54 attacks. These products will likely provide a good protection even for yet unknown attacks. Bitdefender, Kaspersky and Kingsoft also showed a good result, only missing out on certain vulnerabilities or certain circumstances. The average blocking rate was only 74%, which shows that users have to be careful when making their choice for an anti-virus software to protect their Windows XP environment.

Detailed Test Report

Test Environment and Products

The test has been carried out on Windows XP, SP3 (32-bit) English (v5.1.2600 SP 3 Build 2600) and Internet Explorer 8.0.6001.18702IC. Furthermore Microsoft Office Excel 2003 (11.5612.5606) and Word 2003 (11.5604.5606) were installed to process documents exploiting vulnerabilities in this software.

The products and the versions are listed in the table below. All products have been installed and tested in default settings. No options have been modified.

Product Name	Product Version
Avast Internet Security 2014	2014.9.0.2018
AVG Internet Security 2014	2014.0.4577
Avira Internet Security Suite 2014	14.03.350
Bitdefender Internet Security 2014	17.27.0.1146
Eset Smart Security 7	7.0.302.26
Kaspersky Internet Security 2014	14.0.0.4651(f)
Kingsoft Antivirus 2013	2013.SP7.5.042815
Norton Internet Security 2014	21.2.0.38
Qihoo 360 Internet Security 9 Beta	9.7.0.1001 Beta
Tencent PC Manager	8.5.24996.501

Table 1: Tested Products

The tested products were installed on plain Windows machines with the following configuration:

HetisG31 Office-PC
Intel Xeon Quad Core X3360 2,83GHz 12MB FSB1333
4 GB DDR2 667-RAM Kingston (2x 2048 MB)
500 GB SATA II WD Raid Edition III 3,5"

A disk image for each of the products has been created and was used throughout the test. The products had been updated on every day of the test to make sure latest products versions have been used. A final retest of all previously missed cases has been performed on April 28th and 29th with updated products.

Test Samples

In order to create exploits used for the test MetaSploit in v 4.8.2 (Update 1) has been used. These exploits have then been applied with MetaSploit as well.

In total 54 samples were created, targeting 7 different vulnerabilities, combined with different obfuscation and evasion options as well as different payloads to simulate a wide variety of possible malware attacks. The different options are shown in the tables below.

exploit/windows/browser/ie_execcommand_uaf (ms12_063)
exploit/windows/browser/ms10_022_ie_vbscript_winhlp32
exploit/windows/browser/ms10_042_helpctr_xss_cmd_exec
exploit/windows/browser/ms10_046_shortcut_icon_dllloader
exploit/windows/browser/ms12_037_ie_colspan
exploit/windows/fileformat/ms09_067_excel_featheader

exploit/windows/fileformat/ms12_027_mscomctl_bof

Table 2: Targeted Vulnerabilities

generic/shell_reverse_tcp
windows/download_exec
windows/exec
windows/messagebox
windows/shell/reverse_tcp
windows/vncinject/reverse_tcp

Table 3: Used Payloads

Manual modification
Javascriptobfuscator
Jscrambler
Jsutility
Marihnhaverbeke

Table 4: Applied Evasion and Obfuscation

The complete list of the different combinations is given in the appendix.

The exploits that are used in the testing only attack vulnerabilities in Microsoft software. No exploits have been used that attack third party software such as Adobe Reader or Java, as these applications are still supported by their vendors and will receive security updates.

Test Methodology

The creation of exploit samples with MetaSploit usually gives two different types of objects:

1. Actual files, such as documents that can be accessed directly, e.g. on the file system
2. HTTP content that is served from MetaSploit and reacts to client requests

In order to cover this a Windows PC running MetaSploit had been set up. The clients were able to access the web server provided by this PC in order to access the exploits that would then try to attack the vulnerable software components.

The individual steps to run the test were as follows:

1. The exploit has been set up on MetaSploit
2. The client has been reimaged with an up-to-date disk image of the product under test
3. The client then tried to access the web site containing the exploit, served by the MetaSploit system resp. tried to access the document containing an exploit that was created earlier
4. If there were any notifications from the anti-virus software they have been noted and documented (e.g. by creating screenshots or storing report files)
5. Furthermore it was checked whether the exploit was able to execute the payload
6. If there was a detection by the product and no payload was executed then this was counted as successful block
7. If there was no detection and the payload was executed then this was counted as miss (even when some components would have been detected a few minutes later)
8. In case there was no detection and no execution of the payload either, this indicated an error and the test has been repeated or the test case had to be removed from the results

Test Results

Qihoo 360 and Norton achieved the best results in detecting/blocking the 54 attacks. Closely following are Kaspersky and Kingsoft which only failed on a few samples. The overall test results are given in the following table.

Product Name	Blocked Attacks (out of 54)	In %
Avast Internet Security 2014	33	61,11%
AVG Internet Security 2014	37	68,52%
Avira Internet Security Suite 2014	37	68,52%
Bitdefender Internet Security 2014	42	77,78%
Eset Smart Security 7	31	57,41%
Kaspersky Internet Security 2014	51	94,44%
Kingsoft Antivirus 2013	48	88,89%
Norton Internet Security 2014	54	100%
Qihoo 360 Internet Security 9 Beta	54	100%
Tencent PC Manager	10	18,52%

Table 5: Overall Test Results

The average blocking rate was 74%, so 5 products were better than the average and 5 were worse. The worst result was 10 from 54 samples, meaning that only around 18% of the attacks were blocked.

When looking at the data a bit differently, an interesting observation can be made. The following table shows the results of 33 exploits were no obfuscation or evasion has been applied.

Product Name	Blocked Attacks (out of 33)	In %
Avast Internet Security 2014	27	81,82%
AVG Internet Security 2014	24	72,73%
Avira Internet Security Suite 2014	27	81,82%
Bitdefender Internet Security 2014	27	81,82%
Eset Smart Security 7	24	72,73%
Kaspersky Internet Security 2014	32	96,97%
Kingsoft Antivirus 2013	27	81,82%
Norton Internet Security 2014	33	100%
Qihoo 360 Internet Security 9 Beta	33	100%
Tencent PC Manager	8	24,24%

Table 6: Test Results of Samples without Obfuscation

For all products besides Kingsoft the blocking rates for these samples are much better than the results for all samples. The average blocking rate of all products is also higher than before, with 78,79%.

The results indicate that several products may have static detection for certain exploits or certain MetaSploit components (such as the payloads) only and are vulnerable to even basic obfuscation and evasion techniques. This assumption can be verified when looking at the results of the 21 samples that used obfuscation or evasion techniques.

Product Name	Blocked Attacks (out of 21)	In %
Avast Internet Security 2014	6	28,75%
AVG Internet Security 2014	13	61,90%

Avira Internet Security Suite 2014	10	47,62%
Bitdefender Internet Security 2014	15	71,43%
Eset Smart Security 7	7	33,33%
Kaspersky Internet Security 2014	19	90,48%
Kingsoft Antivirus 2013	21	100%
Norton Internet Security 2014	21	100%
Qihoo 360 Internet Security 9 Beta	21	100%
Tencent PC Manager	2	9,52%

Table 7: Test Results of Samples with Obfuscation

By looking at these numbers it is possible to determine products that have generic techniques to detect and protect from exploits. Products that detect less samples than before are likely to have static signatures or weak heuristics that can be easily fooled by real attackers. Kingsoft, Norton and Qihoo 360 are not fooled by evasion or obfuscation in this test. Also Kaspersky only misses out on two samples here. Interestingly, the missed cases of Kaspersky all use the messagebox payload, which of course wouldn't be used in a real attack. All samples using more intrusive payloads (such as reverse shell or execution of a binary) are detected reliably by the product.

The following tables show which products were able to handle which exploit. 'All' is given when all samples have been detected, 'Some' is given when at least one sample is not detected and 'None' is given when no sample was detected.

	MS12-063	MS10-022	MS10-042	MS10-046	MS12-037	MS09-067	MS12-027
Avast	Some	All	All	All	None	All	All
AVG	Some	All	All	All	None	None	All
Avira	Some	All	All	All	None	All	All
Bitdefender	All	All	All	All	None	All	All
ESET	Some	Some	All	All	Some	None	All
Kaspersky	Some	All	All	All	All	Some	All
Kingsoft	All	Some	All	None	All	All	All
Norton	All	All	All	All	All	All	All
Qihoo 360	All	All	All	All	All	All	All
Tencent	Some	Some	Some	None	None	Some	Some

Table 8: Vulnerability Coverage per Product

As can be seen, most products have a solid detection of most exploits. Norton and Qihoo 360 cover all vulnerabilities completely. Bitdefender doesn't cover one vulnerability, Avast, Avira Kaspersky and Kingsoft have misses in case of two vulnerabilities. AVG, ESET and Tencent have misses in at least three cases.

One note has to be made regarding the products that perform well: Not every detection is generic. They also provide static detection (signatures) to detect certain exploits or even MetaSploit modules. So a good result in this test is not a guarantee that they will generically detect all attacks in real life. But the probability that they will detect more new attacks is high.

Conclusion

With the end of support for Windows XP as of April 8th 2014 this still widely deployed system is at risk, more than ever before. The problem is not commodity malware but the problem will be exploits for yet undetected vulnerabilities that will not be patched by Microsoft anymore. Therefore it will be one of the main tasks for anti-virus software to deliver reliably exploit detection when trying to protect Windows XP:

There are basically two possibilities to detect attacks by exploits:

1. Statically by signatures, that will detect certain versions of a specific exploit
2. Generically, to detect the techniques used by exploits instead of detecting the exploit itself

Products that have a good coverage in exploit protection will use both techniques, as neither is enough to prevent all attacks. Older and known exploits can be covered with static signatures, but vendors have to be careful to also cover obfuscated variants. New, unknown or heavily obfuscated exploits will be detected with generic approaches that look for typical behavior of exploits.

As the results of the above testing have shown, Qihoo 360, Kaspersky and Norton provide a very good protection rate against exploits that target Windows components. All of these products use a combined approach in detecting attacks, as described above.