Exploit Protection on Windows XP

A test commissioned by Tencent and performed by AV-TEST GmbH
Date of the report: November 21st, 2014

Content

Executive Summary

AV-TEST examined 6 anti-virus software solutions in regards to their protection capabilities against exploits targeting vulnerabilities on Windows XP, including both Microsoft components as well as third party software such as the Adobe Reader.

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.

In this test three products, namely Bitdefender, Kaspersky and Tencent were able to completely block all 40 attacks. In addition Qihoo also protected the user in nearly all cases. These products will likely provide a good protection even for yet unknown attacks. The other tested products, Avira and Kingsoft achieved worse results. However they were still able to block the majority of attacks and the average blocking rate was at 79.55%. This shows vendors have recognized the problem of these attacks and are implementing counter measures to protect users on Windows XP.

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 Adobe Reader (8.0.0 for Browser based exploits, 9.1.0 for file format exploits) was 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
Avira Antivirus Pro 2015	14.0.7.342
Bitdefender Internet Security 2015	18.17.0.1227
Kaspersky Internet Security 2015	15.0.1.415(a)
Kingsoft Antivirus 2013	2013.SP9.5.111012
Qihoo 360 Internet Security 9.7 Beta	9.7.0.1004 Beta
Tencent PC Manager	10.0.15127.901

Table 1: Tested Products

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

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 November 17th and 18th 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 40 samples were created, targeting 10 different vulnerabilities, combined with different payloads to simulate a wide variety of possible malware attacks. The different options are shown in the tables below.

exploit/windows/fileformat/adobe_flatedecode_predictor02 (CVE-2009-3459)
exploit/windows/browser/adobe_geticon (CVE-2009-0927)
exploit/windows/browser/adobe_utilprintf (CVE-2008-2992)
exploit/windows/browser/ie_cbutton_uaf (MS13-008)
exploit/windows/browser/ie_cgenericelement_uaf (MS13-038)
exploit/windows/browser/ms10_042_helpctr_xss_cmd_exec
exploit/windows/browser/ms10_046_shortcut_icon_dllloader
exploit/windows/browser/ms11_081_option
exploit/windows/browser/ms13_055_canchor
exploit/windows/browser/ms13_080_cdisplaypointer

Table 2: Targeted Vulnerabilities

generic/shell_reverse_tcp
windows/download_exec
windows/exec
windows/shell/reverse_tcp
windows/msgbox

Table 3: Used Payloads

The exploits that are used in the testing attack vulnerabilities in Microsoft software and third party software such as Adobe Reader.

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

Bitdefender, Kaspersky and Tencent were the only product to block all 40 attacks. Qihoo only missed two attacks. Avira protected in 75% of the cases where Kingsoft protected from 55% of the attacks.

The overall test results are given in the following table.

Product Name	Blocked Attacks (out of 40)	In %
Avira Internet Security Suite 2014	30	75,00%
Bitdefender Internet Security 2014	40	100,00%
Kaspersky Internet Security 2015	40	100,00%
Kingsoft Antivirus 2013	22	55,00%
Qihoo 360 Internet Security 9 Beta	38	95,00%
Tencent PC Manager	40	100,00%

Table 4: Overall Test Results

The average blocking rate was 87,5%, so 4 products were better than or equal to the average and 2 were worse. The worst result was 22 from 40 samples.

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.

	CVE-2009-3459	CVE-2009-0927	CVE-2008-2992	MS13-008	MS13-038	MS10-042	MS10-046	MS11-081	MS13-055	MS13-080
Avira	ALL	ALL	ALL	NONE	ALL	ALL	ALL	NONE	NONE	ALL
Bitdefender	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALL
Kaspersky	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALL
Kingsoft	ALL	ALL	SOME	NONE	ALL	SOME	NONE	ALL	NONE	NONE
Qihoo 360	NONE	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALL
Tencent	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALL

Table 6: Vulnerability Coverage per Product

	All blocked	Some blocked	None blocked
Avira	7	0	3
Bitdefender	10	0	0
Kaspersky	10	0	0
Kingsoft	4	2	4
Qihoo 360	9	0	1
Tencent	10	0	0

Table 7: Number of Blocked Exploit Families

As can be seen, most products have a solid detection of most exploits. Bitdefender, Kaspersky and Tencent were able block all attacks from all 10 families. Qihoo had full coverage for 9 exploits and only missed out on one. Avira covered 7 exploits. Kingsoft covered 4 fully and 2 partial and missed four completely.

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, Bitdefender, Kaspersky and Tencent 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. Qihoo only missed one exploit family and also provides a good protection. We strongly advise all vendors to cover exploits with generic detection techniques in order to protect their users.