Software Updates vs. Web Threats

How well does patching software protect against malware?

Dennis Technology Labs
www.DennisTechnologyLabs.com
Follow @DennisTechLabs on Twitter.com

This test explores how far software updates protect Windows 7 systems against vulnerabilities exploited by web-based threats.

It notes the consequences of failing to apply the very latest Windows updates; updates to Oracle JRE (Java); and updates to Adobe Flash Player and Reader.

The results show the level of benefit obtained when applying each set of these updates in isolation and in different combinations.

Executive Summary

- **Updating Windows improves system security by over 90 per cent**

93 per cent of the threats used in this test were rendered harmless by updating the Windows 7 systems fully. Updating third-party applications separately and in isolation increased security slightly, but not in addition to the security levels obtained through applying Windows Updates regularly.

- **Patching supplements, but should not replace, anti-malware protection**

Updating vulnerable software made a large improvement to the systems' security but additional protection was available when adding anti-malware software, either free or paid-for. Adding Microsoft Security Essentials increased the protection level to 99 per cent.

- **Windows users who update regularly achieve much the same security regardless of which anti-malware software they choose**

Systems running anti-malware products that scored very well in our previous tests, without the benefit of recent Windows updates, experienced minimal further advantage once these were applied. However, Windows updates added considerable extra protection when weaker anti-malware products were installed.

Simon Edwards, Dennis Technology Labs, 23rd July 2014

Document version 1.1a

INTRODUCTION

This test explores levels of protection provided against exploit-based web threats when applying updates to Windows 7 and third-party applications often targeted by attackers.

It also notes the consequences of failing to apply the very latest updates.

The following configurations of updates were tested.

UPDATE CONFIGURATIONS

Update configuration	Windows Updates	Oracle JRE (Java)	Adobe Flash Player, Reader
1	✓		
2	✓	✓	
3	✓	✓	✓
4	✓		✓
5		✓	
6		✓	✓
7			✓

In the above table Update configuration #1 includes Windows Updates but no other patching.

In contrast Update configuration #3 updates Windows and third-party software from Oracle and Adobe.

All other combinations were also tested.

The following versions of Windows and third-party software were used to verify the malware. These were used throughout the test unless the configuration (see above) demanded that they be updated.

SOFTWARE VERSIONS

Microsoft Windows	Oracle Java	Adobe Flash Player	Adobe Reader
Windows 7 SP1	Java SE 6 Update 18	Flash Player 10.1.85.3	Reader 9.2

When exposing the systems to web-based threats the default web browser was used. At the time of testing full Windows updates introduced Internet Explorer 11.

Updating benefits

Security experts and technology journalists advise readers regularly to update their software as part of a general plan to keep their personal computers secure.

Updates often plug security holes that may be abused by attackers in order to take some level of control over a victim's system.

Updating, or 'patching', software running on a PC is one way in which to provide protection against malware-based threats. Running anti-malware software also provides protection.

How effective are security updates?

Headlines in both the main-steam and technical press have announced that anti-virus is useless on a regular basis over the years[1] so Windows users may well ask themselves if simply updating PCs and avoiding websites hosting dubious content provides sufficient protection.

Or alternatively, could simply running anti-virus software cover all threats, rendering bandwidth-heavy application updates unnecessary?

All of the threats used in this test were capable of compromising a Windows 7 PC running Service Pack 1 but with no further updates applied to either Windows or third-party software.

This test was run at the same time as an anti-malware protection test, details of which are available in *How were the tests run?,* on page 4.

[1] 2014 - Symantec: Antivirus is 'DEAD' – no longer 'a moneymaker', The Register, http://www.theregister.co.uk/2014/05/06/symantec_antivirus_is_dead_and_not_a_moneymaker/

2012 - Imperva Reports Antivirus Solutions Woefully Inadequate, Reuters, http://www.reuters.com/article/2012/12/05/idUS43043+05-Dec-2012+HUG20121205

2010 - Antivirus is Dead. Long Live Antivirus, Gartner, http://blogs.gartner.com/neil_macdonald/2010/12/23/antivirus-is-dead-long-live-antivirus/

1. Protection Scores

The following results illustrate the overall level of protection achieved.

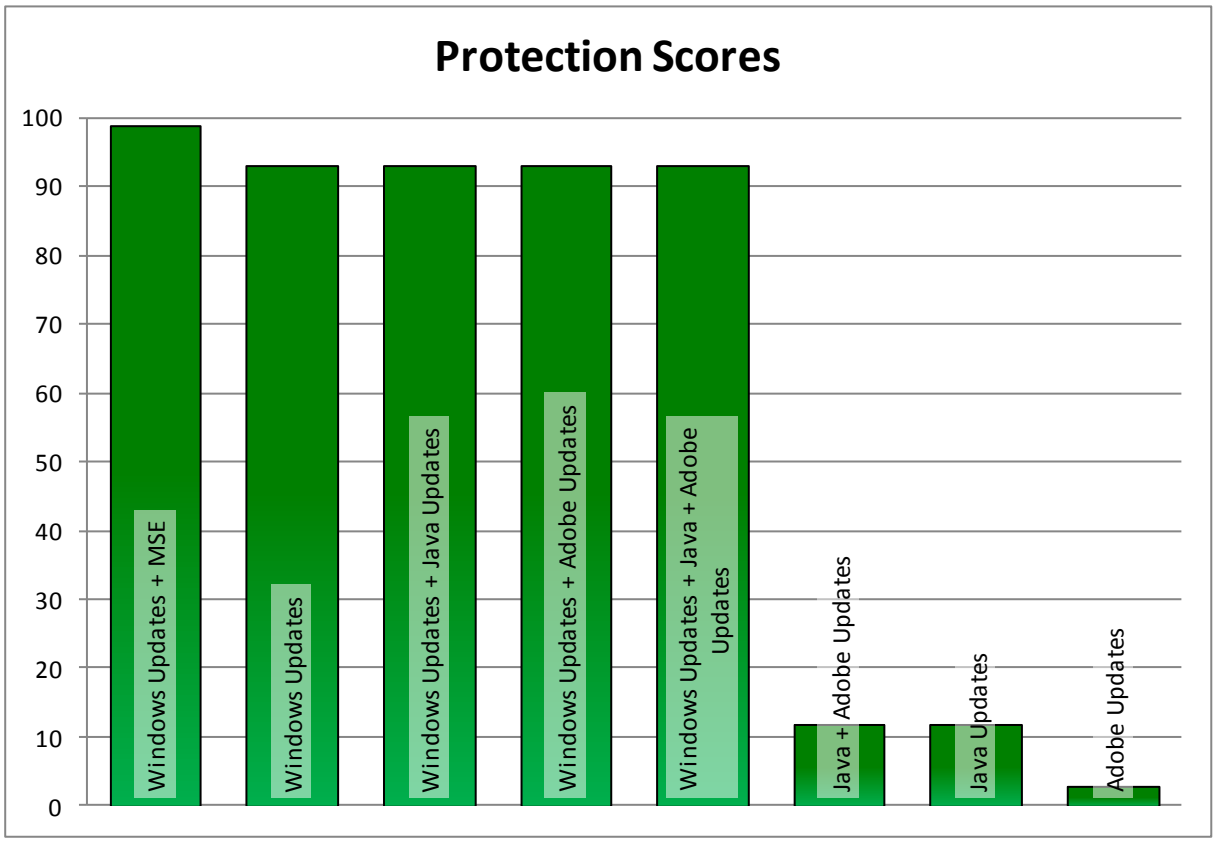
There are no penalties for failing to stop the threat, just a lack of a score point.

The best possible protection score is 100 and the worst is zero.

An unpatched Windows 7 PC would score zero in this test.

The most effective combination was Windows Updates with Microsoft Security Essentials (MSE), Microsoft's free anti-malware product.

PROTECTION SCORES



The protection scores simply indicate how many time each configuration prevented a threat from compromising the system.

PROTECTION SCORES

Product	Protected Scores
Windows Updates + MSE	99
Windows Updates	93
Windows Updates + Java Updates	93
Windows Updates + Adobe Updates	93
Windows Updates + Java + Adobe Updates	93
Java + Adobe Updates	12
Java Updates	12

2. THE TESTS

How were the tests run?

In this test each target system ran Windows 7 Home Premium SP1 running popular third-party applications.

Testers verified that the web-based threats used in the test were able to exploit the system and complete their attacks.

They then ran different combinations of Microsoft Windows, Oracle Java and Adobe Reader/Flash updates on clean systems before exposing those systems to the threats.

The threats may or may not rely on vulnerabilities present in Windows components or the third-party applications that were updated.

The test's methodology is nearly identical to that used in our enterprise, small business and consumer *anti-virus protection tests run over the same period of time*[2].

The above reports include full details of how the test was run, testing policies, tools used and a definition of terms.

What were the threats?

Anti-malware products classify malware using different systems and naming conventions. Some give very specific labels to threats, while others apply more general labels to the same threats.

For example, in this test Norton Internet Security labelled one attack, "Web Attack: Angler Exploit Kit Website" while Kaspersky Internet Security 2014 identified it simply as, "Malicious link blocked. Application: Windows Internet Explorer."

Listing the threats used in a meaningful way is challenging but, in this test, we wanted to explain in some detail the types of attacks that the products faced. Knowing this is helpful in drawing conclusions about the benefits of patching particular software programs.

If, for example, we discovered that attackers were focussed solely on Java-based attacks then we might expect non-Java-based Windows updates to have little positive effect. If, however, attackers focussed mainly on Internet Explorer then Windows updates should improve security by adding a strong baseline of protection to any anti-malware installed on the target system.

When consensus between products was strong we correlated the classifications. In three quarters of cases the threats encountered were as a result of exploit-based toolkits.

Below is the list of 75 threats found in our overall database of 100 attacks used.

Threats	Number of incidents
Angler Exploit Kit	21
Fake Flash Update	14
MSIE CVE-2013-2551	12
Red Exploit Kit	11
Nuclear Exploit Kit	7
Exploit Toolkit	4
Sweet Orange Exploit Kit	1
Blackhole Toolkit	1
Internet Explorer CVE-2014-0322	1
Executable Image	1
CritXPack Exploit Kit	1
Magnitude Exploit Kit	1

There are different versions of these exploit kits in use. We have grouped those above into general 'families'.

The most prevalent threat in this test, the Angler Exploit Kit, targets Oracle Java, Adobe Flash and Microsoft Silverlight vulnerabilities.

The Fake Flash Update threat is a social engineering attack that does not rely on vulnerabilities in Adobe Flash.

MSIE CVE-2013-2551 refers to an attack that targets Internet Explorer directly, affecting versions 6 to 10.

There is a single incidence of Internet Explorer CVE-2014-0322, which affects only Internet Explorer versions 9 and 10.

[2] Anti-Virus Protection reports, April - June 2014, Dennis Technology Labs http://dennistechnologylabs.com/reports/s/a-m/2014/

3. Conclusions

- **Windows Updates installs a safer browser**

There is no doubt that applying security updates prevents attackers from abusing the vulnerabilities that those updates address.

This report shows that 93 per cent of the threats used in this test were countered by updating the system fully using Microsoft's Windows Updates. The reason for this is that Windows Updates introduces Internet Explorer 11.

As a result of Internet Explorer 11's presence very few exploits ran. This was partially due to the browser effectively blocking threats, so very few malicious executable files ran.

In many cases the browser recognised that the threats it was instructed to download were "not commonly downloaded", "unsafe" or "the publisher… could not be verified."

Internet Explorer 11's SmartScreen Filter, which prevented 11 per cent of the attacks, is designed to "detect phishing websites [and] help protect you from downloading or installing malware."[3]

Another reason why Internet Explorer 11 improved the protection level was that the threats found for this test included 13 that targeted older versions of Internet Explorer. These threats had no negative effect on the newer version.

Updating Oracle Java and both Adobe Reader and Flash improved security by only a small amount. Only 12 attacks were blocked by an updated Java, while three attacks were foiled by Adobe updates.

These results do not mean that updating Java and Adobe products is a useless endeavour, but a fully up to date version of Internet Explorer countered these same threats plus very many more.

- **Patching supplements, but should not replace, anti-malware protection**

Updating Windows provides significant protection against the web threats used in this test. Using anti-malware software increases protection.

In this test seven threats were successful in subverting the target when Windows Updates were applied. In a simultaneous test published separately, but using the same threats, all anti-malware products protected against these same seven threats, with two exceptions.

The free anti-malware products from Avast! and Microsoft both missed one of the seven threats (in fact they both missed the same threat).

However, an updated system running either Avast! Free Antivirus or Microsoft Security Essentials would have been safe in 99 out of 100 incidents.

This test, in connection with its companion consumer anti-malware test[4], shows that updating Windows and third-party software, as well as installing anti-malware software, provides excellent levels of protection against malware.

Installing Windows Updates in isolation also provides impressive protection against malware.

- **Windows users who update regularly achieve much the same security regardless of which anti-malware software they choose**

Systems running anti-malware products that scored very well in our previous tests, without the benefit of recent Windows updates, experienced minimal further advantage once these were applied.

However, Windows updates added considerable extra protection when weaker anti-malware products were installed.

Consumer anti-malware products from Kaspersky Lab and Symantec scored 100 per cent without the support of Windows updates.

- **Does avoiding dubious websites help?**

Most of the malicious sites encountered in this test were legitimate sites that had been compromised to serve malware. It is hard to see how sensible use of the web would enable users to avoid these sites.

[3] SmartScreen Filter: frequently asked questions, Microsoft, http://windows.microsoft.com/en-GB/windows7/smartscreen-filter-frequently-asked-questions-ie9

[4] Home Anti-Virus Protection, April – June 2014, Dennis Technology Labs, http://dennistechnologylabs.com/reports/s/a-m/2014/DTL_2014_Q2_Home.1.1.pdf

APPENDIX A: FAQS

- This test was sponsored by Microsoft.
- The test rounds were conducted between 10th April 2014 and 17th June 2014 using the most up to date versions of the software updates available on any given day.
- A live internet connection was available throughout the test.
- The configuration of updates selected for this test were agreed between Dennis Technology Labs and Microsoft.
- Samples were located and verified by Dennis Technology Labs independently.
- Products were exposed to threats within 24 hours of the same threats being verified. In practice there was only a delay of up to three to four hours.
- The sample set comprised 100 actively-malicious URLs.

Do participating vendors know what samples are used, before or during the test?

No. Even we don't know what threats will be used until the test starts.

Each day we find new ones, so it is impossible for us to give this information before the test starts. Neither do we disclose this information until the test has concluded.

Do you share samples with the vendors?

Vendors may request a subset of the threats that compromised their products in order for them to verify our results.

The same applies to client-side logs, including the network capture files. There is a small administration fee for the provision of this service.

What is a sample?

In our tests a sample is not simply a set of malicious executable files that runs on the system.

A sample is an entire replay archive that enables researchers to replicate the incident, even if the original infected website is no longer available. This means that it is possible to reproduce the attack and to determine which layer of protection it was able to bypass.

Replaying the attack should, in most cases, produce the relevant executable files. If not, these are usually available in the client-side network capture (pcap) file.

For more information about malware samples please see the blog post: *What is a malware sample?*[5]

[5] What is a malware sample?, Simon PG Edwards, http://www.spgedwards.com/2013/07/what-is-malware-sample.html