



April 2014

Feature Article: XP-diency: what if you can't upgrade yet?



Table of Contents

| | |
|--|----|
| XP-diency: what if you can't upgrade yet?..... | 3 |
| ESET Corporate News | 6 |
| The Top Ten Threats..... | 7 |
| Top Ten Threats at a Glance (graph) | 11 |
| About ESET | 12 |
| Additional Resources..... | 12 |


XP-dieny: what if you can't upgrade yet?

David Harley, ESET Senior Research Fellow ESET North America
Small Blue-Green World

This article is based on recent ESET blogs concerning the demise of Windows XP: in particular, [5 Tips for protecting Windows XP machines after April 8, 2014](#) by ESET Distinguished Researcher Aryeh Goretsky and [XP-dieny: beyond the end of the line](#) by ESET Senior Research Fellow David Harley.

It won't have escaped your attention that Windows XP has reached its sell-by date as far as Microsoft is concerned. In fact, my colleague Aryeh Goretsky included links to a whole load of ESET's XP-related resources in his blog article [Goodbye Windows XP!](#) But what if you're not yet in a position to move on? Aryeh has already made several useful suggestions in his article [5 Tips for protecting Windows XP machines after April 8, 2014](#) (and I believe he'll be returning to that theme in the near future). Those points are repeated here because they're well worth remembering:

1. The first thing is to make sure that you back up your computer's files regularly, and periodically test you're backup strategy by restoring backups, preferably on a different computer, a few times a year. This helps ensure that in the event of a catastrophe, you will still have access to the information on your computer. The time to worry about your backups is not when faced with a virus, fire, earthquake or other calamity.
2. The next thing to do is to make sure that your copy of Windows XP is up-to-date. Although Microsoft stopped making *new* updates for Windows XP from April 8, 2014, all of the old updates from before then will still be available, and should be applied. This also applies to the device driver software (a device driver is a computer program that allows the operating system to communicate with a particular kind of hardware), which may be available from your computer manufacturer or Microsoft's Windows Update web site.
3. In addition to the operating system and drivers, you should also make sure you have the latest versions of your application software on the computer, and that those are fully-patched and updated. Programs like Adobe Flash, Adobe Reader and Oracle Corp.'s Java are frequently targeted by the criminal gangs that develop and use malware, so keeping these up-to-date is just as important as looking after the operating system. Other software that you use, such as Microsoft Office, web browsers and so forth, should be on the latest version and have the latest patches applied as well.
4. If the computer does not have to be connected to the Internet, disconnect or disable the connection so that the PC can only connect to other machines on the same non-Internet network. This will ensure that Internet-borne threats cannot directly attack your XP PC, and will make it harder for an attacker to steal data off the computer.
5. Make sure your security software is up-to-date, as well. There are lots of security programs available for Windows XP, and most of their authors have committed to supporting Windows XP for years to



come. Some are free, while others are sold as a subscription. A discussion of the features needed to protect Windows XP is outside the scope of this article, but at the very least, I would recommend looking for a security program that combines signature-based and heuristic detection, includes a firewall, and has some kind of host intrusion protection system. Vulnerability shielding and exploit blocking will be useful as well, as Windows XP will no longer be updated by Microsoft to protect against these types of attacks.

In general, of course, best practice is to upgrade from XP if at all possible as *soon* as possible – or even switch to a completely different operating system, though for people who have only used Windows, that’s liable to be a major disruption and a steep learning curve – but I can understand that there are systems around for which it may not really be feasible. For example, there are machines that possibly *can’t* be upgraded to a specification on which a later operating system will run realistically (kiosk machines, netbooks, cash machines). The Register article suggests that many specialist apps may be tied in to Internet Explorer 7, which can’t run on Windows 7 or 8.x: in fact, it attributes the bulk of the problem to the IE7 issue.


There is also hardware such as laboratory equipment that may be handicapped by proprietary software that may only run on older operating system versions, with no upgrade available (or so expensive that it’s economically more viable to pay for custom support while it’s available). I would guess that custom support is probably more economically feasible for those governments (like the UK and the Netherlands) and very large enterprises with large quantities of legacy machines than for small enterprises. And in any case, custom support is supposed to be a short term measure, requiring the customer to

implement a migration plan and declare a project completion date.

Much of the reportage about the end of XP support has focused on the need to upgrade the operating system and, if necessary, the hardware, rather than considering what happens if migrating isn’t currently an option. However, Gavin Clarke’s article for The Register on [Windows XP is finally DEAD, right? Er, not quite. Here's what to do if you're stuck with it](#) and [Gartner’s best practice guide for the secure use of XP](#) are exceptions.

Both articles make some good points:

- Editing the Registry so that Office and media components don’t execute programs by default.
- Control access to removable media and devices like smart phones that can be used for storage and transfer of files (including malware).
- Implement application control and memory protection, using (for instance) a host-based or network intrusion prevention system. Not a guarantee of complete protection, but then nothing is. Certainly a useful layer of protection, and I always advocate multi-layering.
- Keep applications updated and patched. Limit what applications (and types of applications) that are permitted.
- Remove Web browsing and email software from XP systems and provide those services from a patched and updated server. (Wow, that’s old school. Reminds me of the days when my work email and web



experience meant logging into a VMS or Unix server. But a thin client model, while potentially slower, may offer a certain amount of potential mitigation. It should, however, on no account be relied upon absolutely).

- Monitor Windows updates and community resources that might provide a guide to issues that might also apply to XP. Of course, what action you're able to take in such a case might be very limited. Even in a corporate context, I suspect that people and sites still saddled with XP machines are less likely to be expending resources on this kind of environmental scanning.

A point being *missed* by many outside the AV industry, however, is that there are plenty of attacks that don't rely on system exploits, and the other countermeasures discussed by Gartner won't necessarily protect against them. Nor, of course, will anti-virus, but up-to-date AV/security software still offers a useful layer of defence. And while Microsoft is removing availability of MSE for XP and won't support existing installations after July 2015, most AV vendors will continue to support it. ESET, for example, will support it till April 2017 and possibly later. However, it's not safe to assume that antivirus is a substitute for all the regular patches and updates that Microsoft provides for supported operating systems.


One of Gartner's suggestions is that network connectivity should be cut back as far as possible, to mitigate network-borne attacks. This sounds a bit like Marcus Ranum's [Ultimately Secure DEEP PACKET INSPECTION AND APPLICATION SECURITY SYSTEM](#): a pair of wire cutters. Ranum's point could be summarized as saying that connectivity *is* risk: however, the way that most systems are used nowadays really requires

network connectivity. It's true, of course, that the network is the primary attack vector, and you can get around the need for the network by using USB devices or optical media, the 21st century version of sneakernet (walking from one PC to another with a floppy disk). But looking at the added inconvenience, it could be more efficient economically to upgrade, even if means a hardware upgrade. There are less drastic solutions, of course: you could give XP machines internet access via the enterprise perimeter and the protection that offers (or should), while keeping them isolated from other machines on the network. That doesn't guarantee they won't be successfully attacked, but it does lower the risk to other machines.

Another suggestion is to remove administrative rights, which Gartner suggests should be mandatory for all remaining users on XP. *All* remaining users? You really need one privileged account for fixing problems and changing configurations, installing or updating software and so on. But then, no-one should be using a fully-privileged account for *routine* computing work, which I guess was meant to be the point.

Another Gartner suggestion is to have a plan to quarantine XP systems in the event of an attack.

You certainly need to be able to get systems off the network, and time spent on planning is rarely wasted, though the recommendation invites the question, how will you recognize a successful attack, or at any rate recognize it any more promptly than before? And shouldn't you already have a means of isolating any or all systems in the event of a breach? A critical XP exploitation is just one attack scenario, and not necessarily the likeliest. It's likely that XP-specific attack research will decline as XP's market share declines, especially in terms of attacks that target the large enterprises that can't afford to support XP indefinitely.



Also, this is all easier to say than do if you're considering systems that can't be disconnected or shut down without disruption and even damage, as may happen in some SCADA environments. Of course, SCADA systems that follow best practice by isolating critical machines from the network wherever possible are already less susceptible to attack.

ESET Corporate News

[ESET launches GoExplore.net to Celebrate the Best of the Web](#)

ESET announced the launch of GoExplore.net, the new internet initiative which curates the best of the web's content and encourages people to explore the web safely. With the World Wide Web reaching its 25th birthday this year, ESET has launched GoExplore.net to celebrate all things Internet. The site creates a web portal for everyone who wants to explore the online universe, upload interesting content and contribute to curating content for their fellow web surfers. GoExplore.net will offer exclusive interviews with high-profile internet heroes, how-tos, infographics and videos, as well as surveys and poll results.

ESET Announces Enterprise Grade Secure Authentication Software Development Kit

ESET launched the ESET Secure Authentication Software Development Kit (SDK). With this release, ESET provides system architects with a comprehensive developer guide in three, mainstream programming languages to add two-factor authentication (2FA) protection to nearly any system that requires protection. With a wide range of extensibility options, not only does the ESET Secure Authentication SDK provide user management, but it can be easily integrated into custom applications, such as corporate intranets or remote access systems. This integration means there are minimal external dependencies, full data control and zero need for a cloud data store—providing both SMBs and enterprises with all aspects of 2FA capabilities, including auditing, custom SMS gateway usage, logging and user authentication.



The Top Ten Threats

1. Win32/Bundpil

Previous Ranking: 1
Percentage Detected: 2.83%

Win32/Bundpil.A is a worm that spreads via removable media. The worm contains an URL address, and it tries to download several files from the address. The files are then executed and the HTTP protocol is used. The worm may delete the following folders:

- *.exe
- *.vbs
- *.pif
- *.cmd
- *Backup.

2. LNK/Agent.AK

Previous Ranking: 2
Percentage Detected: 1.96%

LNK/Agent.AK is a link that concatenates commands to run the real or legitimate application/folder and, additionally runs the threat in the background. It could become the new version of the autorun.inf threat. This vulnerability was known as Stuxnet was discovered, as it was one of four that threat vulnerabilities executed.

3. Win32/Sality

Previous Ranking: 3
Percentage Detected: 1.66%

Sality is a polymorphic file infector. When run starts a service and create/delete registry keys related with security activities in the system and to ensure the start of malicious process each reboot of operating system.

It modifies EXE and SCR files and disables services and process related to security solutions.

More information relating to a specific signature: http://www.eset.eu/encyclopaedia/sality_nar_virus_sality_aa_sality_am_sality_ah



4. HTML/ScrInject

Previous Ranking: 6
Percentage Detected: 1.66%

Generic detection of HTML web pages containing script obfuscated or iframe tags that automatically redirect to the malware download.

5. INF/Autorun

Previous Ranking: 4
Percentage Detected: 1.58%

This detection label is used to describe a variety of malware using the file autorun.inf as a way of compromising a PC. This file contains information on programs meant to run automatically when removable media (often USB flash drives and similar devices) are accessed by a Windows PC user. ESET security software heuristically identifies malware that installs or modifies autorun.inf files as INF/Autorun unless it is identified as a member of a specific malware family.

Removable devices are useful and very popular: of course, malware authors are well aware of this, as INF/Autorun's frequent return to the number one spot clearly indicates. Here's why it's a problem.

The default Autorun setting in Windows will automatically run a program listed in the autorun.inf file when you access many kinds of removable media. There are many types of malware that copy themselves to removable storage devices: while this isn't always the program's primary distribution mechanism, malware authors are always ready to build in a little extra "value" by including an additional infection technique.

While using this mechanism can make it easy to spot for a scanner that uses this heuristic, it's better to disable the Autorun function by default, rather than to rely on antivirus to detect it in every case.

6. Win32/Qhost

Previous Ranking: 5
Percentage Detected: 1.54%

This threat copies itself to the %system32% folder of Windows before starting. It then communicates over DNS with its command and control server. Win32/Qhost can spread through e-mail and gives control of an infected computer to an attacker.



7. Win32/Conficker

Previous Ranking: 7
Percentage Detected: 1.31%

The Win32/Conficker threat is a network worm originally propagated by exploiting a recent vulnerability in the Windows operating system. This vulnerability is present in the RPC sub-system and can be remotely exploited by an attacker without valid user credentials. Depending on the variant, it may also spread via unsecured shared folders and by removable media, making use of the Autorun facility enabled at present by default in Windows (though not in Windows 7).

Win32/Conficker loads a DLL through the svchost process. This treat contacts web servers with pre-computed domain names to download additional malicious components. Fuller descriptions of Conficker variants are available at http://www.eset.eu/buxus/generate_page.php?page_id=279&lng=en.

While ESET has effective detection for Conficker, it's important for end users to ensure that their systems are updated with the Microsoft patch, which has been available since the third quarter of 2008, so as to avoid other threats using the same vulnerability. Information on the vulnerability itself is available at <http://www.microsoft.com/technet/security/Bulletin/ms08-067.msp>. While later variants dropped the code for infecting via Autorun, it can't hurt to disable it: this will reduce the impact of the many threats we detect as INF/Autorun. The Research team in San Diego has blogged extensively on Conficker issues: <http://www.eset.com/threat-center/blog/?cat=145>.

It's important to note that it's possible to avoid most Conficker infection risks generically, by practicing "safe hex": keep up-to-date with system patches, disable Autorun, and don't use unsecured shared folders.

8. Win32/Ramnit

Previous Ranking: 8
Percentage Detected: 1.26%

It is a File infector that executes on every system start. It infects dll and exe files and also searches htm and html files to write malicious instruction in them. It exploits vulnerability on the system (CVE-2010-2568) that allows it to execute arbitrary code. It can be controlled remotley to capture screenshots, send gathered information, download files from a remote computer and/or the Internet, run executable files or shut down/restart the computer.



9. Win32/TrojanDownloader.Waski

Previous Ranking: n/a
Percentage Detected: 1.07%

Win32/TrojanDownloader.Waski is a trojan which tries to download other malware from the Internet. It contains a list of two URLs and tries to download a file from the addresses. The HTTP protocol is used. The file is stored in the location %temp%\miy.exe, and is then executed.

10. Win32/Dorkbot

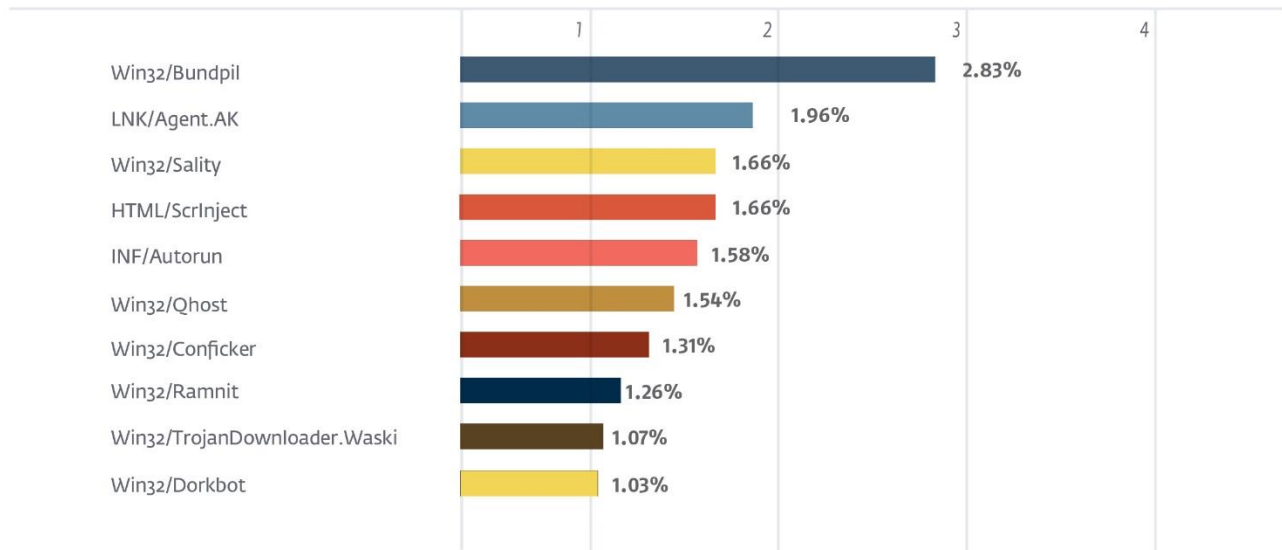
Previous Ranking: 9
Percentage Detected: 1.03%

Win32/Dorkbot.A is a worm that spreads via removable media. The worm contains a backdoor. It can be controlled remotely. The file is run-time compressed using UPX. The worm collects login user names and passwords when the user browses certain web sites. Then, it attempts to send gathered information to a remote machine. This kind of worm can be controlled remotely.

Top Ten Threats at a Glance (graph)

Analysis of ESET LiveGrid®, a sophisticated malware reporting and tracking system, shows that the highest number of detections this month, with 2.83% of the total, was scored by the Win32/Bundpil class of treat.

TOP 10 ESET LIVE GRID / April 2014





About ESET

ESET®, the pioneer of proactive protection and the maker of the award-winning ESET NOD32® technology, is a global provider of security solutions for businesses and consumers. For over 26 years, the Company continues to lead the industry in proactive threat detection. By obtaining the 80th VB100 award in June 2013, ESET NOD32 technology holds the record number of Virus Bulletin "VB100" Awards, and has never missed a single "In-the-Wild" worm or virus since the inception of testing in 1998. In addition, ESET NOD32 technology holds the longest consecutive string of the VB100 awards of any AV vendor. ESET has also received a number of accolades from AV-Comparatives, AV-TEST and other testing organizations and reviews. ESET NOD32® Antivirus, ESET Smart Security®, ESET Cyber Security® (solution for Mac), ESET® Mobile Security and IT Security for Business are trusted by millions of global users and are among the most recommended security solutions in the world.

The Company has global headquarters in Bratislava (Slovakia), with regional distribution centers in San Diego (U.S.), Buenos Aires (Argentina), and Singapore; with offices in Jena (Germany), Prague (Czech Republic) and Sao Paulo (Brazil). ESET has malware research centers in Bratislava, San Diego, Buenos Aires, Singapore, Prague, Košice (Slovakia), Krakow (Poland), Montreal (Canada), Moscow (Russia) and an extensive partner network for more than 180 countries.

More information is available via [About ESET and Press Center](#).

Additional Resources

Keeping your knowledge up to date is as important as keeping your AV updated. For these and other suggested resources please visit the [ESET Threat Center](#) to view the latest:

- [ESET White Papers](#)
- [WeLiveSecurity](#)
- [ESET Podcasts](#)
- [Independent Benchmark Test Results](#)
- [Anti-Malware Testing and Evaluation](#)