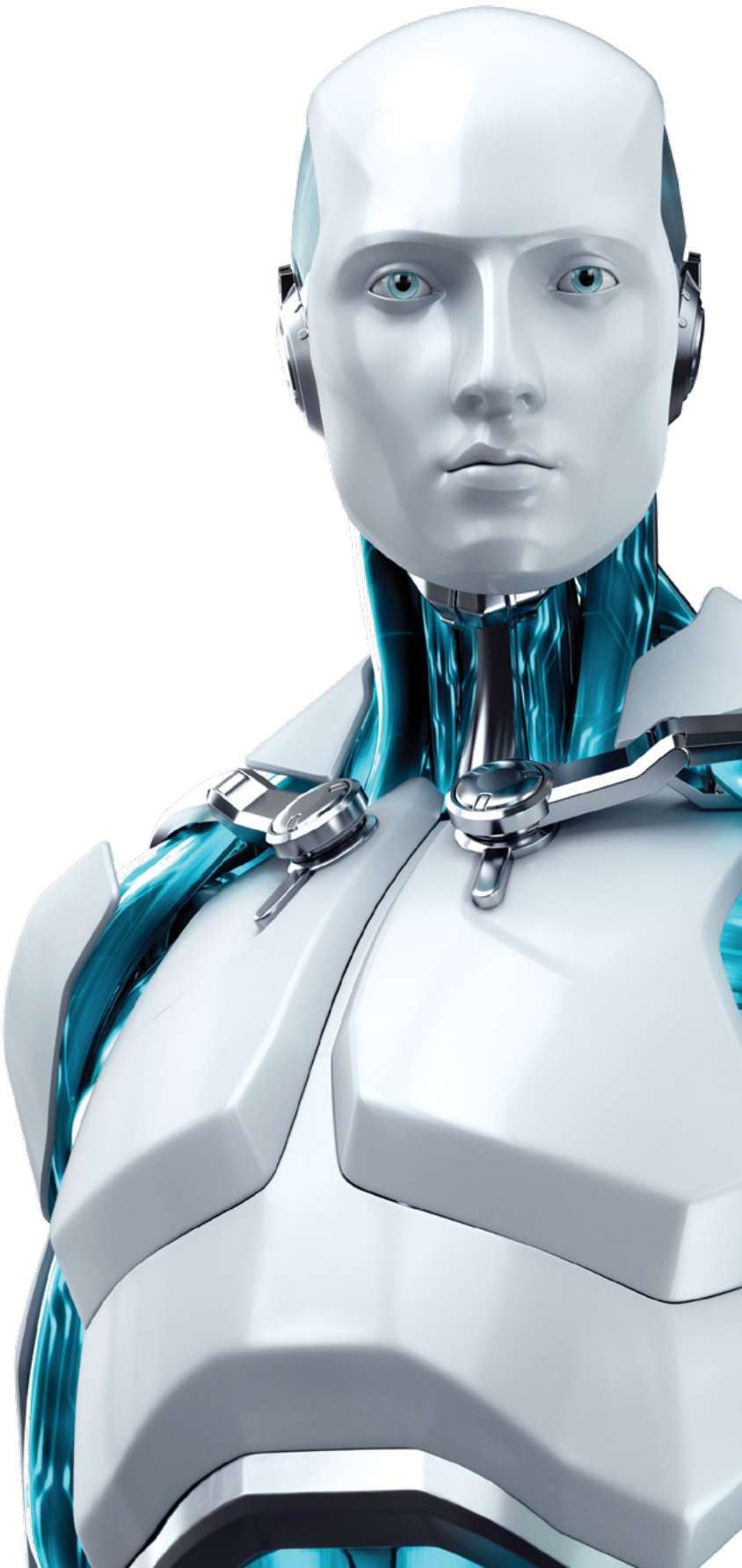
eset
Internet Security

WHITE PAPER

SIX MONTHS WITH WINDOWS® 8



SPRING 2013

ESET Internet Security

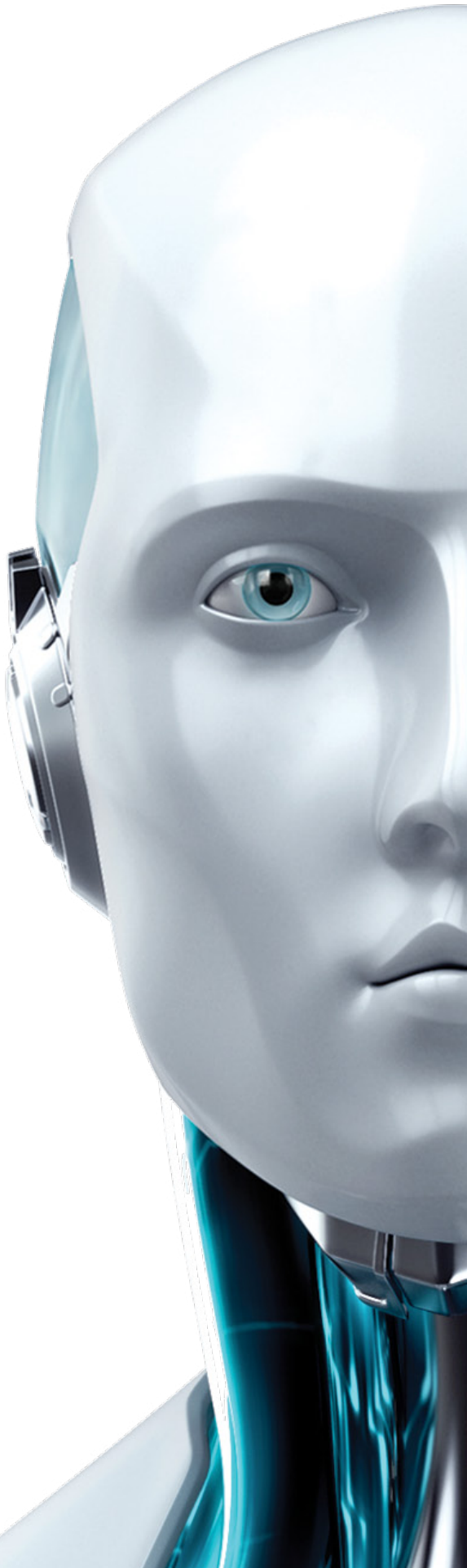


Table of contents

Introduction

Microsoft® Windows 8 has just reached its six-month anniversary [1], and we at ESET® thought now would be a good time to review where things stand with the latest incarnation of Microsoft's flagship operating system.

Today, all of ESET's software for Windows desktops is compatible with Windows 8. That is nothing unusual for ESET or other anti-malware developers, as Microsoft works closely with all anti-malware companies to ensure that their products are ready the same day a new version of Windows is on stores' shelves. At ESET, we were actually able to finish compatibility plans early and announced it on our blog before Windows 8 was released.[2]

Half a year later, most—if not all—other anti-malware companies have their own Windows 8 compatible versions, too. There is nothing unusual or otherwise remarkable about this, but it shows the industry's commitment to keeping computers secure.

Last year, ESET took an in-depth look at Windows 8's security, examining many of the advantages that characterize the new operating system from a security perspective, as well as the threats it might face, in our previous Windows 8 white paper, *Windows 8: FUD* for thought*. [3]

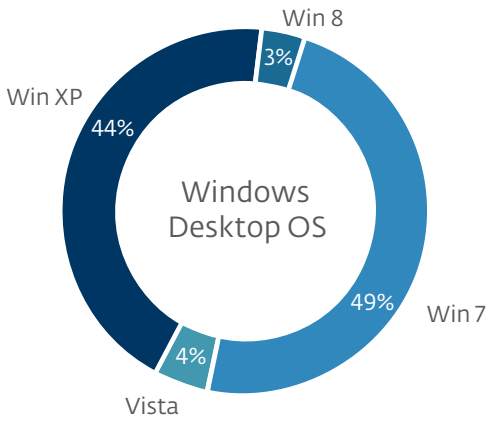
To round out our Windows 8 activities, ESET also presented a webinar, *Windows 8: Is It Time for Your Business To Go There?* and participated in an online hangout discussing *Windows 8, Malware & Security*, hosted by Lenovo®.

With all of these activities, ESET-the-company has been staying on top of Windows 8 security, but what has the experience been like for ESET's customers so far?

From looking at ESET's Live Grid™ telemetry, we see that 3% of our customers have already adopted Windows 8 for their desktop computers. While that number may sound low, it's important to remember that Windows 8 is only half a year old.

By comparison, Windows Vista™ has about 4% usage, and that was released in 2007.

Today, the majority of ESET's customers, are running Windows 7 (49%) on their desktops, followed by Windows XP (44%). There are still small amounts of PCs running Windows NT® 4.0 and Windows 2000; however, these came in at under one-tenth of one percent. Compared to reports from organizations which track Windows operating system version usage, such as the NPD Group and Net Applications, ESET has a slightly higher percentage of customers running Windows 7 and Windows 8, but trails when compared to data from gaming platform developer Valve [4].



Regardless of which version of Microsoft Windows our customers might be using, they all share a common heritage: being derived from the Windows NT kernel, which is now in its twentieth year.

A picture is worth a thousand words

While many of the most interesting improvements in Windows 8 relate to manageability, networking and security, these are largely "under-the-hood" features for most users, in the sense that they do not have many parts readily accessible from either the Start Screen *or* the Desktop. They may be buried deep in the operating system where they can only be managed from the command-line or via Group Policy. For many people, the graphic user interface provided by the Desktop ***is*** the operating system, and one of the biggest changes there is the replacement of the very desktop-centric ***Start Menu***, with the more tablet-centric ***Start Screen***.

Some start-ling behavior

We discussed the reasoning behind the change from the ***Start Menu*** to the ***Start Screen*** in the preceding white paper [5], but it interesting that nearly all of the negative discussions we have heard around Windows 8 focus not on such issues as paramount as performance, compatibility, security or reliability, but rather on distaste for the ***Start Screen***.

Whether you love it or hate it, this change to the Windows graphic user interface is miniscule, especially when compared to the types of changes that go into software as complex as a new version of Windows.

What it lacks in complexity, though, it makes up for in visibility. The ***Start Screen*** is an extremely visible change, and that has its own significance. As behavioral researchers will tell you, people rely foremost on visual cues for information about their environment, and when radical changes in an environment's appearance occur, this can generate a stress response. This has made for some fascinating reading, to put it mildly, in all of the reviews and comments about Windows 8's new look and feel.

One thing that goes largely unmentioned in these good vs. evil discussions of the ***Start Screen*** is that it is the gateway to the new Modern Windows Store apps (formerly called Metro apps before Windows 8 was released). The ***Start Screen*** is the foundation or "dock" upon which these programs' icons, which are now called ***tiles***, are located.

Rise of the Start Menus

Regardless of how you feel about Windows 8's Start Screen, one of the most interesting developments has been the creation of an entire new class of "Start Menu" utility programs, all designed to provide a "Start Menu"-like experience under Windows 8. Some of these programs are free, some are commercial, and they work with varying degrees of success and authenticity.

After a fashion, the emergence of this new class of software is very reminiscent to me of the utility programs designed to purge new computers of preloaded applications and trial versions of software, which are commonly referred to in disparagingly terms by computer owners with unflattering names such as "crapware," "garbageware," "shovelware," and so forth. It seems that when a computer experience is not optimal for the user, a market is created for entrepreneurs to provide solutions to correct the shortcoming, perceived or otherwise.

Interestingly enough, one of the several questions ESET is consistently asked about Windows 8, besides questions about compatibility, is whether we would detect such programs as being malicious, or at least Potentially Unsafe Applications.

The answer to that is a resounding **no**: ESET will not detect software just because it provides a Start Menu-like experience under Windows 8. If it's being detected, it's for some other reason.

Now, you can actually add, or ***pin***, a tile for a desktop Windows program to the ***Start Screen***, but clicking on it will launch the program on the "classic" Windows desktop. Modern Windows apps, though, are designed to run as full-screen programs (or split screen, if you have a high enough resolution display), and unlike their desktop counterparts, do not interact with any other programs or the Windows desktop.

The technical reason for this is that Windows desktop programs and Modern Windows apps are written using two separate application programming interfaces (APIs). An API is the set of instructions used by software to communicate with the operating system or other programs. The Win32® API [6] is the API used by previous versions of Windows, as well as "classic" Windows desktop programs. The new WinRT API is used in Windows 8 to create Modern Windows apps. In this case, each of the two APIs provides developers with different types of functionality in terms of how programs appear on the screen. With Modern Windows apps, applications run either as full screen or split in two across a screen, and support for multiple monitors is limited.

The three faces of Windows 8

At this point, it would probably be helpful to review the three broad categories of Windows 8 devices, the three separate versions of Windows 8 that those devices run, and the differences between them.

First, and foremost, are PCs, the classic personal computer. This classification covers everything from the smallest netbooks to notebooks to desktops and the largest workstations.

Technically speaking, this is also where dedicated servers would fit in, since they are derived from the personal computer. Servers, though, are typically used for very different purposes than PCs, and have their own server operating system, Windows Server® 2012, which is different enough from its desktop counterpart to merit separate discussion.

The personal computer

Regardless of how powerful they are, or who manufactured them, these computers are all capable of running the "PC" versions of Windows 8 and have the following in common:

- Contain a processor (CPU) manufactured by Intel® or AMD. The CPU may have an x86 (32-bit) or x64 (64-bit) architecture, but regardless of its "bittedness," it has to be compatible with the IA-32 (Intel Architecture, although other manufacturers have contributed) set of processor instructions.
- Are capable of using a keyboard, mouse, stylus, touchpad, touchscreen or other devices for input. Of course, not all PCs are going to be equipped with all of the different types of input devices available, but a keyboard option and some kind of pointing device are typically present.
- Can run **both** classic desktop programs written using the Win32 API and Modern Windows apps written using the WinRT API. Additionally, systems running a 64-bit edition of Microsoft Windows can also make use of the Win64 API as well.
- Can install classic desktop programs in different ways, such as downloading from the web, installing from a CD or DVD, and so forth). Modern Windows apps, though, must always be downloaded from the Windows Store.

Like previous versions of Windows for PCs, Windows 8 comes in multiple editions for use in businesses, homes and emerging markets.

The tablet

Windows tablets are the next class of computers. These are a new description for Windows computers used by Microsoft to describe systems running a special version of Windows 8 called Windows RT and not older Microsoft tablet systems, such as Microsoft Windows XP Tablet PC Edition [7]. Here's how these tablet devices differ from PCs:

- Contain a processor (CPU) manufactured by NVidia® or Qualcomm®. These new processors have a different architecture and use a different instruction set than those founds in PCs, known as ARM. If that sounds familiar, it's because the same chip design is used in devices like Apple's iPad® and iPhone®, as well as various Android™-powered tablets and smartphones.
- Are designed to use a touch screen primarily for input. Compared to early generations of touch-screen technology, the requirements for Windows Tablets are fairly high tech: The screens have to work with fingers, as opposed to a stylus, and support multi-touch with up to ten simultaneous contacts. This allows a portion of the display to be used as an on-screen keyboard. Of course, Windows Tablets support various wired and wireless keyboards and mouses, however, Windows RT is designed so that it can be used with just a touch screen.
- Primarily use a wireless connection for network access. This may be a typically 802.11n wireless LAN (WLAN) network connection, but 3G or 4G radios are often available for a wireless wide area network (WWAN) connection, and many devices may support a wired Ethernet connection through a dock or a USB adapter as well.
- Run only run Modern Windows apps written using the WinRT API.
- Install only Modern Windows apps through the Windows Store.

While the availability of third-party software for Windows RT is low compared to Windows 8, it is important to keep in mind that Windows RT has most of the same commands and files that come with Windows 8, allowing for some level of compatibility between such things as scripts and batch files.

Right now, there are not many Windows Tablets on the market, but some that you might be familiar with are the Lenovo Yoga™ 11 and Microsoft Surface™ tablets. There are also multi-touch tablet devices with Intel-compatible CPUs that run Windows 8 as well. Microsoft refers to these as "slates" in order to avoid confusion with the Windows RT-running tablets.

The smartphone

Smartphones are the third class of devices running Windows 8, and the special version of Windows 8 they run is called **Windows Phone 8**. Microsoft has now been in the smartphone business for years, but all of its previous operating systems, Windows Mobile and Windows Phone 7.*n*, were based on Windows CE, an operating system originally designed for PDAs. With Windows Phone 8, Microsoft has broken with this tradition of using Windows CE for its operating system kernel, instead relying on Windows 8 NT-based kernel as the basis for the new generation of its smartphone operating system.

Like the tablets that run Windows RT, **Windows Phone 8** devices do not use an Intel-compatible CPU, instead relying on an ARM-based model manufactured by Qualcomm. To create apps on Windows Phone 8, developers make use of the *Windows Phone Runtime*, which itself is a subset of the WinRT API. Also, applications can only be installed through the *Windows Phone Store*, a similar, but separate service from the *Windows Store* used by both Windows 8 and Windows RT.

If that all seems a little confusing, the following chart shows the differences between the devices, CPUs, operating systems, APIs and software markets.

TYPE OF DEVICE	TYPE OF CPU	RUNS WHICH OS?	USES WHICH API(S)?	SOFTWARE AVAILABILITY
PC *(all-in-one, desktop, laptop, netbook, server, slate, ultrabook, workstation, Surface Pro and so forth)*	32-bit or 64-bit CPU that follows IA-32 instruction set *(a/k/a x86, x86-64, i386, AMD64 e.g.)*	Windows 8	Win32, WinRT, Win64 *(if 64-bit CPU and OS)*	Internet, Retail *(CD's & DVDs)*, Windows Store, etc.
Tablets *(Lenovo Yoga 11, Microsoft Surface and so forth)*	ARM instruction set *(NVidia and Qualcomm CPUs)*	Windows RT	WinRT	Windows Store
Smartphones *(HTC™ 8x, Nokia Lumia™, Samsung Focus™, and so forth)*	ARM instruction set *(Qualcomm CPUs only)*	Windows Phone 8	Windows Phone Runtime *(subset of WinRT)*	Windows Phone Store

Of tablets and tiles

So, now that you have an understanding of the three very different versions of Windows 8 out there, the APIs that they use, and their CPUs, there is probably one question that you now want to ask ESET: *Which of these devices do you protect?* The answer to that question is quite simple: ESET protects PCs running Windows 8. The reasoning behind that answer, though, is quite complex.

ESET is, primarily, a PC software vendor, and the anti-threat software we develop is still primarily for PCs these days, although the threats our software detects are increasingly not PC-based, but web-based, targeting non-Windows tablets and smartphones and so forth. Of course, we also develop versions of our software to run on servers, PCs running other operating systems like Linux™, Apple® Macs, Android-powered smartphones and tablets and so forth. We even have an app for the iPhone. And while it may change in the future, the majority of ESET's customers today run our software on their Windows PCs.

Given that ESET does have non-PC and non-Windows versions of its software available, you are probably wondering where the Windows RT and Windows Phone 8 versions of our software are and that brings us to discussion of the operating systems and the APIs that they support.

Deep in the heart of Windows 8

Windows 8, the version that runs on PCs, is the direct linear descendent of Windows 7. It runs (largely) on the same hardware as Windows 7; even the system requirements are almost identical. Although Windows 8 ***does*** support the new Windows Store and WinRT API, it also allows users to install software using traditional methods and supports the "legacy" Win32 and Win64 APIs. While the requirement that Modern Windows apps install only through the store is not a stumbling point for developing anti-malware software, it is the differences between the Win32/Win64 and WinRT APIs, and the classic desktop and Modern Windows apps they allow you to create, that forego the development of certain types of software.

Anti-malware software needs to interact with computers at a lower level than most other programs, a trait they share with several classes of other applications. Examples of such software include backup, defragmentation, encryption, firewall and VPN programs, all of which need to interact with a computer's CPU or network connection in various ways. What may also be surprising is that programs from computer manufacturers that control hardware features, such as toggling wireless radios on and off, telling you what network you have connected to, reporting on the status of the CPU or cooling fans, also fall into the same category.

The reason behind all of this is that despite their seemingly different functions, these types of programs all require not just access to the lowest layers of the operating system, but the ability for their lowest level of components — known as drivers and services — to communicate "upward" with the layers above them, ultimately interacting with you via the graphic user interface.

Unfortunately, while Modern Windows applications do have the ability to interact via the GUI and perform most types of file-related functions (reading, writing, updating and deleting files, and so forth), they are isolated from accessing the lower levels of the system. The WinRT API provides very limited functionality for interacting with drivers and services, and what is available is very restricted, for example, adjusting speaker volume or screen brightness. This is a very similar situation to that we find with iOS or Android.

While the goal behind "sandboxing" or limiting the WinRT API's access to the operating system is a good thing, since it makes it more difficult for attackers to target the underlying operating system, it also means certain types of applications will not be developed by third parties as Modern Windows apps.

Developers take heed

Microsoft's developer guidelines for Modern Windows applications prohibit developers from creating apps that make use of the Win32 and Win64 APIs, and apps which did so would not only fail to meet the Windows 8 logo guidelines[8], they would likely be detected by Microsoft during the application approval phase for the Windows Store. At the very least, this would strain the relationship between that developer and Microsoft and, at the worst, that developer could be removed from Microsoft's developer program. This is not specific to Microsoft, though: An application developer who violated the guidelines Apple's or Google's markets lay down would likely get thrown out of their developers programs as well.

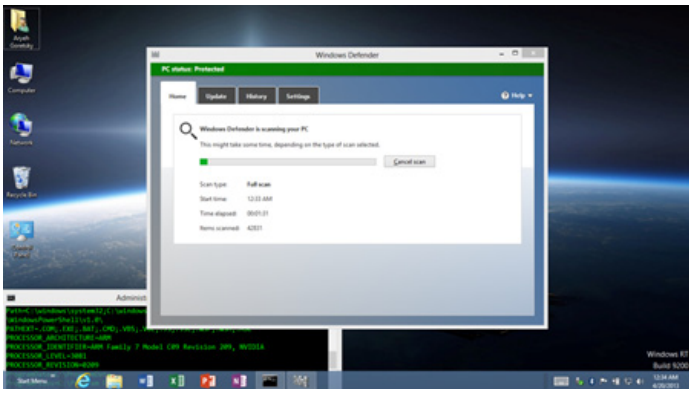
What I would like to point out, though, is that when operating system vendors like Microsoft and Apple limit what kinds of apps developers can create and then screen them, is not, in and of itself, a bad thing from a security perspective: It greatly reduces the chance of an app's being approved that contains malicious code or a vulnerability that could be exploited to attack the operating system. Both Apple's App Store and Google Play™ have been incredibly successful markets for software developers, and these kinds of protections are meant to secure the applet-style ecosystem they nurture. Apple, Google™ and Microsoft all have the ability to withdraw or disable apps in their stores and on devices, so in the event a malicious app bypasses all the prequalification mechanisms, it can be prevented from causing further damage.

While developer guidelines, curatorship and remote removal of apps may seem somewhat draconian, the risks from improperly securing the application marketplace are not inconsequential: Previous versions of Windows had a feature called Windows Sidebar, which ran small programs called Windows Gadgets. As it turns out, it was possible to create a malicious Windows Gadget that could attack the computer by exploiting vulnerabilities in Windows Sidebar. Microsoft did not include support for the Windows Sidebar in Windows 8 and released a tool to disable it under Windows Vista and Windows 7.[9,10]

A few of the anti-malware vendors out there have applications for Windows 8, listed in the Security section of the Windows Store. However, if you take a look at them, these are actually classic Windows programs being sold through the store, or they are tools to provide news and information. Personally, I call the latter "brochure apps," because they only provide information about the company. There's nothing wrong with that — even ESET has a Threat Center app for Apple iOS for viewing news and threat data — but there's a difference between providing company information and protecting a computer from threats.

A small surprise for tablet security

While there are no third-party security apps for Windows RT, such as anti-malware programs or firewalls, this does not mean it is without defenses. Windows RT was derived from Windows 8 and as such has many of the same security features as Windows 8, such as UEFI Secure Boot, and entirely new ones, such as only allowing signed code from Microsoft being allowed to run on its desktop. Since Windows RT is based on Windows 8, that means it comes with the same anti-malware software; Microsoft's Windows Defender, which can be seen in operation under Windows RT in the following screen capture:



While the utility of including such a program may be questionable, it does show Microsoft's willingness to protect Windows RT against platform nonspecific threats which appear via the web-browser, or even against hypothetical WinRT/ARM-based threats that haven't yet appeared at all. In the event such threats *do* appear, it will be interesting to see if Microsoft opens up Windows RT to allow development of third-party security applications.

The Windows 8 threatscape

In the *Windows 8: FUD for Thought* white paper, ESET made some predictions about how Windows 8's new defenses would spawn new attacks. So, a half year later, how did we do?

- We predicted an increase in malicious software which interacts with the users, such as fake antivirus programs and ransomware. While fake antivirus programs have not gone away [11], we have seen a steady move toward ransomware and banking Trojans, which may come from the same sources as the FakeAV programs. [12, 13, 14]
- Targeting of popular social networking, webmail web sites and online gaming services continues unabated, exposing victims to credit card fraud, identify theft and malware. [15, 16, 17, 18]
- We have yet to see attacks specifically using hardware sensors under Windows 8, however, capturing the location of criminals through cell phone tower triangulation and GPS data via smartphone is becoming a common tool by law enforcement, and the radios in these use the same technology as those in tablet and notebook computers. [19, 20, 21]
- We have not found any instances where legitimate software developers have been targeted in order to get malicious apps into the Windows Store; however, we have found apps in there that could certainly be described as questionable. More on that, next…

Predicting the future is often less science than it is an art for practitioners in the field of information security; however, while Windows 8's current market share may be preclude it from targeting by unique attacks, the threat vectors we identified do seem to be increasingly used for all other desktop versions of Windows, too.

Holding the line

One of the major advances in Windows security was the introduction of UEFI Secure Boot in 64-bit editions of Windows 8.[22] Designed to prevent a class of rootkits called bootkits, it provides the bottom-most layer of security upon which Microsoft's Trusted Boot [23] process is built. To date, we have not seen bootkits capable of bypassing UEFI Secure Boot. Rootkits do continue to be a problem on older versions of Windows, as well as 32-bit editions of Windows 8,[24] which do not have Secure Boot functionality due to reasons of legacy compatibility.

Given that Windows 8 is still relatively new and its market share is so far quite small, it is still too early to tell whether the lack of 64-bit rootkits that target it is due to the intrinsic current effectiveness of Microsoft's Trusted Boot process, or to a lack of interest by malware authors in creating 64-bit bootkits. Given that announcing such a bootkit would generate considerable fame in criminal circles, we suspect the answer to be both a combination of technical hurdles and lack of ROI for creating such malware.

It should be noted, though, that despite Windows 8's protections against rootkits, many conventional file-based forms of malicious software, such as viruses, worms, Trojan horses, bots and Fake AV programs, do indeed work under it, although often with a lower chance of success. These programs do not necessarily make use of the same types of functions as their stealthier bootkit brethren, but if they do, they are more likely to be blocked by the vulnerability mitigations introduced in Windows 8, especially when compared to an earlier operating system, such as Windows XP.[25] Of course, a variety of both free and commercial Windows-8-compatible anti-malware software is readily available, should one choose not to rely on the built-in Windows Defender software.

Breaching the gates of the Windows Store

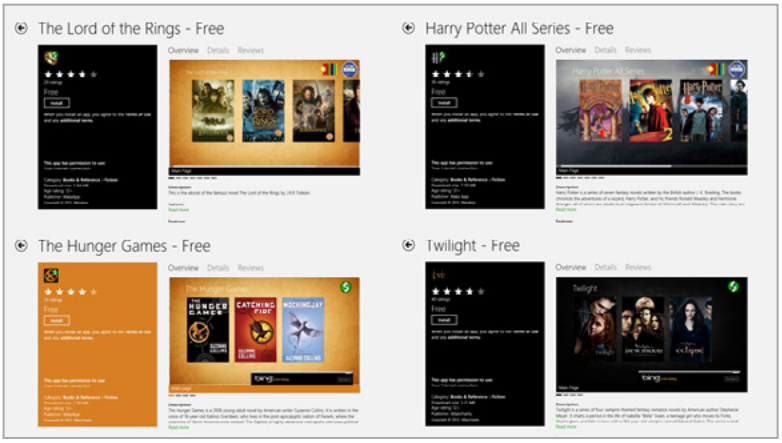
Last year, we looked at the Windows Phone store to see if any malicious apps were available for download through it.[26] At that time, it had just about 60,000 apps in it. As of this writing, the Windows Store for Windows 8 now contains about 60,000 apps, which makes for a good numerical basis for comparison.[27]

When examining the Windows Phone marketplace, we did not come across any apps that behaved like a virus, worm or similar type of malicious program. We did find that four (4) applications, out of the approximately 60,000 that were then available, had been removed for various reasons, including fraud, violating developer policies and a trademark violation. We calculated the "removal-ratio" for Windows Phone apps at 1:15,000, although this is a very small sample size from which to extrapolate. By comparison, the Google Play Store had approximately 800,000 [28] apps in it as of January 2013, but it removed over 60,000 [29] apps the following month, giving the Google Play Store a removal-ratio of 1:13 for Android apps.

While investigating the Windows Store for malicious Modern Windows apps, a similar pattern to the Windows Phone Store appeared: No actual malicious apps were found, but a variety have been removed for similar reasons, including a fake version of VLC Media Player [30], a free video player which is often re-sold by scammers to unsuspecting computer users. An unofficial Windows 8 Complaints app was also removed by Microsoft, likely for trademark violations. [31] In most other instances, apps were removed due to technical issues such as bugs or security issues, although at least one other app, an unofficial BBC news app, was removed for a terms-of-service violation with that organization. [32]

Although no actual malicious software was found during our examination of the Windows Store, ESET did have a bit of a shock when looking through a most unlikely location: The Windows Store's *Top free in Books & Reference* category. This group is best known for containing such apps as ebook and comic readers, encyclopedias and various religious texts so, understandably, we were a bit surprised when we found what appeared to be no less than four pirated bestselling ebook series.

The four ebooks found were J.R.R. Tolkien's The *Lord of the Rings* series, J.K. Rowling's *Harry Potter* series, Suzanne Collins' *The Hunger Games* series and Stephanie Meyer's *Twilight* series:



All four books are being offered as self-contained ebooks, both as free ad-supported apps in the Windows Store and also as ad-free versions priced between $1.99 and $2.99, should one get tired of seeing advertisements. The publishers and Microsoft have all been notified, but as of the time of writing, all of these ebooks were still available in the Windows Store.

Ebook piracy is common, even if exact statistics are hard to come by and somewhat fragmentary. [33, 34, 35, 36] It does seem, though, that the majority of ebook piracy comes from peer-to-peer file sharing and digital file locker services, as opposed to through channels such as vendor marketplaces like the Windows Store. Lest one draw the conclusion that this is solely a Microsoft phenomenon, we should point out that Apple was found guilty of copyright infringement for having pirated Chinese ebooks available in its app store. [37]

BYOD and FYOL (face your own lawsuit)

ESET has been looking at the risks [38] associated with the consumerization of IT and its Bring Your Own Device (BYOD) trend for a while now, although to date those have largely focused on risks to corporate data, [39, 40, 41] and risks in healthcare [42] and the military.[43] We had not, however, given much thought to issues involving the stealing of copyrighted materials, especially as it applied to various ecosystems and online marketplaces.

The ease with which apparently-pirated ebooks can be downloaded from the Windows Store brings up an interesting risk associated with BYOD: When a person uses his/her personal equipment to infringe copyright and consume pirated materials, he/she is solely responsible. But when that equipment is then used at work, is the employer responsible?

This suggests further complexities, such as whether employers have the right to check employees' personal devices, not just for malware or out-of-date software, but also for copyrighted material such as music and videos. Corporations wishing to save money on equipment costs by allowing employees to use their own devices for work may ultimately find that instead of saving any money, they are only shifting internal expenses between their IT and legal departments.

Under Windows 8, the controls available for managing admittance to the Windows Store are not particularly stringent: Access to the Windows Store can be toggled via Group Policy, and companies can publish their enterprise line of business (LOB) apps [44] through a private instance of the Windows Store. [45] This current "on or off" level of granularity may be off-putting to businesses wishing to extend BYOD support to employees with Windows 8 devices, especially given the concerns laid out above.

Conclusion

Despite some predictions that Microsoft Windows 8 would be "doomed" from a security standpoint,[46] Windows 8 is on track with ESET's earlier prediction that it would be the most secure version of Windows ever. In the first six months on the market, no major security vulnerabilities have been exploited. While adoption of this newest version of Windows is not occurring at the same rate at which Windows 7 replaced Windows Vista, that is due more to Windows 7's widespread adoption compared to the comparatively unpopular Windows Vista. In the meantime, Windows 8 continues to slowly grow its presence, especially as more touch-screen-capable devices arrive in the marketplace.

Microsoft has been quite reticent about discussing the successor to Windows 8, code-named Windows Blue, but it does seems to be shifting toward releasing new versions of the operating system which are smaller in total scope but more frequent, similar to Apple's release-cycle model for OS X. [47]

It may be that enterprises are currently reluctant to face the risks associated with copyright infringement in BYOD scenarios. This might be addressed by improvements to both the Windows Store and versions of Windows in the future.

While labeled by some as a transitional operating system between the PC and the tablet, Windows 8 seems to provide a rock-solid foundation from a security perspective, and switching to more frequent release cycles will allow Microsoft to update the operating system's kernel and core security features more frequently to adapt to new threats, as well as more rapid deprecation of older, more insecure features.

The author wishes to thank his colleagues Jean-Ian Boutin, David Harley, Fer O'Neil, Juraj Malcho and Patrik Sučanský for their assistance in preparing this white paper. If you have any questions or feedback about this white paper or would like to contact the author, please feel free to do so via the AskESET@eset.com mailbox.

Author bio

Aryeh Goretsky holds the position of Distinguished Researcher at global security provider ESET, where he is responsible for a variety of activities, including threatscape monitoring, investigations, working with technical staff, and liaising with other research organizations, security mailing lists and web forums. Aryeh was the first employee at McAfee in 1989, where he began his career answering questions about computer viruses and is a veteran of several software and networking companies, including instant-messaging pioneer Tribal Voice and VoIP hardware manufacturer Zultys Technologies.

Aryeh is a manager with the Zeroday Emergency Response Team and is the recipient of several industry awards, including Lenovo's Community Advocate Award, Microsoft's Most Valuable Professional Award, and he is recognized by tech news site Neowin as a Most Valuable Contributor.

Aryeh contributes regularly to both at ESET's blog, We Live Security, where he talks about the latest threats, and ESET's online support forum, where he answers questions about anti-malware technologies.

In his spare time, Aryeh enjoys scanning for viruses and backing up his data.

About ESET

ESET is on the forefront of proactive endpoint protection, delivering trusted security solutions to make the Internet safer. For over 25 years, ESET has helped customers get the most out of their technology by creating a more secure and trusted online experience with antivirus software for consumers and endpoint security solutions for businesses. To learn more about how ESET can protect your environment, go to www.eset.com

References

1. Microsoft. "Windows 8 Arrives." 25 Oct. 2012. Microsoft Corp. https://www.microsoft.com/en-us/news/Press/2012/Oct12/10-25Windows8GAPR.aspx
2. Goretsky, Aryeh. "W8ing for V6: What ESET has in store for Windows 8 Users." 23 Oct. 2012. ESET. http://www.welivesecurity.com/2012/10/23/w8ing-for-v6-what-eset-has-in-store-for-windows-8-users/
3. Goretsky, Aryeh. "A white paper: Windows 8's Security Features." Oct. 9 2012. ESET. http://www.welivesecurity.com/2012/10/09/windows-8s-security-features/
4. Steamworks. "Steam Hardware & Software Survey: April 2013" Valve Corp. http://store.steampowered.com/hwsurvey?platform=pc
5. Goretsky, Aryeh. "A white paper: Windows 8's Security Features." Oct. 9 2012. ESET. http://www.welivesecurity.com/2012/10/09/windows-8s-security-features/
6. Windows Dev Center. "Windows API List." Retrieved 1 May 2013. Microsoft Corp. http://msdn.microsoft.com/en-us/library/windows/desktop/ff818516%28v=vs.85%29.aspx
7. MSDN Library. "Windows XP Tablet PC Edition." Retrieved May 7, 2013. Microsoft Corp. http://msdn.microsoft.com/en-us/library/ms950406.aspx
8. Dev Center. "Windows 8 and Windows RT Compatible Logo Usage Guidelines." Retrieved May 7, 2013. Microsoft Corp. http://msdn.microsoft.com/en-us/library/windows/desktop/jj591630.aspx
9. Raff, Aviv and Amit, Iftach Ian. DEF CON15, 2007, Las Vegas. "The Inherent Insecurity of Widgets and Gadgets." http://www.defcon.org/images/defcon-15/dc15-presentations/dc-15-raff_and_amit.pdf
10. Security TechCenter. "Microsoft Security Advisory (2719662): Vulnerabilities in Gadgets Could Allow Remote Code Execution." Jul. 10, 2012. Microsoft Corp. http://technet.microsoft.com/en-us/security/advisory/2719662
11. Boutin, Jean-Ian. "Online PC Support scam: from cold calling to malware" Apr. 18, 2013. ESET. http://www.welivesecurity.com/2013/04/18/online-pc-support-scam-from-cold-calling-to-malware/
12. Cobb, Stephen. "The Industrialization of Malware: One of 2012's darkest themes persists." Dec. 31, 2012. ESET. http://www.welivesecurity.com/2012/12/31/the-industrialization-of-malware-one-of-2012s-darkest-themes-persists/
13. Editor. "Europol shuts down global ransomware network." Feb. 14, 2013. ESET. http://www.welivesecurity.com/2013/02/14/europol-shuts-down-global-ransomware-network/
14. Boutin, Jean-Ian. "Code certificate laissez-faire leads to banking Trojans." Feb. 21, 2013. ESET. http://www.welivesecurity.com/2013/02/21/code-certificate-laissez-faire-banking-trojans/
15. Lipovsky, Robert. "PokerAgent botnet stealing over 16,000 Facebook credentials." Jan. 29, 2013. ESET. http://www.welivesecurity.com/2013/01/29/pokeragent-botnet-stealing-over-16000-facebook-credentials/
16. Vickery, Jeanne. "Yahoo Hacked: CEO Mriisa Mayer Faces Hacking Incident During First Year on the Job." Feb. 25, 2013. Policymic. http://www.policymic.com/articles/27916/yahoo-hacked-ceo-marissa-mayer-faces-hacking-incident-during-first-year-on-the-job
17. Editor. "Gamers warned of risk of "always online" games such as SimCity and Diablo." Mar. 27, 2013. ESET. http://www.welivesecurity.com/2013/03/27/gamers-warned-of-risks-of-always-online-games-such-as-simcity-and-diablo/
18. Editor. "Twitter blames spear-phishing for recent hacks – and warns news companies to expect more." Apr. 30, 2013. ESET. http://www.welivesecurity.com/2013/04/30/twitter-blames-spear-phishing-for-recent-hacks-and-warns-news-companies-to-expect-more
19. Zetter, Kim. "Secrets of FBI Smartphone Surveillance Tool Revealed in Court Fight." Apr. 9, 2013. WIRED. http://www.wired.com/threatlevel/2013/04/verizon-rigmaiden-aircard/

20. Tuccile, J.D. "LAPD Cellphone Tracking Clarification Still Raises Concerns." Apr. 12, 2013. Reason. http://reason.com/blog/2013/04/12/lapd-cellphone-tracking-clarification-st
21. Sengupta, Somini. "For Congress, a Question of Cellphone Tracking." Apr. 25, 2013. The New York Times. http://bits.blogs.nytimes.com/2013/04/25/for-congress-a-question-of-cellphone-tracking/
22. Goretsky, Aryeh. "A white paper: Windows 8's Security Features." Oct. 9, 2012. ESET. http://www.welivesecurity.com/2012/10/09/windows-8s-security-features/
23. Niehus, Oliver. "Windows 8: Trusted Boot: Secure Boot – Measured Boot." Jan. 9, 2013. Microsoft. https://blogs.msdn.com/b/olivnie/archive/2013/01/09/windows-8-trusted-boot-secure-boot-measured-boot.aspx
24. Matrosov, Aleksandr. "Mysterious Avatar rootkit with API, SDK, and Yahoo Groups for C&C communication." May 1, 2013. ESET. http://www.welivesecurity.com/2013/05/01/mysterious-avatar-rootkit-with-api-sdk-and-yahoo-groups-for-cc-communication/
25. Microsoft. "Microsoft Security Intelligence Report, Volume 14." 2013. Microsoft Corp. http://download.microsoft.com/download/E/0/F/E0F59BE7-E553-4888-9220-1C79CBD14B4F/Microsoft_Security_Intelligence_Report_Volume_14_English.pdf
26. Goretsky, Aryeh. "Windows Phone 8: Security Heaven or Hell?." Feb. 24, 2012. ESET. http://www.welivesecurity.com/2012/02/24/windows-phone-8-security-heaven-or-hell/
27. Pachal, Pete. "Windows 8 Milestones: 100 Million Licenses Sold, 60,00 Apps." May 6, 2012. Mashable. http://mashable.com/2013/05/07/windows-8-100-million/
28. McCarra, Darren. "Google Play will hit one million apps in June." Jan. 4, 2013. The Sociable. http://sociable.co/mobile/google-play-will-hit-one-billion-apps-this-june/
29. Editor. "Android app store has serious clean-up with 60,000 apps removed." Apr. 11, 2013. ESET. http://www.welivesecurity.com/2013/04/11/android-play-store-has-serious-clean-up-with-60000-apps-removed/
30. Callaham, John. "VideoLAN team to get fake VLC Windows 8 app removed from Windows Store." Jan. 10, 2013. Neowin. http://www.neowin.net/news/videolan-team-to-get-fake-vlc-windows-8-app-removed-from-windows-store
31. Callaham, John. "Windows 8 Complaints app removed from Windows Store." Dec. 28, 2012. Neowin. http://www.neowin.net/news/windows-8-complaints-app-removed-from-windows-store
32. Warren, Tom. "Microsoft employee forced to remove unofficial BBC apps for Windows (update)" Mar. 29, 2013. The Verge. http://www.theverge.com/2013/3/29/4160036/bbc-news-apps-removed-from-windows-stores
33. Boutin, Paul. "E-book piracy costs U.S. publishers $3 billion, says study." Mar. 2, 2010. VentureBeat. http://venturebeat.com/2010/03/02/book-piracy-costs-u-s-publishers-3b-says-study/
34. Guzeva, Alexandra. "Pirates in Russian plunder e-book market." Jul. 4, 2012. The Telegraph. http://www.telegraph.co.uk/sponsored/russianow/business/9375763/russia-ebook-market-pirates.html
35. Guzeva, Alexandra. "Pirates in Russian plunder e-book market." Jul. 4, 2012. The Telegraph. http://www.telegraph.co.uk/sponsored/russianow/business/9375763/russia-ebook-market-pirates.html
36. Havocscope. "Illicit Trade Value: Book Piracy." Retrieved May 7, 2013. Havocscope, LLC. http://www.havocscope.com/tag/book-piracy/
37. Yin, Cao. "Copyrights take a bite out of Apple." Apr. 24, 2013. China Daily Information Co. http://www.chinadaily.com.cn/business/2013-04/24/content_16443247.htm
38. Camp, Cameron. "The BYOD security challenge: How scary is the iPad, tablet, smartphone surge?" Feb. 28, 2012. ESET. http://www.welivesecurity.com/2012/02/28/sizing-up-the-byod-security-challenge/
39. Camp, Cameron. "Rogue mobile devices in your enterprise? RSA day one." Feb. 29, 2012. ESET. http://www.welivesecurity.com/2012/02/29/rogue-mobile-devices-in-your-enterprise-rsa-day-one/
40. Zweinenberg, Righard. "From BYOD to CYOD: Security issues with personal devices in the workplace." Feb. 18, 2013. ESET. http://www.welivesecurity.com/2013/02/19/from-byod-to-cyod-security-issues-with-personal-devices-in-the-workplace/
41. Zwienenberg, Righard. VB2012, 2012, Dallas. "BYOD: (B)rought (Y)our (O)wn (D)estruction?" http://go.eset.com/us/resources/white-papers/Zwienenberg-VB2012.pdf

42. Editor. "Report: Growing use of BYOD in American healthcare a consumer worry." Feb. 6, 2013. ESET.
http://www.welivesecurity.com/2013/02/06/report-growing-use-of-byod-in-american-healthcare-a-consumer-worry/
43. Editor. "Army faces "enemy within" as 14,000 BYOD devices pose cybersecurity headache." Apr. 3, 2013. ESET
http://www.welivesecurity.com/2013/04/03/army-faces-enemy-within-as-14000-byod-devices-pose-cybersecurity-headache/
44. Dev Center. "Design case study: Enterprise line of business Windows Store app." Retrieved May 8 2013. Microsoft Corp.
http://msdn.microsoft.com/en-us/library/windows/apps/jj659079.aspx
45. Sutherland, Jeffrey. MSDN Blogs. "Managing "BYO" PCs in the enterprise (including WOA)." Apr. 19, 2012. Microsoft Corp.
https://blogs.msdn.com/b/b8/archive/2012/04/19/managing-quot-byo-quot-pcs-in-the-enterprise-including-woa.aspx
46. James, Geoffrey. "Why the Microsoft Surface is Doomed." Dec. 12, 2013. Inc. Magazine.
http://www.inc.com/geoffrey-james/why-the-microsoft-surface-is-doomed.html
47. Fried, Ina. "Microsoft Confirms Windows Blue Update Coming; Says Windows 8 Passes 100 Million Licenses Sold." May 6, 2013. All Things D.
http://allthingsd.com/20130506/microsoft-confirms-windows-blue-update-coming-says-windows-8-passes-100-million-downloads