Windows 8: FUD* for thought

*Fear, Uncertainty, Doubt

Aryeh Goretsky, MVP, ZCSE

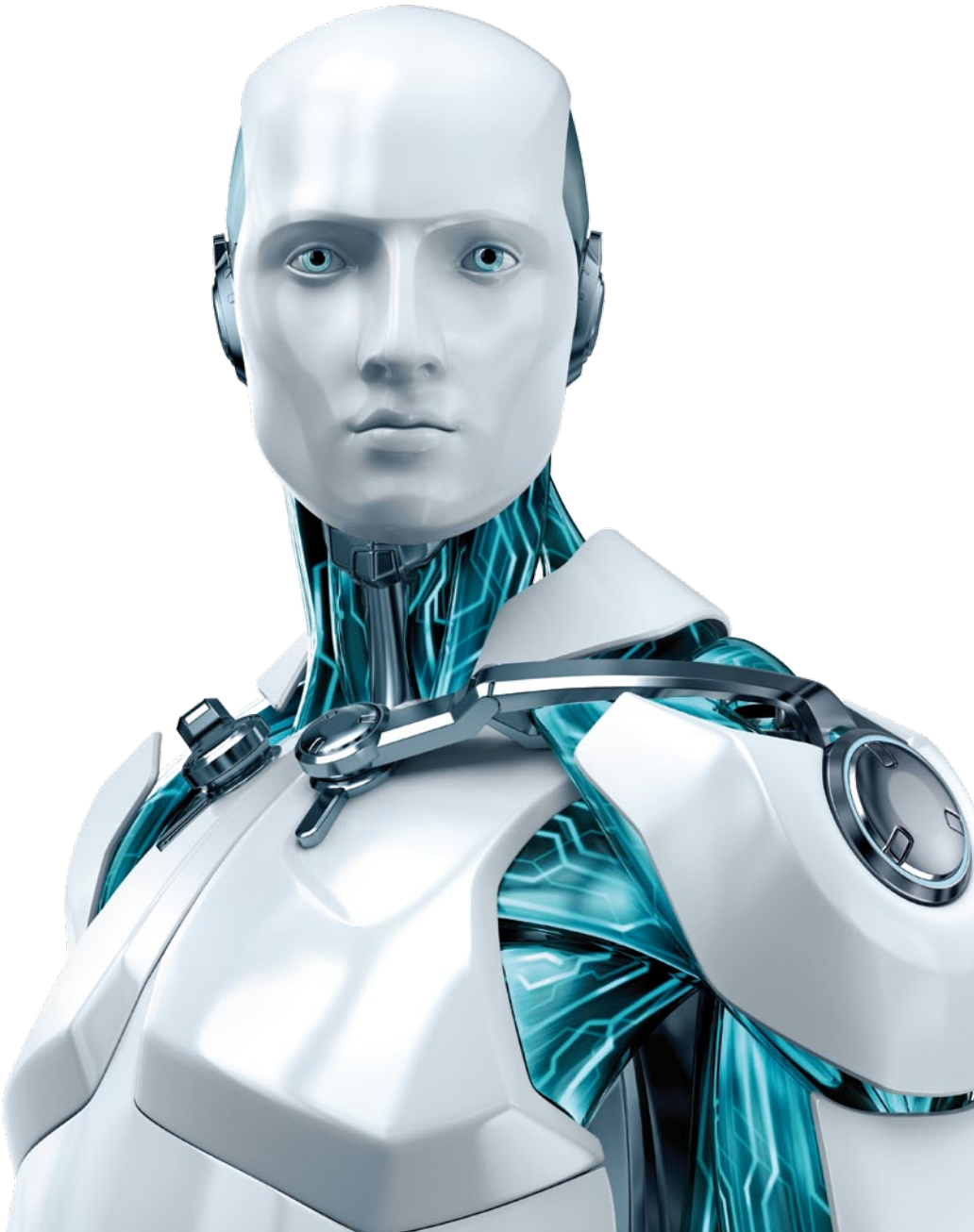


Table of contents

Introduction

In September of 2011, Microsoft released the first public preview of Windows 8, the next generation of their flagship desktop operating system, at the BUILD Developer Conference [1, 2]. Despite a flurry of pre-Microsoft leaks, interest in Windows 8 remained high, and the official release of the Windows 8 Developer Preview received a groundswell of attention in blogs, articles and elsewhere. A subsequent release, titled Consumer Preview, was released at the end of February 2012. While it contained some GUI changes, such as removal of the Start button from the taskbar, most of the changes to it were internal. Three months later, at the end of May, the Release Preview of Microsoft Windows 8 was released, with the user interface, feature set and APIs being close to (if not already) final. Much of the interest in Windows 8 focuses on cosmetic changes, such as the new modern Windows 8 interface (formerly known as the Metro user interface) and replacement of the Start Menu with the Start Screen, but substantial improvements have been made to Windows security, as well. In this white paper, we will look at some of these changes, and what they mean to Windows 8's users.

Defender of the faith

One of the most widely discussed features of Windows 8 is the inclusion of Windows Defender with the new operating system. While this is not a new tool—Windows Defender has been included with all versions of Windows since Vista was released in 2005—previous versions of Windows Defender were limited to protecting users against spyware. The version of Windows Defender included with Windows 8 is actually a rebadged version of Microsoft Security Essentials, which has led at least one prominent journalist to predict the end of antivirus software, or at least those from third parties [3]. If that refrain sounds familiar, it may be because you have heard it before: similar predictions were bandied about when it was announced that Windows Vista would include Windows Defender [4, 5, 6] and a raft of new security features, such as User Account Control [7], a Microsoft implementation of a least-privilege model for users.

Windows Defender as included with Windows 8 is a good product and does, in fact, provide a decent level of protection, especially when compared against other free anti-malware programs. However, Windows Defender does not contain many of the advanced features and functions of paid-for solutions, such as a high level of granularity for threat detection, task scheduling, centralized management and reporting and so forth. As with other free anti-malware programs, support options for Windows Defender are limited.

Many new computers purchased with Windows 8, however, will not have Windows Defender installed as their default anti-malware program. Many computer manufacturers ship their computers with a trial version of a commercial anti-malware program installed on them. This is because those manufacturers receive payments from the anti-malware vendors to pre-load the software onto the computers they sell [8]. Computer manufacturers also receive a royalty when the computer user purchases a license for the trial product, and when the license is renewed. While the amount of revenue this generates from each individual is not huge—perhaps $15-to-30 USD—when multiplied over tens or hundreds of thousands of computers, it becomes millions of dollars in revenue that computer manufacturers get from anti-malware companies. Microsoft has made it easy for computer manufacturers to disable Windows Defender so that they may continue to receive payments from anti-malware vendors in exchange for bundling their anti-malware software [9, 10, 11].

---

[1] Sinofsky, Steven. "Welcome to Windows 8 – The Developer Preview." Building Windows 8 Blog. 13 Sep. 2011. Microsoft Corp. http://blogs.msdn.com/b/b8/archive/2011/09/13/welcome-to-windows-8-the-developer-preview.aspx

[2] Goodin, Dan. "Windows 8 to ship with built-in malware protection." Windows 8: MS Gets Touchy-Feely. 14 Sep. 2011. The Register. http://www.theregister.co.uk/2011/09/14/windows_8_bundles_antivirus/

[3] Kingsley-Hughes, Adrian. "Windows 8 will ship with built-in antivirus protection." Hardware 2.0. 13 Sep. 2011. ZDNet. http://www.zdnet.com/blog/hardware/windows-8-will-ship-with-built-in-antivirus-protection/14757

[4] Fulton, Scott M. "Allchin Suggests Vista Won't Need Antivirus." 09 Nov. 2006. Betanews. http://betanews.com/2006/11/09/allchin-suggests-vista-won-t-need-antivirus/

[5] Ou, George. "What if Jim Allchin is right about no AV on Vista?" Real World IT. 14 Nov. 2006. ZDNet. http://www.zdnet.com/blog/ou/what-if-jim-allchin-is-right-about-no-av-on-vista/368

[6] Allchin, Jim. "Windows Vista: Defense in Depth." Windows Vista Team Blog. 10 Nov. 2006. Microsoft Corp. http://windowsteamblog.com/windows/archive/b/windowsvista/archive/2006/11/10/windows-vista-defense-in-depth.aspx

[7] Microsoft TechNet Library. "User Account Control – Step-by-Step Guide." Windows Vista Technical Library Roadmap. 20 Apr., 2011. Microsoft Corp. http://technet.microsoft.com/en-us/library/cc709691%28v=ws.10%29.aspx

[8] Vance, Ashlee. "For Symantec and McAfee, 'Arms Race' for Security." Business Computing. 5 Jul. 2009. The New York Times Company. https://www.nytimes.com/2009/07/06/technology/business-computing/06virus.html?_r=1&pagewanted=all

[9] Keizer, Gregg. "Windows 8's built-in AV to be security of last resort." Security News. 4 Jun. 2012. ComputerWorld. https://www.computerworld.com/s/article/9227707/Windows_8_s_built_in_AV_to_be_security_of_last_resort

[10] Bright, Peter. "Windows 8's built-in antivirus will put third-party products first." Technology Lab. 4 Jun. 2012. Ars Technica. http://arstechnica.com/information-technology/2012/06/windows-8s-built-in-antivirus-will-put-third-party-products-first/

[11] Kingsley-Hughes, Adam. "Microsoft's Compromise on Windows 8 Security Leaves Consumers Vulnerable." Forbes Tech Blog. 8 Jun. 2012. Forbes Media, LLC. http://www.forbes.com/sites/adriankingsleyhughes/2012/06/08/microsofts-compromise-on-windows-8-security-leaves-consumers-vulnerable/

One of the requirements from Microsoft for Windows 8 is that all anti-malware software should be able to cleanly install, disable and uninstall itself. In the past, switching anti-malware products under Windows has been problematic because some anti-malware solutions left files, drivers, processes, registry entries, services and other remnants on a system after they were uninstalled, which would cause various conflicts as well as compatibility and performance issues when new anti-malware software was installed. These changes for anti-malware software in Windows 8 should not only make it much easier for consumers and businesses to replace Windows Defender with other anti-malware software, but also to switch from one anti-malware program to another.

VERDICT: Windows Defender provides a good level of protection, but is mainly targeted at those who are unwilling—or unable—to purchase a commercial anti-malware solution. While any protection is better than none, and Microsoft is to be applauded for including a product of this caliber in Windows 8, Windows Defender should be thought of as the minimum bar for levels of protection and support that computer users should expect from their anti-malware software. An advantage that Windows Defender has over other free anti-malware programs is that it does not attempt to upsell the user to a paid-for product and toolbars or banner advertisements, nor does it modify existing search settings.

Giving rootkits the boot

Rootkits have been a difficult problem to deal with on Microsoft Windows for some time now because of their increasing complexity. A rootkit is a class of malware whose function is to provide unauthorized access to a system, usually with the privileges of the system's administrator. While this type of backdoor functionality is not necessarily sophisticated and, in fact, predates computer viruses, it is the methods used by rootkits to prevent detection that are problematic.

Rootkits may employ mechanisms to prevent themselves from being detected by anti-malware software using techniques collectively referred to as stealth mechanisms. Also, rootkits may actively avoid removal by anti-malware software by attempting to disable or bypass the protections of not just anti-malware software but the underlying operating system as well. In order to perform these operations, rootkits try to load as early as possible in an operating system's boot cycle.

One particularly problematic class of rootkits is the so-called *bootkit* [12, 13]. As the name implies, a bootkit takes control of a system as early as possible. It actually replaces the boot loader, the initial code used to start a computer, with a copy of itself.

Thinking outside the box to bypass bootkits

To combat rootkits and other low-level threats, ESET introduced a tool called ESET SysRescue in 2009 to create a bootable anti-malware CD or USB flash drive. This media allows you to boot a computer from a clean version of the Windows operating system, without having to worry about a rootkit (or other forms of malware) interfering with removal. Earlier this year, Microsoft introduced a similar tool called Windows Defender Offline, and other anti-malware companies have created similar tools as well.

While bootable disks are highly effective for rootkit detection and removal, they do not solve the problem of infection in the first place, nor do they provide any protection against them. They also can take some time to download and create.

To tackle bootkit infections Microsoft has incorporated changes into the boot process for Windows 8.

[12] Matrosov, Aleksandr and Rodionov, Eugene. REcon 2012. "Bootkit Threats: In Depth Reverse Engineering & Defense." 14 Jun. 2012. http://www.recon.cx/2012/schedule/events/213.en.html

[13] Matrosov, Aleksandr and Rodionov, Eugene. "The Evolution of TDL: Conquering x64." June 2011. ESET. http://www.eset.com/us/resources/white-papers/The_Evolution_of_TDL.pdf

Once a bootkit is resident and active on the computer, it can take complete control of the operating system because it runs before the operating system does, allowing it to subvert the steps an operating system—or anti-malware software—might take to verify its own integrity and secure the system.

Microsoft has been taking defensive measures against malicious code such as rootkits by securing and hardening the code of operating systems, applications and products, a process called Trustworthy Computing (TwC), which is now in its tenth year of operation [14]. Some of these changes made to operating systems to combat rootkits, however, are only available in the 64-bit editions of Microsoft Windows due to support issues: there remains a large base of 32-bit programs which rely, for compatibility reasons, on some insecure functions inherited from earlier Windows versions.

Now, 64-bit editions of Windows are nothing new: Microsoft has been shipping 64-bit editions of Windows Server operating systems for well over a decade, and the first 64-bit edition for consumers was Windows XP Professional x64 Edition [15], released in 2005. It was not until 2007, though, with the release of Windows Vista, that consumers finally began to adopt 64-bit systems en masse, and it was with the 64-bit edition of that operating system in which Microsoft began introducing additional security features.

For Windows Vista, Microsoft began to make changes to the 64-bit editions of its desktop operating systems that were not added in 32-bit editions. In addition to improvements to the core files of Windows, called the operating system's kernel files, Microsoft also made changes to how Windows Vista managed device drivers. Originally, device drivers were just small programs used for communications between the operating system and a computer's hardware, but they now are used for all sorts of low-level access, which is why they are of interest both to those who create malware, and to those who defend against it. In each subsequent version of Windows, Microsoft has continued to make changes and refinements to improve the security of the kernel, device drivers and other components that make up the operating system.

Nuts and bolts

A big change for Windows 8's security posture—and one of the most vocally debated—is the requirement for computer manufacturers to replace the BIOS firmware (software embedded on motherboards) with a new type of firmware called UEFI.

BIOS, short for Basic Input/Output System, is the name of the ad-hoc specification designed to perform some basic self-tests after a computer has been powered on, initialize the computer's hardware and then pass control to the operating system. Originally introduced for the IBM PC in 1981, the BIOS technology used by PCs has been updated numerous times since then to account for new generations of computers. Unfortunately, the basic design has many limitations, some of which directly affect a computer's security.

UEFI, the Unified Extensible Firmware Interface, is a replacement for BIOS technology. Originally called EFI and created by Intel in the mid 1990s for use with its Itanium line of processors, this technology is now managed by the UEFI Forum, a consortium of several hundred companies including Apple, Canonical (Ubuntu), Dell, Hewlett-Packard, IBM, Intel, Lenovo, Microsoft, Oracle and Red Hat [16].

[14] Microsoft. Microsoft Trustworthy Computing web site. Microsoft Corp. https://www.microsoft.com/about/twc/en/us/default.aspx

[15] Microsoft News Center. "Microsoft Raises the Speed Limit with the Availability of 64-Bit Editions of Windows Server 2003 and Windows XP Professional." 25 Apr. 2005. Microsoft Corp. http://www.microsoft.com/presspass/press/2005/apr05/04-25Winx64LaunchPR.mspx

[16] UEFI Forum. "Membership List." Unified EFI, Inc. http://www.uefi.org/join/list

Microsoft draws a line in the silicon

While UEFI is not particularly controversial, one of its features, Secure Boot, has received some criticism: Secure Boot is a feature that prevents a computer from booting into an operating system unless the boot loader code is digitally signed with a certificate derived from a key stored in the UEFI firmware. This digital signature allows the UEFI firmware to verify that the boot loader code it read from the disk into memory is from a trusted source before allowing the processor to execute it. This means the boot loader is actually the very first program to run from a disk when the computer is started.

This is an important security feature, because digital certificates are used to verify the authenticity of code, i.e., that the code is intact and unmodified. Digital certificates have been stolen and used by malware authors to sign code in the past, however, it is still quite rare for any malicious code to use a digital certificate. Blocking unsigned boot loader code basically prevents the computer from running a bootkit, immunizing it against intrusion.

What Microsoft has done is to place a requirement in the Windows 8 logo tests [17] that computers shipping with a 64-bit version of Windows 8 (which will be most desktop and notebook computers) ship with Secure Boot enabled in their UEFI firmware by the manufacturer [18]. The same requirements state that the user must be able to disable this feature, however. While computer manufacturers can ship systems that have not passed Microsoft certification, doing so prevents them from receiving marketing benefits and being able to purchase licenses at volume prices, so skipping certification is not an option for most manufacturers.

Unfortunately, this small change, intended to improve the security of computers at boot time, has received condemnation, mostly from advocates of the Linux operating system, who are afraid this requirement for digitally signed boot code will prevent them from installing Linux or other operating systems that do not contain the appropriate digital signatures in their boot code.

The UEFI specification does not actually specify whose digital keys need to be in the UEFI firmware, and in addition to Microsoft, Linux providers Red Hat [19] and Canonical (Ubuntu) [20] have come up with ways to support UEFI Secure Boot. In addition to that, the specification provides for toggling the Secure Boot mechanism [21]. If that is not enough reassurance, Microsoft has reiterated its position in its Microsoft Hardware Certification Requirements, stating that although Secure Boot must be enabled, the ability to turn it off must also be present on computers in order to pass certification.

VERDICT: While it's too soon to know the long-term effects on security of Microsoft's Secure Boot requirement, in the short term it greatly reduces the attack surface currently exploited by bootkit forms of rootkit malware on systems using BIOS-based firmware.

It is disappointing that Microsoft's efforts to repair the hole in the chain of trust of the PC boot process, which has been in existence for two decades, is being met with skepticism and outright hostility at a time when sophisticated attacks are on the increase. We hope that Microsoft and the critics of its stance on UEFI can work out their disagreements so that the security of all operating systems, not just Microsoft Windows, can be enhanced.

[17] Microsoft. "Windows Hardware Certification Requirements: Client and Server Systems." 2 Jul., 2012. Microsoft Corporation. http://download.microsoft.com/download/A/D/F/ADF5BEDE-C0FB-4CC0-A3E1-B38093F50BA1/windows8-hardware-cert-requirements-system.pdf

[18] Sinofsky, Steven. "Protecting the pre-OS environment with UEFI." Building Windows 8 Blog. 22 Sep., 2011. Microsoft Corp. https://blogs.msdn.com/b/b8/archive/2011/09/22/protecting-the-pre-os-environment-with-uefi.aspx

[19] Burke, Tim. "UEFI Secure Boot." News June 2012. 5 Jun. 2012. Red Hat. https://www.redhat.com/about/news/archive/2012/6/uefi-secure-boot

[20] Langazek, Steve; Kerr, Jeremy and Watson, Colin. "UEFI Secure boot and Ubuntu - Implementation" 22 Jun. 2012. https://lists.ubuntu.com/archives/ubuntu-devel/2012-June/035445.html

[21] UEFI Forum. Unified Extensible Firmware Interface Specification, Version 2.3.1, Errata C. 27 Jun. 2012. Unified EFI, Inc.

Sending criminals on the ELAM

Microsoft has not limited its security requirements for the boot process to requiring digitally signed boot code. Several new security functions have been added to Windows 8 and one of them, of interest both to developers and to users of anti-malware software, is the new Early Launch Anti Malware (ELAM) technology [22, 23]. As its name implies, ELAM allows anti-malware software to be the first non-Microsoft software run while the operating system is still loading. Why is this important, you might ask? ELAM is important because, like UEFI's Secure Boot, it vastly improves the security of the computer at an early stage, in this case, as the operating system has begun to load.

As mentioned in the previous section, some of the most advanced and difficult-to-remove threats facing operating systems like Microsoft Windows are programs such as bootkits, rootkits and others that use stealth mechanisms to prevent themselves from being detected both on disk and in memory. While there are various techniques for performing these actions, one thing they often have in common is the ability to start themselves early on in the boot process. This allows malicious software to take control of the computer at a point even before the operating system finishes loading, let alone security software. It is Microsoft's intent to prevent this behavior entirely by ensuring that the first non-Microsoft code run by the Windows 8 operating system is the special ELAM device driver software belonging to anti-malware software.

It is important to note that ELAM is not the same as a full-featured anti-malware program, but rather a component of such software. ELAM does not have the same features as a full suite of anti-malware software, is not able to perform the same types of actions as a security suite, and has limitations imposed on it which do not affect desktop anti-malware programs. For example, ELAM device drivers are limited to using 128MB of memory to store both its program code and data. More importantly, it has no ability to remove malware. ELAM is strictly a detection technology at this point.

What ELAM is capable of, however, is checking the operating system for malicious code before that code even has a chance to interfere with the system, since it won't be running before ELAM. Once the operating system finishes loading, the ELAM device drivers can pass control to the desktop anti-malware program and further actions such as additional scans and remediation can be taken at that point.

VERDICT: While the effectiveness of ELAM is as yet unproven, the concept behind it is fundamentally sound and it should prove to be a major deterrence to boot-time malware. The technology, however, may need to be periodically updated to overcome existing limitations and provide additional functionality. Advanced functionality for memory and disk manipulation would be useful for enhancing the detection and removal capabilities of anti-malware programs.

[22] Microsoft Dev Center - Hardware. "Early Launch Anti Malware." [paper] 9 Mar. 2012. Microsoft Corp. http://msdn.microsoft.com/en-us/library/windows/hardware/br259096.aspx

[23] Microsoft Dev Center - Software. "Early Launch Anti Malware." [web site] Microsoft Corp. http://msdn.microsoft.com/en-us/library/windows/desktop/hh848061%28v=vs.85%29.aspx

To mend and defend

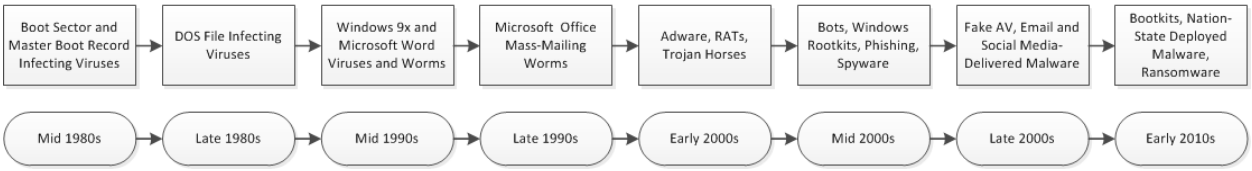
If you think of attacking the operating system as a kind of video game version of the children's game "king of the mountain," you would be right, except the victor is the first one to get his or her code to run and prevent others' code from running, as opposed to the first to make it to the top of the hill and prevent the others from displacing him or her. Microsoft has invested heavily in securing its mountain and flagship product, the Microsoft Windows operating system, by securing systems at multiple points where infection might be attempted: the preboot environment is protected by UEFI Secure Boot, the boot process by ELAM, and the operating system after it has fully loaded by Windows Defender. All of these defensive technologies are meant to protect the system, but does this mean that computers running Windows 8 will actually be completely invulnerable to any sort of attack?

After reviewing the layers of technologies used by Microsoft to protect Windows 8, it is our opinion that it is the most secure version of Microsoft Windows to date. That does not, however, mean that it is invulnerable to all threats: if there is one thing we have seen time and time again it is that those who create malware adapt it to take advantage of technologies as they come into the mainstream. First, let's take a brief look at how attacks have changed over the years.

The evolution of evil

Below is a chart showing how malware has been adapted over the years. It should be noted that the rise of one kind of threat does not necessarily mean the demise of an earlier one. For example, boot sector and file infectors both existed quite happily together in the DOS era. Also, groupings by date like this are always somewhat subjective, since the taxonomy of malware varies between companies.

TIMELINE OF MALWARE EVOLUTION



One more way to look at the history of malicious software is to observe the number of people creating it. The first destructive programs were written by individuals or small groups of like-minded people. As malware became profit motivated, these evolved into shady businesses, sophisticated gangs of organized criminals and now into highly specialized vertical markets within the criminal ecosystem. The past few years have even seen the rise of highly targeted malware deployed by nation-states for various reasons (espionage, monitoring, sabotage and so forth).

Another way to look at malicious software is by its attack patterns: in the beginning years of computer viruses, they were largely undifferentiated. The operating system was often the target, as well as the programs it ran. The release in 1995 of Windows 95 heralded the end of the DOS era of computer viruses, but gave rise to network worms. As Microsoft improved the security of Windows, attackers went after applications, using the programming languages built into Microsoft Office to create worms and other malware. As the security of Office gradually improved, attackers moved to the web and the first attempts at monetizing malware began to occur. As Internet usage grew around the globe, it became a more practical platform in its own right for criminal activity, as well, leading to web-browser based attacks. As web browsers have become more secure, attacks on other components and application frameworks such as Adobe Flash, PDF, and Oracle Java have accelerated, which is where we are today.

Attacking Windows 8

As attackers have moved up the attack chain from operating systems to business applications to web browsers to browser plugins they have also changed how they interact with computer users. Their malware may now be stealthier and less damaging than it was years ago (as befits malware whose goal is theft rather than destruction: there's rarely a profit in trashing a system). Where attackers have become far more adept is in the techniques they use to trick people into running their creations.

Attacks via social engineering have become pervasive over the past several years. These range from low-volume attacks targeting a sole individual or at best small groups of people, to widely used attacks from so-called "Fake AV" or "ransomware" programs. The former are usually silent and exist to steal corporate data, which the latter show alarming warning messages designed to trick unsophisticated computer users into purchasing a fix for a problem that does not exist or was caused by that program in the first place. Combating programs that rely on social engineering can be challenging, since they typically rely on human psychology and not purely technical methods to infect a system.

Social engineering: a hidden flaw?

As Microsoft further secures Windows and the programs that run under it, it is possible that attackers will shift increasingly to tricking computer users into running their programs, and if a person is persuaded to run a malicious program, they will generally ignore any warnings they receive from their system. While Windows 8 does contain additional warnings for users about unknown software they may be trying to run, it is unknown how users will respond to such alerts, given the amount of "alert fatigue" users currently experience from popups and warnings appearing on a daily basis. This confusion may be increased by Windows 8's Start Screen and its Modern Windows 8 (formerly known as Metro design language) apps. These are significantly different from previous versions of Windows, and this unfamiliarity may mean that users become confused as to whether the messages they see are legitimate, or social engineering attempts by criminals.

Sensory (mis)perception

Another poorly understood area of Windows 8's security is the threat potential from its use of hardware sensors [24, 25, 26]. Adding sensors in computers is not a new idea—IBM started embedding accelerometers into their ThinkPad line to detect sudden movement in 2003 [27, 28]. Windows 8, however, places a new emphasis on sensors, and computer manufacturers have been busily integrating them into their new designs.

It is inevitable that any type of technology will be open to new types of use and abuse, and it is possible that sensors (or their related subsystems) may either be attacked or used in attacks. Lest this sound too fantastical, consider the following: law enforcement regularly uses GPS positioning systems and cell phone data to track criminals and other people of interest.

---

[24] Sinofsky, Steven. "Supporting sensors in Windows 8." Building Windows 8 Blog. 24 Jan. 2012. Microsoft Corp. https://blogs.msdn.com/b/b8/archive/2012/01/24/supporting-sensors-in-windows-8.aspx

[25] Microsoft Dev Center - Hardware. "Windows Sensor and Location Platform." Microsoft Corp. http://msdn.microsoft.com/en-us/library/windows/hardware/gg463473.aspx

[26] Vembar, Deepak. "Ultrabook™ and Tablet Windows 8* Sensors Development Guide." 6 Sep. 2012. The Code Project. http://www.codeproject.com/Articles/450245/Ultrabook-and-Tablet-Windows-8-Sensors-Development

[27] Lenovo Support. "Active Protection system overview - ThinkPad General." 19 Sep. 2011. Lenovo. http://support.lenovo.com/en_US/detail.page?LegacyDocID=migr-53167

[28] ThinkWiki. "Active Protection System." 29 Nov. 2010. ThinkWiki. http://www.thinkwiki.org/wiki/Active_Protection_System

In February 2012, it was revealed that a journalist and photographer were killed by an artillery barrage, probably after their location was triangulated through their satellite phone [29]. For a more germane example, consider how many smartphone and tablet apps use location data to present advertising targeted to the device locale.

While location telemetry might be the likeliest data to be abused, it is not the only one. Data from barometers and thermometers might be spoofed to force a computer to turn itself off, or an unscrupulous manufacturer might falsify data in order to deny warranty service. The same scenarios are also possible with accelerometer, gyroscope and magnetometer sensors and their data.

Developers: the new targets of opportunity?

In addition to the use of digitally signed code for the boot loader and device drivers, Microsoft has increased its reliance on code signing for applications, as well [30]. Modern Windows 8 (formerly called Metro design) applications submitted to the Windows Store must be digitally signed, and developers of desktop applications are strongly encouraged by Microsoft to digitally sign their programs as well. Since digital certificates help to establish the provenance of a program and thus its reputation, attacks targeting digital certificates may increase.

We have already seen several attacks targeted at certificates as well as specifically at software developers:

- The Stuxnet worm has made use of digital certificates stolen from Chinese hardware manufacturers JMicron Technology Corp. and Realtek Semiconductor Corp. in order to install code onto computers it infected [31, 32, 33].
- Multiple attacks on certificate authorities, the entities which issue digital certificates, allowed hundreds of fake certificates to be generated in the names of reputable businesses and organizations. One of the certificate authorities went out of business as a result [34, 35, 36].
- The Induc virus targeted software developers and spread slowly between their computers through the programs they wrote. It may have spread for months or even years before being detected [37].

Given that the theft or forging of a single digital certificate can affect tens of millions of computers—or more—both certificate authorities and developers should regularly review and update their security procedures to ensure they do not become victims of cybercrime or unwittingly allow their customers to do so.

[29] York, Jillian C. and Timm, Trevor. "Satphones, Syria and Surveillance." 23 Feb. 2012. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2012/02/satphones-syria-and-surveillance

[30] Haber, Jeb. "Microsoft SmartScreen & Extended Validation (EV) Code Signing Certificates." 14 Aug. 2012. Microsoft Corp.https://blogs.msdn.com/b/ie/archive/2012/08/14/microsoft-smartscreen-amp-extended-validation-ev-code-signing-certificates.aspx

[31] Bureau, Pierre-Marc. "Win32/Stuxnet Signed Binaries." 9 Aug. 2010. ESET.http://blog.eset.com/2010/07/19/win32stuxnet-signed-binaries

[32] Goretsky, Aryeh. "A few facts about Win32/Stuxnet & CVE-2010-2568." 9 Aug. 2010. ESET. http://blog.eset.com/2010/07/22/a-few-facts-about-win32stuxnet-cve-2010-2568

[33] Abrams, Randy. "Why Steal Digital Certificates?" 22 Jul. 2010. ESET. http://blog.eset.com/2010/07/22/why-steal-digital-certificates

[34] Leyden, John. "Comodo-gate hacker brags about forged certificate exploit." Enterprise Security. 28 Mar. 2012. The Register. http://www.theregister.co.uk/2011/03/28/comodo_gate_hacker_breaks_cover/

[35] Harley, David. "Dead Certs." Cybercrime Corner. 15 Sep. 2012. SC Magazine. http://www.scmagazine.com/dead-certs/article/212064/

[36] Zetter, Kim. "DigiNotar Files for Bankruptcy in Wake of Devastating Hack." Threat Level. 20 Sep. 2011. Wired. http://www.wired.com/threatlevel/2011/09/diginotar-bankruptcy/

[37] Lipovsky, Robert. "The Induc Virus is back!" 14 Sep. 2012. ESET. http://blog.eset.com/2011/09/14/the-induc-virus-is-back

Summing it all up/Windows 8 by the numbers

In this white paper, we have discussed a few of the more interesting changes to Windows 8's security. It is important to note that there are hundreds of improvements, security-wise, and examining each one would be outside the scope of a short white paper.

Upgrading to Windows 8 is a no-brainer from a security perspective: doing so greatly increases your security. However, most people (or organizations, for that matter) do not rush out the day Microsoft releases a new version of Windows and immediately begin upgrading all of their computers. They look at other things, such as what software they want to run, peripherals they want to use, and even the user interface.

In the case of Windows 8, there has been a lot of backlash over the last of these—not because of any complaints about the lack of change, but rather because of the scope and nature of changes to the look-and-feel of the operating system: gone is the familiar Start Menu, a staple of the Windows user interface for nearly twenty years, to be replaced with the fingertip-friendly Start Screen. And the Windows Desktop, with its subtle Aero Glass transparencies, has been changed to a simpler look that consumes less power—a very important concern for tablets, which have energy-sucking touch screens but only limited room for batteries. While these wholesale changes are meant to usher in an entirely new generation of Windows usage and have already received some critical acclaim [38] for their design, these changes have also been met with confusion on the part of some existing Windows users [39].

ESET is neither a market analyst nor a market research firm, however, we are anti-malware researchers, and that means we do have a keen interest in the computing landscape around us, which is what makes the following two quotes from market research firm IDC so interesting. First, one discussing tablet computer shipments:

> *"Total worldwide tablet shipments for the second quarter of 2012 (2Q12) are estimated at 25 million units; up from 18.7 in the first quarter of 2012. That represents a quarter-over-quarter increase of 33.6% and a robust year-over-year growth rate of 66.2%, up from 15 million units in the second quarter of 2011."*
>
> Source: Strong Apple Shipments Drive Robust Tablet Market Growth in Second Quarter, According to IDC. Aug. 2, 2012. IDC. (emphasis ours)

Compare with the second press release, just three weeks later, on PC shipments:

> *"The worldwide PC market is now expected to grow just 0.9% in 2012, as mid-year shipments slow. [...] IDC now expects worldwide PC shipment growth will average 7.1% from 2013-2016, down from the 8.4% compound annual growth rate (CAGR) previously forecast for 2012-2016."*
>
> Source: IDC Lowers PC Outlook As Shipments Decline In Second Quarter Ahead Of Fall Product Updates. Aug. 23, 2012. IDC. (emphasis ours)

This has certainly not gone unnoticed by Microsoft, whose value was eclipsed in May 2010 by Apple [40] and its entire sales revenue overtaken by just the Apple iPhone in August 2012 [41].

---

[38] Caulfield, Brian. "Windows 8 Beta 'Reviews': A Little Weird, a Lot Good." 5 Mar. 2012. Forbes Media LLC. http://www.forbes.com/sites/briancaulfield/2012/03/05/windows-8-beta-reviews-its-a-little-weird-and-a-lot-goodwindows-8-previews-trimmed-to-what-counts-the-end/

[39] Pirillo, Chris and Pirillo, Joe. "How Real People Will Use Windows 8." 7 Mar. 2012. Lockergnome, Inc. https://www.youtube.com/watch?v=v4boTbv9_nU

[40] Helft, Miguel and Vance, Ashlee. "Apple Passes Microsoft a No. 1 in Tech." Business Day Technology. 26 May 2010. The New York Times Company. https://www.nytimes.com/2010/05/27/technology/27apple.html

[41] Worstall, Tim. "Apple's iPhone Is Now Worth More Than All of Microsoft." 19 Aug. 2012. Forbes Media LLC. http://www.forbes.com/sites/timworstall/2012/08/19/apples-iphone-is-now-worth-more-than-all-of-microsoft/

These numbers make it easy to see why Microsoft has renewed its emphasis on tablet computing. Its ability to compete in this "PC-less environment" depends on quickly adapting its strategy to embrace the heirs apparent for the PC and the server, the tablet and the cloud. Or, in other words, what Microsoft needs to do is both out-Apple Apple and out-Google Google. Accomplishing that, though, means putting a version of Windows in front of users that places tablet and cloud options first, and de-emphasizes the old Windows features. Windows 8 is a bold new reimagining of Windows, and as CEO Steve Ballmer said, it's also the riskiest strategy [42]. What remains to be seen is whether it will be a successful strategy.

The author wishes to thank his colleagues Malware Researcher Jean-Ian Boutin and Senior Research Fellow David Harley 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.

[42] McDonald, Neil and Pescatore, John. "Steve Ballmer, CEO, Microsoft, interviewed at Gartner Symposium/ITxpo Orlando 2010." 21 Oct. 2010. Gartner. https://www.youtube.com/watch?v=iI47b3a9cEI

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 contributes regularly to both the ESET Threat Blog, where he talks about the latest threats, and ESET's online support forum, where he answers questions about anti-malware 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 is recognized by tech news site Neowin as a Most Valuable Contributor. In his spare time, Aryeh enjoys scanning for viruses and backing up his data.

About ESET

ESET is a pioneer and global leader in antivirus and Internet security software. ESET business solutions offer proactive, fast and effective server-to-endpoint protection for Windows, Mac and Linux environments. To learn more about how ESET can protect your virtualized environment, go to **www.eset.com**

www.eset.com