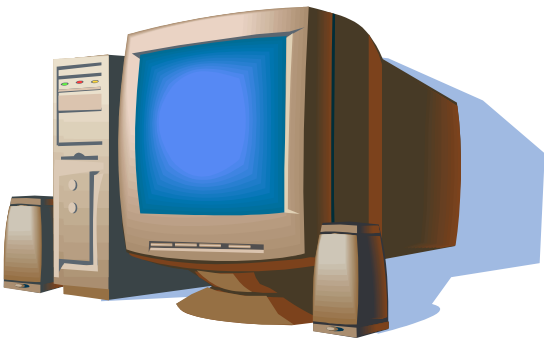
Security of the new Windows 8:

What does 8.1 fix?

Phillip Longo



Dr. Malladi

COM 405 Operating Systems

November 21, 2014

Introduction

Windows 8, the operating system that came out in 2012 as a sequel to the popular Windows 7, did not come out to the same fanfare that the seventh edition managed to garner. Designed as an operating system to help run the new Microsoft tablets and touch screen computers, it was confusing to many of the more common and less tech -savvy computer users. After years of use, many people were well acquainted with opening the start menu through the button on the bottom left corner of the screen, but when Windows 8 came out, it removed that button, forcing users to hit the start button on their keyboards instead. This caused a lot of confusion amongst new consumers and those that weren't well-adjusted to using computers. Once users found the menu, it opened up the separate menu that covered the desktop with many different colored and shaped boxes that contained Microsoft specific programs and other programs from the desktop, which only further confused new users. Perhaps the biggest problem outside of marketing issues due to the menu was that, keeping Windows 8 backwards compatible with Windows 7, malware from the old operating system could penetrate Windows 8 and effect it day one, despite the new security measures (Phneah). A year later, Microsoft released an update to Windows 8 that was intended to fix all of the problems it had, though mostly the user end issues: Windows 8.1. The update to the operating system offered a spectrum of improved security, with new ways for businesses to remain secure in the work environment, such as IT being able to lock down devices and other remote security options (Microsoft, "Windows 8.1 Security and Control"). Of course, no matter what new ways to protect your data comes up, code is volatile and people will show up to exploit it, using it for nefarious means. What problems Windows 8.1 already has and how Microsoft tries to secure them is a major part of making sure Windows stays the majorly used operating system it already is.

Background

In 2013, rumors started to float around the Internet about a Microsoft product labeled "Blue," hinting at a wave of updates directed towards the Windows 8 operating system and would lead to a continuous yearly model of updates and revisions to Microsoft software. Shortly after, a copy of the 8.1 operating system was leaked, showing numerous design changes from Windows 8. Finally, the vice president of corporate communications Frank Shaw confirmed the "Blue" project, labeling it as a way to get all devices to work together, no matter what they are doing or where they are. (Chacos) The problems began shortly after a public beta was released, where some users experienced a bug that would corrupt the Boot Configuration and cause a start up error, but this bug was later said to only effect the new Microsoft Surface RT tablet and had a 1 in 1000 chance of actually occurring. (Newman) The 8.1 operating system updating was finally released to the public on April 8, 2014, changing the minimum system requirements so that it could be installed on devices with 16GB of storage and 1GB of RAM, likely for installation purposes on tablets and other similar devices. (Fitzsimmons) In order to push the 8.1 operating system into the main stream, very shortly after releasing 8.1, Microsoft announced that after May 13, 2014 those that did not install the update would not receive any updates. (Popa) Unfortunately for Microsoft, things did not go as planned, as a bug was discovered that would make the Windows Software Update Service unable to download the update, which occurred in certain network configurations. (Bright) This forced Microsoft to push back the update deadline.

While Windows 8.1 was mostly created to change the user interface and make it more user friendly, it also provided new security features. One of these is the automatic encryption of compatible hardware that is based on BitLocker. This encryption is immediate when the user first starts using Windows 8.1, with the recovery key for the user's data stored on their Microsoft

account or though an Account Directory login. This allows the key to be acquired through any computer the user logs in from. (Cunningham) Windows 8.1 improves on the previous fingerprint recognition and allows users to authenticate themselves for login into the computer, into the user account, and into Windows applications. (Geier) It also adds an update to Windows Defender for an intrusion detection system that scans connections through the network for malware and allows third-party VPNs to trigger connections automatically. (Geier) In terms of enterprise management, it adds support for corporate networks to enroll users and their devices to have better control over access to company resources and their security requirements. This also allows the ability to wipe corporate data from the connected Windows devices remotely.

Operating System Vulnerabilities

As Windows 8.1 only fixes a couple of security problems from the previous operating system, it still has some of the issues that Windows 8 had. The biggest vulnerability that the Windows 8 has is the backwards compatibility with Windows 7. While many people clamor to be able to use their older programs on newer operating systems, it unfortunately causes most of Window's problems, as it allows the malware that affected Windows 7 to run unaltered on Windows 8. Luis Carrons is quoted as to say that "hackers typically work on malware that runs not only on Windows 8 but on previous versions of the operating system as well." When Windows 8 was first released, it quickly had new phishing attacks and fake antivirus specifically for the new operating system. Sophos, a developer of network security hardware, managed to intercept a phishing scam that said it came from the Windows 8 team, the email pretending to offer free software that would take them to a website asking for their personal information. Windows 8 also doesn't take any measures in trying to prevent social engineering. With phishing email scams constantly being sent every day, there will be some confused people that fall for it

and lose their precious and valuable information. The Windows Defender antivirus that comes with Windows 8 is a perimeter-based program, meaning it catches malware based on the digital signature of the file. In the preview release of Windows 8, vulnerabilities were found in the system and likely were still there when it officially released. (Phneah) Even the tiniest chink in the system's armor will be found by the most dedicated hackers. A French penetration-testing company called Vupen claimed to have managed to find a way past the zero-day defenses of the operating system quickly after Windows 8 was released and it is unknown if it was fixed, as neither party would release information on what was found. These are the biggest problems that Windows 8 and 8.1 have with them.

Security Solutions

Each of these problems has their own set of possible solutions though. To stop the old malware from Windows 7, a proper and updated antivirus is the best solution, as most Windows 7 malware has already been identified and set up to be quarantined out of the system. Examples of good and popular antivirus software includes Norton and Trend Micro. The best way to stop new malware however is to constantly update your antivirus when possible and be careful around suspicious emails. It might be best, when a new user sets up an email account, to have a quick one page pop-up tell users what to look out for in possibly scam emails. If Microsoft wants to take a step forward in dealing with phishing emails and social engineering attacks, they might have an email scanner that looks for patterns in the header and in the email itself that are commonly occurring in spam. This would include wrongly spelled words and odd attachments, or even scanning as to where the email is coming from, instantly sending them to a blocked folder where they can't be accidently opened and the malware can be unleashed. Of course, this would raise privacy concerns amongst some users who believe Microsoft would be invading

their personal messages. Instead of a the signature-based Windows Defender, it might be best if Microsoft changed it to a live antivirus that is constantly scanning for new malware intrusions, but this could cause the operating system to lag and slow down other processes. Unfortunately, there is no way to stop zero day attacks nor is there a way complete way to stop hackers, as the most it can do is pose a challenge, a challenge many in the cyber world would gladly take and likely surpass. There will always be those that will put personal gain or glory over the safety of others, and that is probably the most dangerous threat to Microsoft and to information safety.

Personal Analysis

In my own analysis, I believe that Windows 8.1 is probably the best operating system available if you do not care entirely about possible viruses. It is the most user friendly despite the user interface issues in Windows 8, and has the most support of outside software. Unfortunately, it is the most unsafe as it is the most targeted system on the market because it is the most common system on the market. If you are worried enough about viruses, the best operating system would likely be the Mac OS. Otherwise, Windows 8.1 is perfect for all your regular needs, as it is cheap and practically all programs you need will work on it.

Conclusion

Overall, Windows 8.1 is certainly an upgrade to Windows 8, in terms of updates to not only the user interface, but to the system's security as well. The ability to automatically encrypt and the remote access controls it gives to businesses are both appealing to organizations and users who want to protect their data. Sure, there are some problems that Windows 8.1 kept when it was updated, most of these problems can be avoided if you know how to avoid or how to protect yourself from them. Windows 8.1 is likely the best operating system currently available

on the market if you are not completely phobic of getting a virus, but with Windows 10 looming on the horizon, it may quickly be dethroned by its successor. Only time will tell if Windows 10 becomes victim to the dreaded even-numbered curse that the Internet believes plagues Microsoft or if becomes the next best thing on the market.

Works Cited

Botezatu, Loredana. "Malware Already Bypassing Windows 8 Security Mechanisms, French Pen-Tester Says." HOTforSecurity. N.p., 2 Nov. 2012. Web. 26 Nov. 2014.

Bright, Peter. "Windows 8.1 Update Halted to Some Enterprise Users amid WSUS Issues." *Ars Technica*. IDG, 9 Apr. 2014. Web. 21 Nov. 2014.

Chacos, Brad. "Is 'Windows Blue' a Set of Coordinated Updates for All Microsoft Products?" *PCWorld*. IDG, 8 Feb. 2013. Web. 21 Nov. 2014.

Cunningham, Andrew. "Windows 8.1 Includes Seamless, Automatic Disk Encryption—if Your PC Supports It." *Ars Technica*. Ars Technica, 17 Oct. 2013. Web. 26 Nov. 2014.

Geier, Eric. "Windows 8.1 Steps up Security with Biometrics, Encryption, and More." PCWorld. N.p., 16 July 2013. Web. 26 Nov. 2014.

Newman, Jared. "Microsoft Releases Fix for Surface RT Slates Borked by Windows RT 8.1 Update." *PCWorld*. IDG, 21 Oct. 2013. Web. 21 Nov. 2014.

Phneah, Ellyne. "5 Security Issues to Watch in Win 8." *ZDNet*. ZDNet, 9 Nov. 2012. Web. 21 Nov. 2014.

Popa, Bogdan. "One Day Before the Deadline, Some Users Still Can't Install Windows 8.1 Update." *Softpedia*. SoftNews, 12 Mar. 2014. Web. 21 Nov. 2014.

"What's New in Windows 8.1." *What's New in Windows 8.1*. Microsoft, n.d. Web. 26 Nov. 2014.

"Windows 8.1 Security and Control." *Windows 8.1 Security*. Microsoft, n.d. Web. 21 Nov. 2014.