Windows XP's End of Life

Understanding the Risks and Impact to Point-of-Sale and Automated Teller Machines

Introduction

An era is passing. The venerable workhorse of personal computer operating systems Windows XP was removed from Microsoft's list of supported operating systems on 8 April 2014. Announced in 2007, this end of support means Microsoft will no longer release any XP software updates, automatic fixes or service packs. Support for Windows XP Embedded systems expires on 12 January 2016.[1] However, Microsoft reconfirmed they will continue to update the anti-malware engine and signatures through 14 July 2015.

Introduced in 2001, XP was the most widely used operating system up until August 2012, when it was surpassed by Windows 7. As of February 2014, Windows XP still resides on roughly 30% of personal computers worldwide.

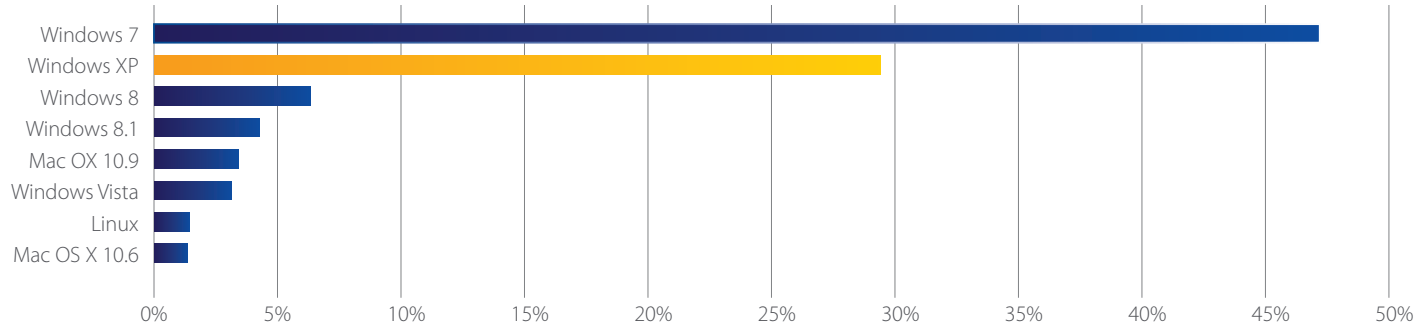
[1] Microsoft Embedded Product Lifecycles & Support

OVER
95%
of the world's ATMs are running on Windows XP
Source: NRC

Today, many Point-of-Sale (POS) payment applications were programmed to reside on personal computers running XP. Windows XP is already a highly vulnerable platform based on its longevity and its overall architecture. Modern operating systems like Windows 7 and 8 have more sophisticated security features built in, making them less of a target to hackers, who would rather exploit vulnerabilities in older unpatched systems versus expending time and energy developing exploits only to have them undone by a monthly security patch. Anyone using Windows XP, whether it is for personal computing or business operations, should be planning now to upgrade to a newer and more secure operating system.

Additionally, the retirement of XP will impact another business sector – Automated Teller Machines (ATM) owners and deployers. According to NCR, the largest ATM supplier in the U.S., over 95 percent of the world's ATMs are running on XP. Migration or upgrading to newer operating systems and hardware has been slow in the ATM industry, leaving thousands of machines to run on the outdated software.

Desktop Operating System Market Share



Desktop OS Market Share as of February 2014 according to Net Applications.

Merchant Point-of-Sale (POS) and Automated Teller Machine (ATM) Impact

For all the merchants and ATM deployers currently using a POS/ATM system on XP, this presents a serious threat to their overall security posture and their Payment Card Industry (PCI) Data Security Standard (DSS) compliance. Merchants and ATM deployers choosing to continue to run XP after support ends will still have functioning computers, POS systems and ATMs, but according to Microsoft, will be five times more vulnerable to security risks such as viruses and malware.

In 2013, the security firm Verizon, reported that 75% of the breaches they surveyed were "opportunistic attacks." An opportunistic attack occurs when a victim is not specifically chosen as a target; they are identified and attacked because they exhibit a weakness the attacker knows how to exploit. Verizon also noted that hackers are not using sophisticated attacks to compromise entities with three-quarters of breaches caused by low or very low difficulty attack vectors. "When you consider the methods used by attackers to gain a foothold in organizations – brute force, stolen cred[entials], phishing, tampering – it's not all that surprising that none receive the highly difficult rating. Would you fire a guided missile at an unlocked screen door?"[2] Having an unpatched application or operating system is like an unlocked screen door and securing that door becomes crucial to maintaining any entity's security.

The Consortium for Cybersecurity Action's (CCA) 20 Critical Security Controls is mapped to the top hacker threats. The fourth control listed, which addresses patching, "Continuous Vulnerability Assessment and Remediation: Automated vulnerability scanning, port checking, and patch management solutions" is mapped to eight of the top 10 threat actions. Furthermore, as more software and hardware manufacturers continue to optimize for newer versions of Windows, many programs and POS/ATM devices will no longer be compatible with XP. Conversely, current applications coded to XP will also be outdated and likely not supported by the vendor anymore leading to additional unaddressed vulnerabilities.

[2] Verizon 2013 Data Breach Investigations Report (DBIR)

Unpatched Systems and PCI DSS Compliance

The PCI Security Standards Council (SSC) addresses the issue of non-supported operating systems in their Frequently Asked Questions.

"PCI DSS Requirements 6.1 and 6.2 address the need to keep systems up to date with vendor-supplied security patches in order to protect systems from known vulnerabilities. Where operating systems are no longer supported by the vendor, OEM or developer, security patches might not be available to protect the systems from known exploits, and these requirements would not be able to be met."[3]

While the SSC admits it may be possible to implement compensating controls to meet the intent of the requirements, these compensating controls must protect the system from all unsupported code vulnerabilities - a nearly impossible feat, even for the most advanced security software. Furthermore, the use of compensating controls should be considered only a temporary solution, meaning merchants and ATM operators should have an active migration plan to upgrade to a supported operating system.

Challenges and Threats

Although Microsoft has announced that it will continue to provide anti-malware support for Windows XP until July 2015, the root causes of malware infection are no longer going to be addressed once the support date passes. Microsoft will release "signatures" to identify some common forms of malware for Windows XP, but will not protect against the root causes of malware infection itself.

Merchants and ATM operators should have an active migration plan to upgrade to a supported operating system

Security holes characterized by Microsoft as both **important**, "A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of user data…" or **critical**, "A vulnerability whose exploitation could allow code execution without user interaction…or unavoidable common use scenarios where code execution occurs without warnings or prompts", will quickly begin to accumulate, leaving XP users with little awareness of exactly how they are exposed. It is safe to assume that exposure to multiple security vulnerabilities will quickly reach a tipping point in which Windows XP can no longer be trusted to protect sensitive applications and data.

Using the last batch of critical security updates (from 12 March 2013) as a measure of the type and severity of security exposure, it's not hard to imagine the scope of attack vectors expanding dramatically soon after support ends. Typically, once criminals identify a Windows vulnerability, they attempt to develop exploit code allowing them to gain a foothold on systems that don't have the security fix installed. **After 8 April 2014, that's all Windows XP systems.**

If even one of the several critical vulnerabilities affecting Windows XP in the last Microsoft security update were left un-patched, it could spell big trouble:

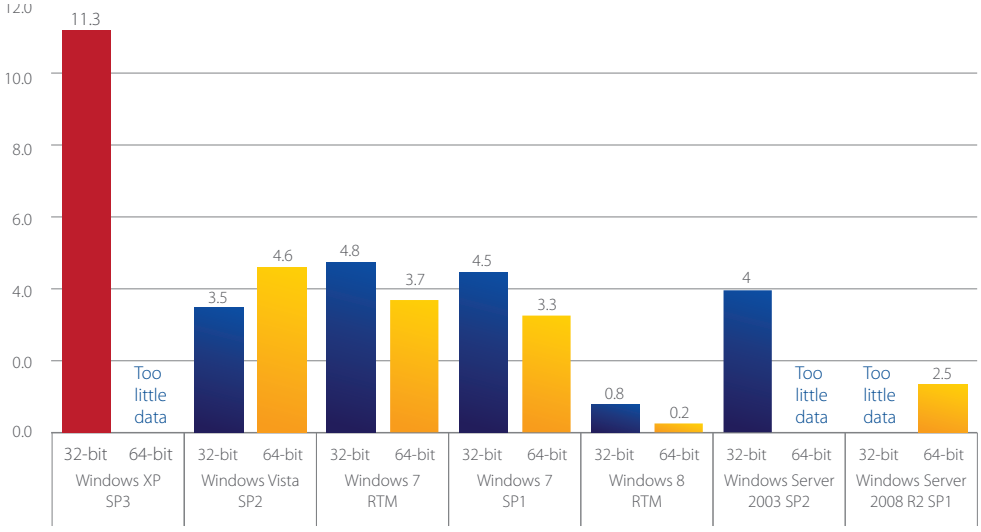
- **Cumulative Security Update for Internet Explorer (2809289):** The most severe vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Internet Explorer.
- **Vulnerability in Silverlight Could Allow Remote Code Execution (2814124):** The vulnerability could allow remote code execution if an attacker hosts a website that contains a specially crafted Silverlight application that could exploit this vulnerability and then convinces a user to view the website.
- **Vulnerabilities in SharePoint Could Allow Elevation of Privilege (2780176):** The most severe vulnerabilities could allow elevation of privilege if a user clicks a specially crafted URL that takes the user to a targeted SharePoint site.

[3] PCI SSC Knowledge Base, Article Number 1130, 6/27/13

Maintaining Trust in Payment Applications

The risk of running a payment application atop an unsupported, vulnerable operating system cannot be overstated. For merchants especially, the operating system is a critical layer of security which essentially moves into the untrusted column, taking payment applications with it. Attackers have already overcome Windows XP's built in security mitigation controls and are now poised to target payment applications with accelerated interest. According to Microsoft's own analysis, malware infection rates for Windows XP are vastly higher than operating systems like Windows 7 and Windows 8.

Malware Infection Rates for Windows



Malware Infection rate by operating system and service pack in the fourth quarter of 2012, reported by Microsoft Security Intelligence Report volume 14

Maintaining trust in the payment application will involve making some difficult choices and taking quick action.

- **Consult with your sponsoring bank or payment processor on whether your payment application is supported by Windows 7 or 8.** Keep in mind, upgrading from XP may involve more than just updating the operating system. Most hardware that is currently running XP may not have the processing speed and memory to run more advanced operating systems. A move to migrate to Windows 7 or 8 may involve upgrading the hardware running it as well.
- **Completely disallow Internet web browsing on Point of Sale systems running Windows XP.** Many of the most damaging attacks are the result of Internet browsing activity. To reduce the risk of malicious software infection, disallow Internet browsing from POS systems or any other non-payment related functions like email. POS systems should be single-purpose, meaning all other applications and functionality that is not part of payment processing should be disallowed or removed.
- **Add file integrity monitoring to the POS or ATM as a preventative measure.** Already part of PCI-DSS requirements, file-integrity monitoring or change-detection systems check for changes to critical files, and notify when such changes are noted. This is one of the best detection methods for payment card-stealing malware.
- **Take a touch-once approach when upgrading ATM and POS systems.** When migrating to supported operating systems also consider implementing EMV Chip card acceptance. For more information on EMV Chip refer to the Visa EMV roadmap

Conclusion

Many people like to take a "if it's not broken, why fix it" attitude to business operations. Changing from one operating system may seem costly and painful but the alternative will be worse. Take action now to prevent hackers from targeting you and your business as a data breach candidate. Invest now in securing your payment processing environment and you can then concentrate on building your business for the future.

VISA