The Ongoing Legacy of Windows XP

CUK-17.03.16 CD **21.03.2016**

Introduction

2016 may not seem like the optimal time to write about Windows XP Operating System (OS), given that four major releases of Windows have now superseded it. Many will have consigned it to the Recycle Bin of history and long forgotten the *Bliss*[1] of booting it up, but for some, moving on is difficult! This report provides a quick primer on the current place of XP in the OS market, the resultant risks and some advice on mitigation of the risk of still running it. CERT-UK is keen to hear from the CiSP membership about your current experience with running Windows XP systems in 2016, if/how you have mitigated the risks and how big an issue you think this is across your industry.

How pervasive is Windows XP in 2016?

Windows XP, which was initially released in late 2001, finally went out of support in April 2014. This meant that Microsoft stopped providing all forms of security patching and updates for the OS. In the 13 years between release and end-of-support, Windows XP had become hugely dominant in terms of OS market share across personal and business users. In spite of the successive releases of other Windows OSs (Vista in early 2007, Windows 7 in late 2009 and Windows 8 in October 2012), XP maintained a significant user base.

Even in 2016, as we move into the era of Windows 10, XP has not gone away. Whilst exact usage numbers are difficult to determine, estimates of market share range from 3-5%[2] up to 11%[3]. From here, some 'back-of-the-napkin' calculations are required. Considering:

- Windows 10 sits somewhere around 15% overall market share
- Windows as a platform holds somewhere around 90% market share
- Microsoft stated in January 2016 that Windows 10 is now active on 200 million devices[4]

This means that a very rough estimate is 1.5 billion overall devices running Windows, with XP still running on up to 130 million devices.[5] The enduring popularity of Windows XP is further illustrated by the fact that an unofficial service pack was developed following the end of Microsoft support.[6]

It is probably not surprising that industry users lag behind personal users in updating to newer version of Windows, in particular industries which tend to operate equipment with a long cycle of deployment before replacement. ATMs are a notable example, with a significant number of UK ATMs still running Windows XP. Microsoft did provide a special extended support period for the embedded version of XP used in ATMs. However, that extended period ran out in January 2016.[7] Many large corporates,

[1] *Bliss* was the official name given to the standard Windows XP desktop background photo of verdant green fields under an azure sky.
[2] http://gs.statcounter.com/#desktop-os-GB-monthly-201506-201601
[3] http://www.netmarketshare.com/report.aspx?qprid=11&qpaf=&qpcustom=Windows+XP&qpcustomb=0
[4] https://blogs.windows.com/windowsexperience/2016/01/04/windows-10-now-active-on-over-200-million-devices/
[5] Microsoft themselves stated that there were 1.5 billion devices running Windows in 2014 (see, for example, http://www.neowin.net/news/microsoft-we-have-15-billion-windows-devices-in-the-market), so the numbers calculated here may be an under-representation for 2016. There is also a likely 'dark figure' of systems running unlicensed copies of Windows.
[6] http://www.theinquirer.net/inquirer/news/2362314/windows-xp-gets-an-unofficial-service-pack-4
[7] http://www.theregister.co.uk/2015/12/08/xp_embedded_atm_security_cutoff_panic/

who have otherwise upgraded to later versions of Windows, also have a small number of XP systems running some legacy applications within their estate.

The Risk of Running Windows XP

The implications of still running XP are simple – systems are less secure, and more vulnerable to cyber-attack. There are many known vulnerabilities which affect the OS[8] which are not being patched, and there are recent reports of disruption caused by viruses and malware exploiting vulnerabilities in XP.[9] XP is not receiving any more updates, and Microsoft has even stopped providing malware signatures for the XP version of its Security Essentials product, though third party anti-virus and anti-malware tools continue to provide support (anti-virus and anti-malware should not be thought of as a way to entirely mitigate the lack of updates and patches however).

Ultimately, the reality of the risk involved in running XP will differ on a case by case basis. Consider questions such as "*does the XP system carry out some function which is business critical?*", "*does the XP system process or access information which requires high confidentiality, high integrity or high availability?*" and "*is the XP system connected to the company network?*" The more often you respond with a "yes", the greater the risk arising from use of Windows XP.

Remedial Actions

So what should you do if you are still among those using XP? The best answer is the shortest one – *upgrade!* If the main reason that you are still running XP is due to the cost or complexity of upgrading, or just inertia, you should consider the risk of potential financial loss or business interruption that could arise from a cyber-attack or data breach. Upgrading from Windows XP is highly recommended unless it is strictly necessary for your business – and if this is the case, the risk of doing so should be understood, documented, and otherwise mitigated as far as possible.

If you absolutely must run XP to operate some legacy software or process, consider the following:

- Contact your software vendors to discuss the situation. There may be some workable alternative that does not require running XP. Changing a software solution, as complex a process as it may be, can remove the requirement and associated risk of using XP.
- If the XP system is being used only to run a specific application or set of applications, consider application whitelisting which will prevent any processes outside of an authorised baseline to run. Allow only the absolutely critical applications and processes to run.
- If possible, run the XP system offline, or else strictly isolate it on the network.
- Limit access as strictly as possible. If the system requires infrequent administration or human interaction, you could completely remove the monitor and any I/O devices to reduce the chance of unauthorised activity.
- Remove the internet browser, or if for some reason a browser is strictly necessary, run a supported browser - Firefox and Google Chrome still support Windows XP (with Service Pack 2) for now, though Chrome support will end in April 2016. Also consider browser extensions to disable certain types of content such as JavaScript.

[8] https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-739/Microsoft-Windows-Xp.html

[9] See, for a recent example, http://www.itnews.com.au/news/how-the-qbot-malware-downed-melbourne-healths-systems-414041