POLITICO

Microsoft XP's massive cybersecurity problem

By: Shaun Waterman
April 7, 2014 08:00 PM EDT

http://www.politico.com/story/2014/04/microsoft-xp-cybersecurity-problem-105451.html?hp=f1

Microsoft will cut off support to its 12-year-old operating system Windows XP at about 1 p.m. Eastern time on Tuesday, leaving more than a quarter of the world's computers effectively undefended against hackers and cybercriminals.

And because outdated software renders the computers that run it vulnerable to malicious programs deployed by hackers, that's bad news for everyone in today's ultra-connected world.

Security experts liken the estimated 500 million computers still running the antiquated XP program to a group of unvaccinated children: Their vulnerability to infection puts at risk the health of the whole population.

"It's a matter of herd immunity," said Gary McGraw, chief technology officer of Virginia-based software security firm Cigital, "If there's a group using old, outdated, unpatched software, it makes us all collectively more vulnerable."

For users at home, the risks are bad enough: Outdated software means their computers can be infected to send cybercrooks password and login information for their bank or online shopping accounts. But for companies, a single unpatched machine is a back door hackers can use to get around expensive security measures and take over an entire network.

Microsoft says the software has long passed its use-by date and wants customers to upgrade by buying a more recent — and more secure — operating system, like Windows 7 or 8.

The Microsoft cutoff should come as no surprise to anyone still using XP: Since September 2007, the company has been warning customers about its plans to discontinue support. Nevertheless, misplaced frugality, ignorance about the change or just inertia mean that XP remains the second-most widely used personal computer operating system on the planet.

In part, that's because Microsoft dominates the the operating system market — more than 90 percent of computers run their products — but its also because the operating system the company originally rolled out to replace XP, Windows Vista, was widely acknowledged to be a disaster.

In China, just over half of all computers use XP, and even in the United States, nearly 1 in 5 computers owned by consumers and businesses are still running it, according to Jenni Cullen of StatCounter, a Dublin-based Web analytics firm that tracks operating system usage.

Indeed, StatCounter's figures suggest that consumers might have been quicker to switch out XP than businesses. "It appears that XP usage peaks Monday-Friday and falls off at the weekend," Cullen said in an email, "This possibly indicates that home users have been quicker than businesses to ditch XP."

McGraw says that many businesses will be "caught with their pants down" by the cutoff.

"Microsoft has been warning for six years about this," he said. "Smart organizations have dealt with it already."

"You can't just install a system and leave it for 10 years," he said. "You have to factor in upgrade costs to your IT budget," and those companies that didn't will find themselves "with a massive technical debt coming due" on Tuesday.

"Patch Tuesday," the second Tuesday of each month, is when Microsoft publishes its regular package of updates and security fixes for its whole family of software products — including the various versions of Windows, Office and Outlook.

The collection made available for download Tuesday includes the final updates for XP, which first went on sale in October 2001.

The software patches are needed to fix flaws in the code discovered by hackers or their "white hat" equivalents who help Microsoft discover security flaws.

"Newer platforms are way more secure," McGraw said. Older systems like XP are like "an inner-tube with 8000 patches on it … it's mostly patch and not much tube at this point."

But from now on, the Redmond, Wash.-based software giant will no

longer be fixing flaws found in XP. A growing number of unpatched vulnerabilities will begin to plague the program, exposing it to infection from specially written malicious software code called malware.

Worse still, XP shares much of its code with its successor programs, Windows 7 and Windows 8. So, whenever Microsoft publishes a fix for a vulnerability in one of those two operating systems, hackers will be able to reverse engineer the patch, uncover the vulnerability it was meant to fix and write malware that can exploit it in unpatched XP systems.

Malware surreptitiously takes over a computer, either to steal a user's login and password for bank or other financial services sites, or to recruit the computer to a botnet — giant networks of tens of thousands of compromised machines that are used to send spam and launch internet attacks.

Botnets and other malware-infected computers have been compared to the broken windows and trash-strewn corners of the offline world. Sociologists found during the 1980s that such apparently minor issues were in fact major contributors to the crime rate in high-crime neighborhoods — fix the broken windows, catch the kids jumping subway turnstiles, and authorities can make big inroads against crime.

So it is online, say security experts. "Botnets are major enablers of cybercrime," said one U.S. cybersecurity official, not authorized to speak on the record.

The official added that the results of continued use of unsupported XP systems are predictable, and can easily be discerned by looking at what happens to computers running pirated versions of Microsoft operating systems, which cannot be patched.

"The botnets of the world are populated by PCs running unpatched [operating systems]," the official added.

Microsoft declined to make anyone available for interview, but said in a statement the company was "focused on ensuring that customers are aware that support for Windows XP is ending April 8, and that they migrate from Windows XP to a modern operating system such as Windows 8.1 as soon as possible to ensure that they have the latest security, mobility and productivity tools."