Will XP Be Attacked in April 2014?

by Sharon D. Nelson, Esq. and John W. Simek

© 2014 Sensei Enterprises, Inc.

Unless you've been hibernating, you know that support for Windows XP SP3 will end on April 8, 2014. This means that Microsoft will not be providing any security updates after that date. Should you care and quickly run out and purchase an upgraded operating system? Many critics are claiming that Microsoft is stopping support in order to increase sales of the more current operating system software. Others are predicting that the sky will fall as hackers are just waiting to release their latest malware right after April 8th. We believe that there will be attempts to compromise Windows XP systems, but it is hard to believe that there will be a massive attack on April 9th. Sometime in the future, yes. Immediately, probably not.

Why all this hoopla over replacing Windows XP? Many systems are currently running XP and you probably don't even realize it. The majority of airport scheduling systems run XP to drive the monitors displaying departure times, gate assignments, etc. for the thousands of flights that occur every day. Imagine the impact if airport flight displays suddenly go dark. A bigger risk exists in the banking industry. Most ATMs run XP as the operating system. A compromise of an ATM could cause a huge amount of financial damage, especially if the exploit was spread across the entire ATM network.

Why should you care as a lawyer? Well, there's an ethical duty for lawyers to protect the confidentiality of their clients' information. Without the continuing security updates, your computer system could be compromised by the bad guys, putting your client's data at risk. As a result, some bars may determine that you are subject to disciplinary action for failure to reasonably protect client data if you continue to use Windows XP after April 8th.

Failure to comply with a lawyer's ethical duties isn't the only potential gotcha. Many law firms use their computers to process credit card payments from their clients. If the computer is running Windows XP, there is a possibility that it will be infected with malware after the XP end-of-life date. The malware could intercept the credit card payment information. This means you have to deal with possible fines for violating the requirements of PCI DSS (Payment Card Industry Data Security Standards), state data breach laws and a public relations disaster if you have a data breach. In short, it wouldn't be a very good day. It will be even worse if you use QuickBooks on the same compromised machine. That would put all of your financial data at risk, including any trust account information. Your first bounced check would be an unwelcome clue that a hacker had just siphoned money out of your bank account following a successful attack on your XP-based computer.

So what are you waiting for? Run, don't walk and replace that soon-to-be-malware-magnet XP machine. Unfortunately, there is no direct upgrade option from XP to one of the modern operating system. You'll have to transfer your data manually and potentially upgrade some of your application software. No matter what, ditch that XP computer and keep those security updates coming.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com .