SIM2K
Adapting Technology to Your Business Needs

6•16
Information you can use

SIMformation

Does Windows 10 Upgrade Go too Far?

In the attempt to move the world to Windows 10, Microsoft is now using what some have called "heavy-handed tactics" to force people into the upgrade. The "Get Windows 10" pop-up that users of Windows 7 or 8.1 are seeing recently received an overhaul that seems designed to confuse users who have been exposed to this pop-up for a year now.

SIM2K has had users running a Windows 7 PC being upgraded to Windows 10 without their knowledge. The process can kick off automatically even if you don't touch a thing on your computer. In late 2015, the "Get Windows 10" (GWX) pop-up changed its message to say "Upgrade Now" or "Start download, upgrade later." The only way to decline the upgrade was by clicking the **X** button in the GWX pop-up's right-hand corner and closing the window.

Earlier this year, however, Microsoft pushed the Windows 10 download out as a "Recommended Update." That means anybody using the default Windows Update setting automatically received the installation files and a prompt to install the new OS, which again could only be refused by exiting via the **X** in the corner of the pop-up's window.

In late May Microsoft altered the GWX prompt. On the surface, it's an improvement; the box clearly states when your PC will be upgraded, and even adds a (still small and easily skippable) line that allows you to reschedule or change the upgrade timing. But here's the catch: The redesigned GWX pop-up now treats exiting the window as consent for the Windows 10 upgrade.

So after more than half a year of teaching people that the only way to say "no thanks" to Windows 10 is to exit the GWX application – and refusing to allow users to disable the pop-up in any obvious manner – Microsoft made it happen that this action now *accepts* the Windows 10 upgrade rather than canceling it.

And if you don't find that small link to reschedule or cancel the Windows 10 upgrade – or, say, if the pop-up appears while you're away from your computer – your system will automatically begin the process at the scheduled time. In other words, your PC can potentially upgrade to Windows 10 without you asking it to *or* explicitly approving the upgrade.

Windows 7 and 8 users have seen and declined the Windows 10 update numerous times. By forcing out Windows 10 as a Recommended Update and changing the behavior associated with exiting the GWX pop-up, Microsoft is actively striving to push the operating system on people who are not ready for the upgrade or don't want it.

In fact, this month, a petition was launched asking the Electronic Frontier Foundation (EFF) to investigate Microsoft's "aggressive" tactics to get users to upgrade to Windows 10. "Microsoft's practices with their newest operating system, named Windows 10, has been ignorantly unethical at best and malicious at worst," wrote the petition organizer, who listed media accounts of the company's upgrade strategy. "Reports everywhere state that people are being tricked or *forced* into upgrading to Windows 10 from their current, preferred version of Windows." [*Emphasis in original*.]

SIM2K wants all users to be aware of this tactic and to not fall into an unplanned upgrade. We have ways to block this download and subsequent call for installation, which we have performed for many clients. While we support upgrading to Windows 10, it still remains an option, not a requirement. If you have not tested a Windows 10 PC on your network with all your business software, we continue to recommend this as the first step rather than just leaping into upgrades.

Many clients are purchasing new PCs with Windows 10, so if tested, adding these to your network is not an issue. However, Windows 7 is still a viable, stable platform so there is no need to upgrade in you do not have to, which at this time is the case other than Microsoft's urging users to make the switch. And if you have not tested Windows 10, having a machine suddenly "update itself" might be problematic, so we wanted you to be aware of this change in Microsoft's notice. If you have questions on either upgrading or blocking the Windows 10 installation, please contact us.

Malware Evades Microsoft Tool

Hackers have launched large-scale attacks that are capable of bypassing the security protections added by Microsoft's Enhanced Mitigation Experience Toolkit (EMET), a tool whose goal is to stop software exploits.

Security researchers from FireEye have observed Silverlight and Flash Player exploits designed to evade EMET mitigations such as Data Execution Prevention (DEP), Export Address Table Access Filtering (EAF) and Export Address Table Access Filtering Plus (EAF+). The exploits have been recently added to the Angler exploit kit.

Angler is one of the most widely used attack tools used by cybercriminals to launch Web-based, "drive-by" download attacks. It is capable of installing malware by exploiting vulnerabilities in users' browsers or browser plug-ins when they visit compromised websites or view maliciously crafted ads.

First released in 2009, EMET can enforce modern exploit mitigation mechanisms for third-party applications – especially legacy ones – that were built without them. This makes it much harder for attackers to exploit vulnerabilities in those programs in order to compromise computers.

While EMET is often recommended as a defense layer for zero-day exploits – exploits for previously unknown vulnerabilities – it also gives companies some leeway when it comes to how fast they patch known flaws.

With widespread exploits now able to evade EMET mitigations, the tool should no longer be relied on to protect old versions of applications like Flash Player, Adobe Reader, Silverlight or Java until a company can update them.

Unfortunately, organizations are sometimes forced to keep old versions of browser plug-ins and other applications installed on endpoint computers in order to maintain compatibility with custom-made internal Web applications that haven't been rewritten in years.

"Applications such as Adobe Flash, web browsers, and Oracle Java should be patched routinely, prioritizing critical patches, or removed if possible," the FireEye researchers said. "Because the Web browser plays an important role in the infection process, disabling browser plugins for Flash or Silverlight may also reduce the browser attack surface." Contact SIM2K for more information on browser safety and anti-malware measures.

More Chromebooks Sold

More personal computers powered by Google's Chrome OS shipped in the US during the first quarter than those running Apple's OS X in the same period, according to research company IDC.

"Chrome PCs overall, including Chrome desktop units like the Chromebox, out-shipped all Apple personal computers, desktop plus notebook, in the US for Q1," said an IDC analyst who tracks device shipments.

Chromebooks, the inexpensive notebooks that run Chrome OS, also out-shipped Apple's MacBook, MacBook Air and MacBook Pro notebooks in the U.S. The first-quarter battle wasn't even close, according to the notebook-only shipment numbers IDC released.

Apple shipped an estimated 1.17 million Mac notebooks in the US during the first three months of 2016; IDC said 1.6 million Chrome OS notebooks shipped in the same span. In other words, 37% more Chromebooks shipped than Mac notebooks.

IDC's shipment data for Chrome OS and OS X systems were estimates generated using information from vendors and Asian component suppliers. Google, which developed Chrome OS, does not reveal shipment numbers: Most Chromebooks originate from third-party OEMs (original equipment manufacturers), including Acer, Asus, Dell, Hewlett-Packard and Lenovo. And although Apple disclosed global Mac sales in its April 26 earnings call with Wall Street, it did not break down that figure by geographic region.

Chromebooks have sold primarily to educational organizations, particularly K-12 schools, because of their low price and easy manageability. "People buy Chromebooks because they're looking for the cheapest device," said an independent analyst who characterized schools as "price sensitive" to explain their leaning toward Chromebooks.

Meanwhile, Mac sales contracted by 12% in the first quarter when compared to the same period in 2015, the second largest decline in nine years. The Mac average selling price in the first quarter was $1,266, or four times as much as the average price of 30 different Chrome OS personal computers that Google lists on its website.

While Apple first made inroads in schools with the Apple II, it appears that their day of dominance may be over as schools and other users have turned to Chromebooks and access to the Google suite of products. SIM2K does support Chromebooks and can help you with evaluating the various models if you are interested.

Congress Nixes Yahoo Mail

The IT department of the U.S. House of Representatives has blocked access to Yahoo Mail and the Google App Engine platform due to malware threats.

On April 30, the House's Technology Service Desk informed users about an increase in ransomware-related emails on third-party email services like Yahoo Mail and Gmail.

"The House Information Security Office is taking a number of steps to address this specific attack," the Technology Service Desk said. "As part of that effort, we will be blocking access to Yahoo Mail on the House Network until further notice."

"The recent attacks have focused on using .js files attached as ZIP files to e-mail that appear to come from known senders," the House's Technology Service Desk said. "The primary focus appears to be through Yahoo Mail at this time."

The increase in ZIP and RAR attachments that contain malicious JavaScript (JS) files has been observed by multiple security companies in recent months. Microsoft has offered recommendations such as using the Windows AppLocker group policy to restrict .js files but there is no indication the House has instituted these recommendations.

The House Information Security Office also banned access to appspot.com, the domain name used by applications hosted on the Google App Engine platform. This ban appears to be unrelated to the ransomware attacks and is in response to indicators that attackers have been using Google's platform to host a remote access trojan named BLT since June 2015, according to unnamed congressional sources.

Banning an entire service because some cybercriminals abuse it seems like overkill, especially when this can cause downtime to legitimate applications. Dropbox, Blogger, Google Docs and many other free services are routinely abused by cybercriminals to host malware. Banning them all, instead of specific malicious URLs, would likely be impractical.

However, this points out that the spread of ransomware has impacted our government, just like SIM2K has warned our clients. Ransomware has become the new "public enemy #1" for the IT field, which is why we have encouraged clients to take steps now as it continues to be a "not if, but when" situation that a ransomware infection will sneak into your company. We have covered Ransomware in several issues of SIMformation as well as in blast e-mail messages to our clients, outlining our stance here and how we can help you mitigate any potential infection. If Congress is taking drastic steps like this, please contact SIM2K and let us help you with defenses, too.

"Random Tid-Bytes"

Edge not ... Edgy for Internet Users

Microsoft's Edge browser has slipped to its smallest-ever percentage of Windows 10 in the US, according to data from a consortium of government websites. Edge, the default browser in Windows 10, was used by 22.1% of those running the new operating system in April, data from the Digital Analytics Program (DAP) showed. DAP's April measurement of Edge's portion of Windows 10 was the smallest since the operating system's release in July 2015, falling below the former low-end mark of 22.4% set in November. Worldwide, Edge was also off earlier numbers. US-based Net Applications, for example, which measures user share, tapped Edge's global share of Windows 10 at 30.6%, flat for the third month in a row but lower than 2015's numbers, which ranged from 36% (in September) to 31% (in November). And StatCounter's global usage share for Edge as a fraction of Windows 10 was 12.7% in April, a new low.

Laplets Taking Over

Still using a tablet? That iPad or Android model is starting to look like a Model-T. While the Apple iPad is still dominant (at 32.5% market share), the Microsoft Surface Book increased in market share by 9% in Q1 (to second place and 25%) over the same quarter last year while the iPad leveled off. Also, laplets like the Surface Book accounted for 33% of all tablet sales. The trend suggests that more people are buying a 2-in-1 that works as a laptop and as a touch tablet when you detach the display. Why laplets? In some ways, it doesn't make sense for business users. They are heavier, usually run Windows 10 instead of a "true" mobile operating system with plenty of touch apps, and are a bit clunky. The Surface Book is about three times as thick as the latest iPad. Yet, users crave the highest level of functionality possible. If you take an iPad along on a trip, you will need a mobile keyboard if you want to do any serious typing. A laplet provides everything users need for work and play. With a Surface Book, you can type up an entire novel with its keyboard. Disconnect the display, and you can sit back on a plane and watch a movie. Most importantly, most laplets also run full desktop apps like Photoshop and Microsoft Office. Laplets have a ways to go, though. For one, they are still underpowered for high-end games and data-intensive apps. They are meant for productivity and consuming media, which hits a sweet spot for most users, but it's not a machine an engineer would love for CAD/CAM diagraming.

Apple Now Embraces Intel?

Intel has missed out on the iPhone party until now, ceding business to other chip makers in the process. But that could be about to change. Apple will use modems from Intel in some models of its next smartphone, replacing chips from Qualcomm. An Intel modem will go into iPhones for the AT&T Wireless network in the US and some international versions, a report says. One factor in Apple's decision could be that it likes to use multiple suppliers, meaning it's not at the mercy of one vendor if a vendor decides to raise prices.

SIMformation is the monthly newsletter from SIM2K. Information presented here is designed to inform you of trends in the business world affecting information technology. For questions or comments, write SIM2K, 6330 E. 754th St., Suite 336, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

Cloud Security Tips

We continue to be faced with questions about moving data and services to "The Cloud". Security of your information continues to be the most important factor in making this decision. Many security experts, software companies and cloud service providers believe that cloud computing may be a more secure way to store data given that all the attention on the Cloud has made the cloud hosts more attentive to security issues.

The experts will say that most small businesses do not have high security measures in place for their data on-site and lack tight password protection policies, firewall management and backup procedures. They see business owners backing up their entire network to a USB drive and leaving it in their car overnight, or are using weak passwords for important access points to their network, which are much bigger security risks than storing it in a highly secure, highly redundant cloud platform. Of course, as a SIM2K customer, we hope we have moved you well past these bad examples of data management and you do have one of our services such as SIM2K® Serenity, SIM2K® Backup Backstop and SIM2K® Remote Backup Service.

However, there is some validity in the experts' belief that Cloud companies may have more enhanced security measures. But, it is important to select a cloud provider who actually does have these security safeguards in place. There are important questions you should ask before trusting any data into the Cloud.

1) Who outside my company will have access to my data?

If the Cloud company cannot segregate data to the point where your files are "eyes only" to your people, think again about this company. Also, check what the policy is for that company's access to data – will the hosting company have access to actually be able to open and read your files, or do they merely have the ability to check that files are received, backed up and restorable.

2) What security measures are in place whenever a mobile device/laptop is lost or stolen?

Employees tend to save password information on devices which could provide easy access to your Cloud files. What is that capability of the hosting company to block users, force password changes or otherwise secure your data should this happen. And, what is the time frame for completing this? If you have to put in a support request that takes a day to be acted upon, that's not appropriate. There should be a procedure for escalating this sort of request.

3) What is the frequency of data backups, and can data be restored?

How often is your data backed up, and, just as important, where is the data backed up? For example, if you are in retail and have hundreds of transactions each day, you don't want to see your data backed up weekly - you would lose a huge amount of information should there be a crash. If you only make small data changes, like an occasional letter or only do weekly bookkeeping, then a weekly backup might not be an issue. But find out first before committing to any Cloud host and be sure that the backup schedule is suitable for your business data volume. Ask where this data is being backed up – to the same device where your production data is being kept, or to an off-site location? This becomes important should there be a disaster that destroys the host computer farm. Finally, what is the policy for the Cloud host for restoring data from a backup if needed? First of all, do they actually check that your data can be restored in a readable fashion, then, what does it take to complete a restore? Is it something you can initiate, or do you have to rely on their services for this. This all comes into play if you do have issues with data and need to turn to a backup - the longer this takes, the longer your employees are not being productive.

4) What happens if the Cloud provider goes out of business?

Hopefully you have done due diligence on your Cloud provider company and are assured of their stability before ever committing data to them. But companies to fail, so what is their game plan in this eventuality? Do they have a migration plan to get your data to another company, or are you faced with attempting to download terabytes of data to your own network on short notice to "save" your files.

5) Where is my data actually stored?

This is important from the standpoint of physical security. Is the Cloud provider's server farm domestic or in a foreign nation? If in the US, is it in an urban area or perhaps in an area prone to flooding, wildfires or tornadoes? Is it in an area with "clean" electricity that doesn't have voltage spikes or be prone to outages? And, is the server farm in a secured facility or just some warehouse space in an industrial park?.

Any data storage has risk, whether in the Cloud or on your own network. There is no way to completely guarantee absolute security. We still believe there are advantages to setting up a private cloud solution for our clients as then we can address these questions posed here with you to your satisfaction, rather than relying on a third party company to be in full compliance with your requirements. If you are considering a move to the Cloud, please contact SIM2K and let us help coach you through this process to find the best solution for your company.

SIM2K
6330 E 75th St., Suite 336
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com