SIM2K
Adapting Technology to Your Business Needs

6•20
Information you can use

SIMformation

Global Pandemic and Cybercrime

As economies stall, how will cybercriminals react? Will they change targets, techniques, or priorities? Will more people, whether inside or beyond your organization, present a threat? Experiences and insights from past recessions can help us prepare for what's ahead.

Cybercrime rose during the last recession in 2008. Regulatory Data Corp said it saw an average rise of 40% in cybercriminal activity for the two years following the recession’s 2009 peak. In 2009, Reuters reported that internet fraud in the US rose 33% in 2008, while McAfee’s Virtual Criminology Report from that period suggest there was a large surge in malware, bots and Trojans around 2008 compared to the year before. While that trend hasn’t abated since, the change in the digital landscape presents greater opportunity for attackers.

The recession of 2008 occurred in a very different technology landscape. Things like cloud services and smartphones were still in their nascent phase, while the selling of cybercrime tools and services on the dark web had yet to be commoditized. Because of this, Forrester says it’s hard to make predictions based on the 2008 recession. “In 2020, however, we are much more dependent on technology than even a decade ago, so expect to see cybercrime increase,” the company says.

Phishing will remain a prime tactic. Attackers are not developing new techniques or changing tactics around phishing. They are simply re-skinning their existing capabilities with the new related themes. In the same way that COVID-19-related lures have skyrocketed during the course of the pandemic, we are beginning to see financial related lures emerging. There has been a spike over the last two weeks of thousands of domains being registered with words like ‘stimulus,’ ‘relief,’ ‘refund’ and ‘rebate’ in them”, along with a rapid change from COVID19-related e-mails to, “Here’s how you get your check from the government,” or, “Here’s how you get a relief loan.”

Organizations can expect further phishing lures purporting to be from the likes of the Small Business Administration in the US and similar government bodies in other countries. Reports of payroll scams quickly emerged around the IRS and stimulus checks.

Ransomware will continue to be a popular method of attack because it makes money. Business e-mail compromise (BEC) will also be popular. Unfortunately, there are so many records for sale on underground markets that you can easily find your way into a business. You only need 10% of those passwords to still be working to have a successful operation. As well as exploiting access themselves, attackers might sell that access to third parties who might be better placed to make money through fraud or ransomware. Attackers, like enterprises, will have to adapt to different monetization models due to the changes from the pandemic. Financial conditions aren’t what they were six months ago, which decreases the likelihood of ransom payments, and things like cryptomining could increase.

Off-the-shelf hacking tools will get cheaper. Never very expensive to begin with, ready-made hacking tools might become even cheaper and more accessible. There are reports that cybercriminals, especially the lower-tier threat actors, are already offering steep discounts on their services as certain types of exploit kits become less rewarding during lockdowns. “Cybercriminals are experiencing the same thing that we're experiencing in the real world and seeing a drop,” says a security expert. “We’ve seen people offering deep discounts, especially point of sale because so many retail organizations are closed.”

More people will **use hacking tools** given predictions for permanent job losses estimated to be in the millions. A new report from the Global Initiative Against Transnational Organized Crime warns that in the face of a recession that young people, especially those with any IT skills, may turn to cybercrime. “High unemployment rates among young people in the developing world and limited job opportunities in the legitimate IT sector create push factors for ‘deviant globalization’,” warned the report.

Insider threats increase as companies worry about fraud committed by insiders due to fears over job losses, reduced pay or targets being harder to achieve due to a difficult financial landscape. “Layoffs and furloughs always lead to a bigger concern around insider threat,” according to experts. “Going all the way back to the .com bust in 2000, we’ve seen it in the past that insider threat activity increased dramatically during those rounds of layoffs.” Forrester says that due to large-scale working from home, behavioral analysis of employees isn’t as easy as it was previously. Routines are different and more liable to fluctuate compared to traditional office behavior. “Firms need to adopt zero-trust policies to limit the information employees have access to, make sure they have analytic tools that reflect the environment employees now work in, and receive advanced notice of job actions so that they can monitor and prevent insider threat activity.”

Other threats include the increase activity by nation-state actors conducting espionage or seeking trade secrets and patent information, and the possibility that your third-party vendors will not survive, opening the possibility of security holes in unsupported software applications.

SIM2K is ready and able to help your company assess your security efforts and help boost your preparedness against cybercriminals in this - interesting - landscape. Call us today.

Virtual Desktops See Surge

With the coronavirus forcing a telecommuting change, going from corporate workers begging to be allowed to work from home to companies insisting that they now do stay at home to work, Microsoft released the latest desktop-as-a-service (DaaS) program, Windows Virtual Desktop (WVD).

It appears that a lot of businesses are latching on to WVD as a way to solve their sudden telecommuting difficulties. A manager at Microsoft noted that there are "6 times more WVD users active now than expected during 2020."

Given that most companies are dealing with the astronomical rise in telecommuting by trying to manage Windows 10 users remotely has not been pretty. The tech chat is full of comments from system administrators saying things like "I've had about a billion calls on how to use the VPN, and don't talk to me about securing and patching Windows 10 remotely."

With more people than ever before working from home, and with the thought that this may be the "new normal," it may be time for DaaS to move to the forefront.

It doesn't have to be Windows, of course. For example, Chromebooks were built from day one as DaaS devices. While enterprise adoption of Chromebooks has not taken off like their use in education has, when paired with GSuite, they actually are a fast, inexpensive and powerful DaaS device.

Thanks to the pandemic, companies have had more than enough IT change on their hands to even think about shifting to a new platform. That's where WVD comes in. It may be really different in some ways, but as far as end users are concerned, it's still Windows. With the latest Windows Virtual Desktop Spring 2020 update, you run Windows 10 VMs from Azure, Microsoft's Cloud service. It also supports the older Windows Server Remote Desktop Services (RDS) desktop and apps, Office 365 ProPlus apps for the enterprise and other third-party Windows apps. The spring WVD release is in public preview, so it doesn't come with service-level agreements. Be that as it may, IT insiders report that many companies are running it in production.

However, this is still a new venture that IT pros are still learning. There is not a lot of information about WVD on Google or in the knowledge base repositories, so while Microsoft has details on how to deploy it, subsequent requests for support are still going unanswered as administrators figure out the fine points of WVD. Even so, those companies using it figure it is easier to manage users working remotely with WVD than it is to try to keep them safe and effective using old-style Windows.

Some IT pundits had predicted that DaaS would come into wide use by 2025. Now, this pandemic response has made them believe that most "office" computers would be running Windows as a service much earlier – except now the "office" may be "work from home."

Microsoft is certainly invested in promoting this approach, as it gets them away from having to rely on individual users to keep Windows updated and everyone on the same version. By pushing out Windows as a service, and allowing companies to standardize the user experience for all workers through a virtual desktop, this could be a major shift in the approach the enterprise takes to provisioning their employees. SIM2K will continue to monitor developments in this area and inroads of WVD in the marketplace.

Microsoft Adds Features to Edge

Microsoft has announced some business-designed additions and improvements it plans for the Edge browser. The Chromium-based Edge, which Microsoft debuted in stable form in January, was to have been slowly rolled out to a subset of users "in the coming weeks" after a Jan. 15 announcement. That didn't happen. Whether because of Microsoft's own delays, the disruption of lock-downs and work-at-home orders resulting from the coronavirus pandemic, or a combination, Microsoft never got around to distributing the new Edge. That will now change. Edge will be "delivered via a measured roll-out that you'll see ramping up over the course of the next few weeks," says Microsoft.

Windows 10 Home and Windows 10 Pro devices that are not being managed by IT will be eligible for the automatic replacement of old Edge with new Edge. Windows 10 Enterprise and Windows 10 Education will be immune from the Microsoft-mandated switch, as will Home and Pro systems joined to an Active Directory or Azure Active Directory domain. But, if you have to have Chromium Edge, users have been able to manually download and install Chromium Edge, and will continue to be allowed to do so.

Some of the new business-related updates to Edge include a new "WORK" category displayed for all Microsoft 365 customers. It slips into the already-available ALL/IMAGES/VIDEOS/MAPS/NEWS/SHOP choices at the top of Bing's results page. WORK slots between ALL and IMAGES and, when selected, shrinks the results to work-related files, locations, people, sites and so on - assuming a user has logged in with his or her work or school account.

Edge also now supports Windows Information Protection (WIP) in Windows 10. WIP, formerly known as Enterprise Data Protection (EDP), enforces data protection rules set by the organization, preventing accidental data leaks when employees blend personal and work tasks on a single device. IT-mandated policies, such as which apps can access corporate data, are enforced by WIP. Administrators can bar uploads from being sent to non-work locations, automatically encrypt work files when downloaded from a designated work locale, and more.

The other major business-oriented improvements to Edge center around synchronization, an important component of any browser when users have multiple devices and want to keep everything lined up. Administrators also now have access to a policy for managing which data types can be synced, letting them, say, block password sync but allow collections, extensions and bookmarks to synchronize. Edge will also feature enhancements to its handling of multiple profiles, particularly those dedicated to work by virtue of company credentials and generic personal profiles, usually linked to a Microsoft Account for log-in. Automatic Profile Switching which will detect work-related links - for example, an intranet site or a line-of-business web app - and then if necessary switch from the personal profile then in use to the work profile, without requiring another sign-in session.

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. 75th St., Suite 336, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

Android Apps Improve Productivity

Google is launching several new mobile features including One-tap Assistant Action Blocks along with new features for Live Transcribe and Sound Amplifier.

Teased last year, **Action Blocks** are designed for those that have a hard time learning or remembering how to navigate their phone. Given that even common tasks often require multiple steps, Google is adding customizable homescreen Android widgets to make the entire process a single tap. The problem with apps is that they require a certain amount of cognitive function, and so the user will have to make choices, they'll have to remember things, they'll have to enter text, they'll have to change text.

The new Action Blocks app lets you create a shortcut for any existing Google Assistant capability. This includes making calls, sending texts, playing videos, starting playlists, and controlling smart home devices. Users then select a custom image that will be memorable to them and place that widget on the homescreen. Depending on the action, the necessary app will immediately open or Google Assistant slides up with the requested information. The Action Block icon—for example, a photograph of a cab—triggers the corresponding Assistant command, like ordering a rideshare. Action Blocks can be configured to do anything the Assistant can do, in just one tap: call a loved one, share your location, watch your favorite show, control the lights and more. The Action Blocks app is available on the Play Store today and requires Android 5.0 or later.

Action Blocks actually lets you string together multiple Assistant commands and put them into a single button. So if, for instance, you wanted to make a simple one-tap button you could press to catch up when you start your day or come out of a meeting, you could type in combination commands like these:

- Take my phone off silent and read my reminders
- Take my phone off silent and read my messages
- Take my phone off silent and what's my next meeting

In addition to allowing you to bundle multiple Assistant commands into a single button, Google's Action Blocks add-on will let you perform tasks on both your phone and another Assistant-connected device. For instance, you're working from home, and you want to take a quick break for some quiet thought and reflection. You could create an Action Block with the following command:

- Put my phone on silent and play classical music on my office display

Google has also updated **Live Transcribe** so it can now vibrate your Android device when somebody nearby says your name. Google's real-time speech-to-text service now supports custom words/names for "different places and objects not commonly found in the dictionary."

There's also the ability to search past conversations if you have "Saving Transcriptions" from the past three days enabled. The tool now supports 70 languages, including: Albanian, Burmese, Estonian, Macedonian, Mongolian, Punjabi, and Uzbek.

Finally, **Sound Amplifier** now supports Bluetooth headphones, while the tool can boost audio from media playing on-device on Pixel phones, instead of just what's playing around you.

"Random Tid-Bytes"

Voice Passwords Next "Big Thing?"

Face recognition is having a moment. Apple mainstreamed face unlocking for smartphones with its Face ID. Several companies in the United States and China have developed face-recognition systems that can ID faces even when most of those faces are covered by a face mask. Everyone is talking about face recognition. On face value (no pun intended), it appears that face recognition will serve as the dominant biometric system over the next 20 years. But now experts feel that Voice ID will become extremely important over the next decade. Google is slowly rolling out a new Google Assistant feature called Voice Match, which enables the identification of users to authenticate purchases by the sound of their voice. Voice Match was introduced in 2017 as a new feature in the Pixel 2 smartphone and Google Home smart speakers. Back then, Voice Match enabled Google Assistant to tell who was speaking in order to choose the right calendar, e-mail and media services. It has continued to be upgraded to offer better, faster recognition of different voices, and could be the next thing in providing biometric security, moving users away from text passwords.

Exploiting the Coronavirus: Malicious Zoom Installer

Whether you're working from home or trying to stay in touch with loved ones, video conferencing apps like Zoom are becoming the new normal. Cybercriminals have exploited this type of application before, but their latest scam may be the trickiest yet. Scammers are sending out phishing e-mails with links to download the latest version of Zoom. When clicked, the link takes you to a third-party website – not the official Zoom site – to download an installer. If you download and run the file, the program truly does install Zoom. However, it also places a remote access trojan on to your computer, giving cybercriminals the ability to observe everything you do, includimg keylogging, recording video calls, and taking screenshots. Remember, if an e-mail directs you to install or update an application, do not click on the link in the e-mail. Instead, go directly to the official website through your browser. This ensures you are accessing the real page and keeping your credentials safe.

Honda Factory Shut Down

On Sunday, June 7, Honda experienced a disruption in its computer network that has caused a loss of connectivity, thus impacting its business operations. The cyber attack, which began Sunday, has stopped employees from being able to access certain computer programs and thus halting production. Marysville's Honda plant sent home A-shift first thing Monday morning when employees were met with entrances that would not open. The Honda server became infected with the 'Ekans' Malware which affected Honda operations worldwide but has not yet had any impact on consumers. The Ekans Malware targets systems which control machinery. It is designed to terminate 64 different software processes on victim computers, including many that are specific to industrial control systems. That allows it to then encrypt the data that those control system programs interact with, breaking the software used to monitor infrastructure, like an oil firm's pipelines or a factory's robots. That could have potentially dangerous consequences, like preventing staff from remotely monitoring or controlling the equipment's operation. Much like other ransomware, EKANS encrypts data and displays a note to victims demanding payment to release it.

Going Incognito - What is Private Browsing, Really?

Private browsing. Incognito. Privacy mode. Web browser functions like those trace their roots back more than a decade, and the feature – first found in a top browser in 2005 – spread quickly as one copied another, made tweaks and minor improvements.

But privacy-promising labels can be treacherous. Simply put, going “incognito” is as effective in guarding online privacy as witchcraft is in warding off a common cold. That’s because private browsing is intended to wipe local traces of where you’ve been, what you’ve searched for, the contents of forms you’ve filled. It’s meant to hide, and not always conclusively at that, your tracks from others with access to the personal computer.

At their most basic, these features promise that they won’t record visited sites to the browsing history, save cookies that show you’ve been to and logged into sites, or remember credentials like passwords used during sessions. But your movements through the web are still traceable by Internet providers – and the authorities who serve subpoenas to those entities – employers who control the company network and advertisers who follow your every footstep.

Most browsers have added additional, even more advanced privacy tools, generically known as “anti-trackers,” which block all kinds of bite-sized chunks of code that advertisers and websites use to trace where people go on the web in attempts to compile digital dossiers and/or serve targeted advertisements.

Although incognito modes and anti-tracking features don’t compose a true system, they’re certainly complementary. If you’re using the browser’s privacy mode without its anti-tracking tools, you’re drastically shorting your effort at remaining concealed.

To get on the practical side, here are instructions for the top four browsers: Google Chrome, Microsoft’s Chromium-based Edge, Mozilla’s Firefox and Apple’ s Safari.

How to go incognito in Google Chrome
The easiest way to open an Incognito window is with the keyboard shortcut combination Ctrl-Shift-N (Windows) or Command-Shift-N (macOS). Another way is to click on the menu on the upper right – it’s the three vertical dots – and select New Incognito Window from the list. The new Incognito window can be recognized by the dark background and the stylized “spy” icon just to the left of the three-dots menu. Chrome also reminds users of just what Incognito does and doesn’t do each time a new window is opened. The message may get tiresome for regular Incognito users, but it may also save a job or reputation; it’s important that users remember that Incognito doesn’t prevent ISPs, businesses, schools and organizations from knowing where customers, workers, students and others went on the web or what they searched for.

Incognito in Microsoft Edge
Edge, the default browser for Windows 10 – and now available for macOS, too – borrowed the name of its private browsing mode – InPrivate – from Internet Explorer the now-obsolete-but-still-maintained legacy browser. InPrivate appeared in IE in March 2009, about three months after Chrome’s Incognito and three months before Firefox’s privacy mode. When Edge was first released in 2015 and then relaunched as a clone of Chrome in January 2020, InPrivate was part of the package, too.

At the keyboard, the combination of Ctrl-Shift-N (Windows) or Command-Shift-N (macOS) opens an InPrivate window.
A slower way to get there is to click on the menu at the upper right – it’s three dots arranged horizontally – and choose New InPrivate window from the menu.

How to do private browsing in Mozilla Firefox
After Chrome trumpeted Incognito, browsers without something similar hustled to catch up. Mozilla added its take – dubbed Private Browsing – about six months after Google, in June 2009, with Firefox 3.5.

From the keyboard, a private browsing session can be called up using the combination Ctrl-Shift-P (Windows) or Command-Shift-P (macOS). Alternately, a private window will open from the menu at the upper right of Firefox – three short horizontal lines – after selecting New Private Window. A private session window is marked by the purple “mask” icon at the right of the title bar of the Firefox frame. In Windows, the icon is to the left of the minimize/maximize/close buttons; on a Mac, the mask squats at the far right of the title bar.

Like other browsers, Firefox warns users that private browsing is no cure-all for privacy ills but is limited in what it blocks from being saved during a session. “While this doesn't make you anonymous to websites or your internet service provider, it makes it easier to keep what you do online private from anyone else who uses this computer,” the caution reads.

How to browse in peace with Apple's Safari
Chrome may get far more attention for its Incognito than any other browser, but Apple's Safari was actually the first to introduce private browsing. The term private browsing was first bandied in 2005 to describe Safari 2.0 features that limited what was saved by the browser.

To open what Safari calls a Private Window on a Mac, users can do a three-key combination of Command-Shift-N, the same shortcut Chrome adopted. Otherwise, a window can be called up by selecting the File menu and clicking on New Private Window. Safari tags each Private Window by darkening the address bar. It also issues a reminder of what it does – or more accurately – what it doesn’t do. “Safari will keep your browsing history private for all tabs of this window. After you close this window, Safari won’t remember the pages you visited, your search history or your AutoFill information,” the top of the page note reads.

So if you share a PC at home while your office is closed, and access company sites or share company logins, etc., this is one way to be sure your family doesn’t come in behind you and do a “gee, what’s this...” look into your business applications, or use your company credit card to buy the latest Fortnight add-on. Call SIM2K for more information on home privacy during these travel restrictions.

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