SIM2K
Adapting Technology to Your Business Needs

5•22
Information you can use

SIMformation

Russians Losing Cyber War

When Russia launched its all-out attack against Ukraine in February, the world expected the invaders to roll over the country quickly. That didn't happen, and Ukraine today, though still under assault, has so far thwarted Russia's ambitions to conquer it.

Russia has also been fighting a quieter war against Ukraine, a cyberwar, deploying what had been considered the most feared state-sponsored hackers in the world. And in the same way that Ukraine has fended off Russia's military might, it's been winning the cyberwar as well. In that cyberwar, as always, the terrain is primarily Windows, because it represents the largest and most vulnerable attack surface in the world. The facts about what exactly is going on have been shadowy. But there's plenty of evidence that Ukraine may keep the upper hand.

The first loss Russia suffered in the cyberwar came at the very beginning of its invasion – in fact, even before the invasion began. Russia used the extensive railways of its partner in the war, Belarus, to rush soldiers, tanks, heavy weapons and other war materiel to the Ukraine border. Once the invasion began, it used the same railroads as a primary supply chain for its troops, and to send more tanks and weapons into Ukraine.

But then came the Cyber Partisans, a hacktivist group of exiled Belarus tech professionals. At the first signs of the Russian buildup, the Cyber Partisans attacked the Belarussian train system, slowing troop movements, supplies and weaponry. They worked in concert with Belarusian railroad workers and dissident Belarusian security forces. The Washington Post notes that they played "a role in fueling the logistical chaos that quickly engulfed the Russians, leaving troops stranded on the front lines without food, fuel and ammunition within days of the invasion."

The Cyber Partisans were successful, in part, because Belarus's train system runs on the more-than-year-20-old Windows XP, a hacker's best friend. A Cyber Partisans spokesperson explained, "Tanks cannot be transported by planes. Heavy artillery cannot be transported by planes. So, they do need to use these trains. Cyber Partisans attack the internal network of the railway systems, as well as equipment, software, and any databases that are associated with the railway systems…. Windows XP is a really old program and it can be easily attacked…. They didn't secure the systems. So, as much as people admire the work of Cyber Partisans, we should also state that it was not that hard to hack, because [the Belarus] regime disregarded simple cybersecurity practices."

The Cyber Partisans aren't the only ones involved in the cyberwar against Russia. The Ukrainians are, too – and there's evidence they've held off what has long been considered the perhaps most fearsome cyberwarriors in the world: Russian intelligence agencies and the hacking groups they support.

A Microsoft report found plenty of evidence that Russia is engaged in a "hybrid war," using soldiers and weaponry in tandem with cyberattacks and the online spread of misinformation. For example, the report found the Russians targeted a government agency with malware in coordination with hitting government buildings with missile strikes.

As the Russians turned their ground and missile attacks towards the east and south, they also coordinated cyberattacks there.

Throughout the war, many of the Russian attacks targeted Windows machines. Russian hackers frequently used the Windows utility SecureDelete to, in the words of Microsoft, "permanently delete data from targeted devices."

A Microsoft investigator looking into the biggest and most complex cyberattacks, says of the Russian cyberattacks: "They brought destructive efforts, they brought espionage efforts, they brought all their best actors to focus on this…. It's definitely the A-team."

The New York Times reported, "…Ukrainian defenders were able to thwart some of the attacks, having become accustomed to fending off Russian hackers after years of online intrusions in Ukraine…. Ukrainian officials said they believed Russia had brought all of its cyber-capabilities to bear on the country. Still, Ukraine managed to fend off many of the attacks."

The Microsoft expert added: "Ukrainians themselves have been better defenders than was anticipated, and I think that's true on both sides of this hybrid war. They've been doing a good job, both defending against the cyberattacks and recovering from them when they are successful." This doesn't mean, of course, that the Ukrainians will eventually win the cyberwar or the physical war. But the evidence so far shows they can at least hold their own in the cyberwar with the Russians, which bodes well for their future.

California To Limit Employee Monitoring

The California State Assembly is considering new rules that would offer workers greater protection from the use of digital monitoring tools by employers. The "Workplace Technology Accountability Act" would create a way to protect workers against the use of technologies that can negatively affect privacy and wellbeing.

The bill would "establish much needed, yet reasonable, limitations on how employers use data-driven technology at work," the bill's author said. "The time is now to address the increasing use of unregulated data-driven technologies in the workplace and give workers – and the state – the necessary tools to mitigate any insidious impacts caused by them." The use of digital surveillance software grew during the pandemic as employers sought to track employees' productivity and activity when working from home, installing software that uses techniques such as keystroke logging and webcam monitoring.

The bill, which was approved by the committee on a 5-2 vote and now moves to the Appropriations Committee for more debate, makes three core proposals:

- To ensure employees are notified prior to the collection of data and use of monitoring tools and deployment of algorithms, with the right to review and correct collected data.
- To limit the use of monitoring technologies to job-related use cases and valid business practices.
- To require employers to conduct impact assessments, with worker input, on the use of algorithms and data collection to identify potential harms and discriminatory impacts.

Among those opposing the measure is the California Chamber of Commerce. "Based on our initial review…, quite frankly the bill is unworkable," said the California Chamber of Commerce. The business group argues it would place unnecessary demands on employers to store and review collected data and ensure technologies are compliant, while potentially hitting small business employers with penalties up to $20,000 for violations.

Regulating workplace management and monitoring technologies is an growing priority for lawmakers in the US and in Europe. Although though the General Data Protection Regulation put in place some rules against the misuse of worker data by employers, the European Commission recently drafted proposals that would offer greater protection to gig workers that are supervised by algorithms.

The bill's prospects for passage by the full Assembly were not immediately clear. If passed and signed into law, it would apply to all businesses that use monitoring tools and could have ripple effects beyond just California. The state is home to many big tech firms and often adopts worker protection measures that could similar legislation in other states.

As we have seen, policy decisions in California are often the bellweather for other states to follow. While this subject has not come up in Indiana, it is something to watch for in the future.

As If the Song Isn't Bad Enough

In February, researchers identified spear phishing e-mails containing new malware that shares infrastructure with playbooks associated with North Korean campaigns. The spear phishing e-mails were written to appear as though they were sent from a nuclear security expert who currently works as a consultant for in the U.S. The e-mails were sent using a public e-mail address with the expert's name and had a subject referencing North Korea's nuclear issues. The e-mails had a malicious Excel macro document attached, which when executed led to a new Microsoft Visual Basic (VB) script-based malware family which has been dubbed "BabyShark".

BabyShark is a relatively new malware. The earliest sample found from open source repositories and data sets was seen in November 2018. The malware is launched by executing the first stage HTA from a remote location, thus it can be delivered via different file types including PE files as well as malicious documents. It exfiltrates system information to C2 server, maintains persistence on the system, and waits for further instruction from the operator.

Researchers determined the phishing emails targeted at least:

- A university in the U.S. which was to hold a conference about North Korea denuclearization issue at the time
- A research institute based in the U.S. which serves as a think tank for national security issues, and where the previously referenced nuclear expert currently works.

An expanded search in public repository samples identified additional malicious document samples delivering BabyShark. The original file names and decoy contents of these samples suggested that the threat actor might have interests in gathering intelligence related to not only North Korea, but possibly wider in the Northeast Asia region.

Since the release of this initial research, malicious attacks leveraging the BabyShark malware have continued. In fact, they have widened their operation to target the cryptocurrency industry. The malware's server-side implementation showed that the malware author has made certain efforts to maintain the operational security for operating the malware and C2 infrastructures. The threat actor leverages other commodity and custom developed tools in their campaigns. In this case, they were PCRat and KimJongRAT, but these may be changed to other malware families in the future. Malicious attacks using the BabyShark malware also seem likely to continue based on our observations and may continue expanding into new industries.

Threat actors are using the Russian/Ukraine conflict as a diversion for increased activity, so you should be aware of new attacks being levied against all networks and have your anti-virus and security tools up-to-date. Call SIM2K for help.

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 214, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

Passwords on the Outs?

In an unusual show of alliance, Apple, Google and Microsoft have joined forces to expand support for password-less logins across mobile, desktop and browsers.

Passwords are notoriously insecure, with easily guessed credentials accounting for more than 80% of all data breaches, per Verizon's annual data breach report. While password managers and multi-factor technologies offer incremental improvements, Apple, Google and Microsoft are working together to create sign-in technology that is more convenient and more secure.

The announcement that the tech companies are expanding support for a password-free sign-in standard from the FIDO Alliance and the World Wide Web Consortium means you'll soon be able to use your smartphone to sign in to an app or website on a nearby device, regardless of the operating system or browser you're using. You'll use the same action that you take multiple times each day to unlock your smartphone, such as with a verification of your fingerprint, face scan or a device PIN.

Users will also be able to automatically access their FiDO sign-in credentials, or "passkeys," across multiple devices – including new ones – without having to re-enroll every account.

While the three companies have long supported the password-less sign-in standard created by the FIDO Alliance, users are still forced to sign into each website or app with each device before they can use the password-less feature. Over the next year, the three companies will implement passwordless FIDO sign-in standards across macOS and Safari; Android and Chrome; and Windows and Edge. This means that, for example, users will be able to sign in on a Google Chrome browser that's running on Microsoft Windows, using a passkey on an Apple device.

This will make it much more difficult for hackers to compromise login details remotely since signing in requires access to a physical device.

"Working with the industry to establish new, more secure sign-in methods that offer better protection and eliminate the vulnerabilities of passwords is central to our commitment to building products that offer maximum security and a transparent user experience – all with the goal of keeping users' personal information safe," said an Apple executive.

This new collective commitment was commended by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), which called it "the type of forward-leaning thinking that will ultimately keep the American people safer online. At CISA, we are working to raise the cybersecurity baseline for all Americans," the agency said. "Today is an important milestone in the security journey to encourage built-in security best practices and help us move beyond passwords. Cyber is a team sport, and we're pleased to continue our collaboration."

While the password has so far survived many attempts to kill them for good, this could be one of the final nails in the password's casket. SIM2K will watch this evolution across the various platforms and keep you informed when (and if) this approach proves beneficial. Call us if you have questions.

"Random Tid-Bytes"

Zultys Announces MXArchive Service

MXarchive enables storage of all your important data on a dedicated, secure separate server. Having your system server bogged down by thousands of megabytes of stored data can be detrimental to the speed, integrity, and security of the system. Zultys MXarchive is the solution to this problem. When utilizing an MXarchive server, recorded data generated by the MX system will be downloaded from the MX to the archive for indefinite, secure storage. These records can then be accessed and viewed at any time using the MXarchive Viewer application. This includes Instant Messages/SMS, voicemails, call recordings, faxes and other call attachments from conferences. A viewer screen allows you to quickly review stored information and retrieve records as needed. MXarchive will work with any Zultys installation – Cloud, on-premise and virtual.

Where's Ripley when you need her?

Besides the name of the creature that "stars" in the Alien movies, Xenomorph is also the name given to an Android banking Trojan. Researchers found this Trojan distributed on the official Google Play Store, with more than 50,000 installations. The researchers dubbed this malware Xenomorph because it shows similarities to another banking Trojan that is generally known as Alien. The researchers found Xenomorph on the Google Play Store under the name Fast Cleaner, pretending to be an application aimed at speeding up the device by removing unused clutter. In reality this application was a Trojan dropper which contacted a remote server and downloaded one of several payloads based on certain parameters. One of these payloads was the banking Trojan Xenomorph. The Fast Cleaner app has now been removed from the Play Store but not before it was downloaded more than 50,000 times. The main task of this banking Trojan is to steal credentials, combined with the use of SMS and Notification interception to log and use potential 2FA tokens. It does this by mimicking legitimate banking apps, opening a copy of the original interface of the legitimate banking app and this overlay sends entered data like usernames and passwords to the threat actor.

Stalkerware Shows Decline in Installations

Malwarebytes revealed that detections for apps that can non-consensually monitor another person's activity reached their highest peak ever in 2021, but that, amidst the record-setting numbers, the volume of detections actually began to significantly decrease in the second half of the year. Documented to have a clear intersection with situations of domestic abuse, it was not only stalkerware-type activity that increased during the global pandemic, but also cases of domestic abuse as reported by state and federal prosecutors and by shelters. In 2021, Malwarebytes recorded a total of 54,677 detections of Android monitor apps and 1,106 detections of Android spyware apps. However, although the overall numbers are up, detections have taken a downward turn since the peak of May and June 2020. The Federal Trade Commission issued an enforcement action against a stalkerware developer, and Google removed several ads that promoted stalkerware, contributing to the decline in installations.

Androme? Chroid?

Google has launched the first official beta version of this fall's Android 13 update. But unlike most Android betas, this release doesn't have most of the software's key features – rather, is focused primarily on under-the-hood improvements. But it also shows the continuing evolution of the Android operating system alongside the Chrome operating system, both Google's property.

Thanks to the way Android is created, it's possible to review Google's Android 13 code and get a glimpse at some still-under-wraps elements that are actively being developed. Here, specifically, are three features to improve your Android usage.

1. Android 13 will set the stage for a better big-screen experience

After years of neglecting and basically giving up on the Android tablet form, Google is bringing its focus back to big-screen Android computing. All signs suggest the Android 13 release will build upon the big-screen optimizations introduced in the Android 12L "feature drop" Google worked on right after the launch of Android 12 last fall.

Specifically, Android 13 will optimize the core Android interface for larger screen experiences. That means when you're using a tablet or a folded-out foldable phone with Android 13, you'll see different elements on different halves of the screen and gain access to some powerful desktop-like multitasking tools – including a clearly Chrome-OS-inspired new taskbar that lets you access your favorite apps from anywhere and even drag them to create an on-the-fly split-screen setup.

2. Android 13 will essentially create a whole new category of devices

Aside from its core interface improvements, Android 13 is poised to introduce some new tablet-specific features that could change what the term "tablet" even means in our minds. Android 13's code includes loads of material related to a new "hub mode" for large-screen devices. This new feature appears to allow tablets to be treated as shared devices when docked – with access to a specific set of selected "communal apps" in that context – and then let multiple users pick the tablets up and sign into their own personal profiles.

As part of that, Android 13 introduces a freshly revamped interface for Android's long-underappreciated multiuser support system. And it includes a souped-up screen saver system that seems to let you add widget-like "complications" into a device's idle-time display in order to make it more info-rich and useful.

All combined, these elements add up to create a whole new kind of use case for Android tablets – one that can open up lots of interesting doors both on the home front and in the office and other business environments. It's no wonder Google's so confident Android tablets and Chrome OS tablets can coexist harmoniously and address completely different needs.

3. Android 13 will make notifications even smarter

Android's notifications have always been one of the platform's strengths and advantages over competing smartphone operating systems. But Android 13 takes it to a higher level.

First, Android 13 include a crafty new system where you can touch and hold any notification and then drag and drop it onto either side of your screen to create an instant split-screen between the associated app and whatever else you were already viewing. When combined with the taskbar drag-up option discussed above, this brings Android's long-buried and neglected split-screen feature back into the forefront and makes it feel like a native part of the core interface instead of an awkwardly tacked-on afterthought. It makes notifications even more useful and interactive, too. And it might just turn split-screen into something lots of us actually use.

Beyond that, Android 13 introduces a new notification permission that requires all apps to ask you for permission to send alerts before they're able to do so. That means by default, no app will ever be allowed to notify you unless you explicitly say you want to receive its notifications. It's a subtle but significant shift that puts the power in the user's hands and should considerably cut down on needless notification noise.

And remember: All of this is still just scratching the surface. The full Android 13 picture likely won't become clear until later in the year, closer to the final Android 13 rollout. Based on what tech experts are seeing so far, though, there are many reason to get excited – and plenty of reasons to watch closely for what comes next in the weeks and months ahead.

Google is making it clear it is ready to take traditional Android tablets seriously again and bring them onto equal footing with the Chromebook tablet experience. And the more closely we see what the company is up to, the more obvious it's becoming that much of its inspiration for the Android tablet setup is indeed coming straight from the realm of Chrome OS. At its core, the shift adds up to create a whole new phase for Google's Android-Chrome-OS alignment – one in which Chromebooks are now serving as the model and the source for Android's incoming improvements. It's a big shift from the pattern seen playing out over the past several years, but ultimately, it's the same philosophy – only flip-flopped for a different type of device form.

Whether you use an Android device, a Chromebook, or both, you can take heart in the fact that the two platforms are pushing each other forward and aiding each other's evolutions in some pretty phenomenal ways. It may not be the future most folks once expected to see play out with Google's two primary platforms, but it's absolutely a future that maximizes each side's strengths.

At the end of the day, all patterns and strategies and philosophies aside, all that matters to Android users is that they get the most effective possible experience, no matter what type of device being used at any given moment. And from the looks of it so far, it sure seems like Google's latest efforts will go a long way in connecting its virtual universes and bringing users the best of both worlds.

SIM2K
6330 E 75th St., Suite 214
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com