SIM2K
Adapting Technology to Your Business Needs

11•21
Information you can use

SIMformation

Russian Hacker Group Still Active

Nobelium, the Russian hacking group responsible for breaching SolarWinds, is still at it. The Russian hackers behind that successful 2020 breach of US federal agencies compromised as many as 14 technology firms since May as part of another apparent espionage campaign, Microsoft said.

The hackers have been hitting a different part of the supply chain than in the 2020 breach: companies that buy and distribute software and manage cloud computing services. Microsoft did not name the victim companies or identify the ultimate targets of the alleged Russian spies.

The Microsoft statement follows reporting that the Russian hacking group had been leveraging compromised technology vendors to try to infiltrate US and European government networks in previously unreported activity. “This recent activity is another indicator that Russia is trying to gain long-term, systematic access to a variety of points in the technology supply chain and establish a mechanism for surveilling – now or in the future – targets of interest to the Russian government,” said Microsoft. The hackers have tried to break into more than 140 software resellers and other tech firms through common techniques such as phishing, according to Microsoft. The ultimate goal is to “impersonate an organization’s trusted technology partner to gain access to their downstream customers.”

It’s the latest look at a Russian group that has confounded US government and corporate defenses. The hackers are best known for using tampered software made by federal contractor SolarWinds to breach at least nine US agencies in activity that came to light in December 2020. The Biden administration in April attributed the spying campaign to Russia's foreign intelligence service, the SVR, and criticized Moscow for exposing thousands of SolarWinds customers to malicious code. Moscow has denied involvement.

The suspected Russian operatives often cast a wide net of potential victims before sifting through them for valuable targets. That’s what happened in May when the hackers impersonated a US government agency and sent malicious emails to 150 organizations in 24 countries, according to Microsoft. Among the apparent targets of that spying campaign were an ex-US ambassador to Russia and anti-corruption activists in Ukraine. And just this month, the NSA has disclosed an attack at breached nine organizations in the defense, energy, health care, technology and education sectors. The attackers are exploiting a vulnerability in software that corporations use to manage their network passwords. The FBI warned the public in September that hackers were exploiting the software flaw and urged organizations to update their systems. Days later, the hackers scanned 370 computer servers running the software in the US alone, and then began to exploit the software.

Whoa Up on Windows 11

You have probably heard that Windows 11 is now being released. But don’t leap right into this. While Microsoft may make it sound like “just click here to update” or even might send it your way with an automatic update (if you have your PC set to accept these), there are some pitfalls with Windows 11. Therefore, SIM2K asks that you check with us before attempting to update – in fact, let us manage these updates for you.

The stumbling block for Windows 11 is that there are hardware requirements in place that some older PCs do not meet. For example, the Dell that I am using to write this month’s SIMformation is an XPS - top of the Dell line – but it is 6 years old. While it has an Intel Pentium chip and lots of memory and storage, what it lacks is what is known as TPM – a Trusted Platform Module. A TPM is a security chip that can be embedded in a laptop or plugged into most desktop PCs. It’s basically a lockbox for keys, as well as an encryption device a PC can use to boost its security.

When you boot your PC, one chip wakes up and begins activating other components. Once all of the hardware is ready, it goes to the storage drive to start the operating system. In a secure environment, the PC first makes sure the operating system is secure. But without a point of reference, the PC has no idea whether any part of the system has been tampered with. With a TPM, the PC can compare notes using the information stored in the locked-down TPM. If it all matches, the boot proceeds as normal. If something is amiss, red flags go up.

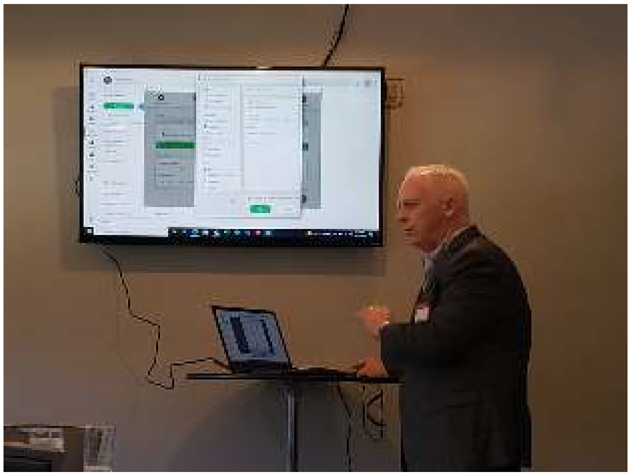
TPMs originally came as standalone chips, and originally they were used only in corporate computers, where security was more of a concern and customers would pay the premium for the add-on. More recently, AMD and Intel have integrated firmware-based TPM into their CPUs. That’s made TPM support far more available. However, you need to have a recent PC with one of these upgraded chips.

But, like most of the Tech field, there are work-arounds but these require delving into the arcane areas of the computer, the BIOS. This is something that we do not recommend you do, as you can quickly turn a working computer into a doorstop if done wrong.

This is why we would ask you to check with SIM2K first. We can ascertain if your hardware is compatible with Windows 11 and then, if you really want the upgrade, will do so. But as a final note, Windows 10 is still good through 2025, and the early reviews of Windows 11 are less than stellar – more cosmetic than substance – so don’t be in a rush to upgrade. Call us first.

New Zultys Features

SIM2K recently hosted a “Lunch and Learn” with our Unified Communications Systems partner, Zultys, to introduce several new features coming to the Zultys products.



Kevin Murphy from Zultys introduces new features for ZAC at the SIM2K Lunch and Learn.

One of the advanced features is now the ability to add guest users into a ZAC chat/video session. You can send the outside person a link that enables them to join in the discussion, share files and videos, just like they were on your Zultys system. This will facilitate collaboration with external guests who otherwise would be excluded from the ability to share information in real time through ZAC.

Other new features include the ability to just click on an icon during a call to turn it into a video call, or to share screens with click of another icon.

Zultys is also releasing the new “Z series” of desktop phones designed to work in areas where advanced calling features are not necessary, such as classrooms, examination rooms and warehouse/factory stations.

Zultys is also now offering a plug-in for Microsoft Teams that enables Teams users to incorporate the capabilities of Zultys in a Teams discussion. This can be as simple as just using Zultys for the audio/video connections rather than the Microsoft tool, up to being able to use the ZAC chat, file share and other features along with Teams. An icon appears on the Teams screen when the Zultys plug-in is added for easy one-click access to these features.

Finally, Zultys is adding more features to WebZAC wherein users can access ZAC through a browser and not have to download and install the ZAC client offering more flexibility for remote workers to use the ZAC features from any device. Call SIM2K for more information on Zultys and these new features whether you are a current Zultys user or interested in an advanced communications platform.

Do You Reuse Passwords?

Microsoft has issued a warning to those who reuse their passwords across multiple online accounts. The company said it had identified an uptick in the use of “password spray” attacks over the past 12 months. They involve hackers gathering a list of usernames and passwords leaked online and plugging them in to various websites. Cyber crooks hope to eventually stumble across a working combination that gives them access to someone’s e-mail or social media accounts. From there, they can attempt to break into more sensitive accounts such as your bank or iCloud.

The attacks were identified by Microsoft's Detection and Response Team (DART), which is dedicated to identifying the latest cyber attack methods. The researchers identified two commonly used kinds of password sprays. One involves matching known usernames to commonly used passwords, such as “password” or “123456". The hope is that they will eventually “guess” the correct combination for as many users as possible.

The second technique involves usernames and passwords that have been leaked online in the past. The 2012 LinkedIn hack, for instance, saw the usernames and passwords of 6.5 million users sold online. Google estimates that over 4 billion username and password combinations have leaked in recent years. Hackers can plug these combinations into other websites in the hope that you’ve reused them across multiple online accounts.

One way to check on your accounts is through the free Password Checkup software that can be loaded in Google Chrome and lets you know if your account details have been compromised in a cyber attack or data breach. Once installed, the Chrome extension runs in the background of your browser and checks any login details you used. If your password or username matches a Google database of more than 4 billion compromised credentials, the software will flag them.

An alert that pops up on your screen reads: “Password Checkup detected that your password for [website] is no longer safe due to a data breach. You should change your password now.” It gives you any exposed accounts in a small list that you can click through to change your passwords. All information is encrypted, and Google says it has no way of seeing your data. Alternatively, popular web-tool “Have I Been Pwned” also lets you check if you’ve ever been hacked.

Reusing passwords is not a “best practice” in the IT world, but we recognize most people do this for the convenience. SIM2K can work with you to develop a password strategy to make them memorable without having to use the same one over and over.

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.

No End to Chip Shortage?

Earlier this year, the chip shortage seemed like it might ease sometime in 2022. Now, that forecast appears to have been optimistic. "The shortages are going to continue indefinitely," according to the head of Deloitte's semiconductor industry practice. "Maybe that doesn't mean 10 years, but certainly we're not talking about quarters. We're talking about years."

It is becoming clear that snarls in the semiconductor supply chain are weighing on economic growth. Both GM and Ford said that missing chips led to slashed profits for the third quarter, and Apple is rumored to be cutting this year's production targets for its iPhone lineup, the company's cash cow. Chip woes have become so widespread that Wells Fargo thinks the pressures will curtail US GDP growth by 0.7 percent.

The causes of the chip shortage are myriad, and none of them has a quick fix. For one, people keep buying new phones, tablets, and laptops, and they continue to use network-heavy services like video streaming, video conferencing, and more, which increases data-center use. That appetite has collided head-on with a variety of supply shortages. Recently, substrates that make up printed circuit boards have become scarce. Compared with advanced semiconductors, PCBs are relatively low-margin and easy to manufacture. Most chip companies don't make their own, but without PCBs, semiconductors can't talk to other chips in a computer. A fire at major substrate factory in July 2020 took a significant source offline. As a result, PCB factory capacity is expected to lag demand.

The world's semiconductor manufacturers are swamped, and they're a long way away from being able to meet demand. New plants ("fabs") take years to build and optimize, and companies are hesitant to invest if they think surges in demand will be temporary. While demand is up, whether or not it will persist beyond the pandemic is unclear. Leading-edge fabs cost around $5 to $10 billion, multiple times what they cost a decade or two ago. As manufacturing techniques have advanced, the buildings themselves get more costly to construct, and the machines that make the chips have grown more expensive. Intel, Samsung, and TSMC have all announced new fabs in recent months. But those won't come online for years.

Numerous other problems have piled on, ranging from factory fires to shipping delays. In March, a fire tore through a fab owned by Renesas Electronics. The Japanese company was a key supplier for the automotive industry, and it was already working overtime to make up for the loss of capacity at Asahi Kasei Microdevices, another automotive supplier, which had a fire in one of its fabs in October 2020.

Shipping delays that have plagued so many other businesses haven't skipped the semiconductor industry, either. All of this has contributed to lengthening lead times. At the end of last year, it took 13 weeks for a typical order to be fulfilled; now it's taking almost 22 weeks. Buyers aren't helping. As lead times stretch on, companies are placing more orders and holding more inventory in the hope that they won't get caught without the chips they need.

As manufacturers add incrementally to existing facilities, Deloit says we could see some shortages easing sooner than others. Such additions typically take between 12–18 months to complete. Entirely new fabs, though, take two to three years, he said. Given today's long lead times, incremental capacity may not be enough.

"Random Tid-Bytes"

Changes Coming to Mail Services

Because it could affect many users and businesses, Microsoft is giving everyone fair warning – a year in advance. On Oct. 1, 2022, Microsoft will be disabling basic authentication for its online mail services. This isn't the first time the company has warned us about this. It had planned to disable authentication earlier this year before realizing it couldn't do so without impacting businesses and users still struggling amid the pandemic. Hence, the delay. What is basic authentication? It's what we're used to already – access by username and password to old-fashioned Post Office Protocol or "pop" email, where you log in and download emails to your computer. You might think POP access using basic authentication should be secure enough, assuming you don't click on malicious links, do keep your computer up to date, and use a secure browser. As it turns out, attackers can use weaknesses built into this older protocol to break into online mail servers. As long as those mail servers have to support these older protocols, attackers can use any number of brute force attacks and other devious methods to break into your mailbox.   If you already use a web interface to log into your e-mail and don't use an e-mail application at all, you will not be impacted. In that case, you're basically relying on whatever authentication the web interface supports. If you use an application such as Outlook or other e-mail clients, you may need to redo your account to trigger the app to set up your account with modern authentication protocols

Legislation Requires Ransomware Disclosure

In an effort to better understand and clamp down on the ransomware economy and its related use of cryptocurrencies, legislation has been introduced that would require companies and organizations to report any paid ransomware demands to the Secretary of the Department of Homeland Security. If passed, the "Ransom Disclosure Act" would require a broad set of companies, local governments, and nonprofits that actually pay off ransomware demands to report those payments to the government. Companies would need to report this information within 48 hours of paying a ransom. The bill requires companies to report when the attack occurred, what ransom was demanded and what was actually paid. Companies would also need to disclose what currency they paid the ransom in, including whether the payment was made with any cryptocurrency. Companies would also have to offer "any known information regarding the identity of the actor demanding such ransom." The Ransom Disclosure Act would also require the Secretary of Homeland Security to develop penalties for non-compliance and to, one year after the passage of the bill, publish a database on a public website that includes ransom payments made in the year prior.

Trojan Discovered that Affects All Code

Virtually all compilers – programs that transform human-readable source code into computer-executable machine code – are vulnerable to an attack in which malware can introduce targeted vulnerabilities into any software without being detected, according to new research. The vulnerability disclosure was coordinated with multiple organizations, some of whom are now releasing updates to address the security weakness.

Researchers with the University of Cambridge discovered a bug that affects most computer code compilers and many software development environments. At issue is a component of the digital text encoding standard Unicode, which allows computers to exchange information regardless of the language used. Unicode currently defines more than 143,000 characters across 154 different language scripts (in addition to many non-script character sets, such as emojis).

Specifically, the weakness involves Unicode's bi-directional or "Bidi" algorithm, which handles displaying text that includes mixed scripts with different display orders, such as Arabic – which is read right to left – and English (left to right). Computer systems need to have a way of determining conflicting directionality in text. Enter the "Bidi override," which can be used to make left-to-right text read right-to-left, and vice versa. Bidi overrides enable even single-script characters to be displayed in an order different from their logical encoding.

Here's the problem: Most programming languages let you put these Bidi overrides in comments and strings. This is bad because most programming languages allow comments within which all text – including control characters – is ignored by compilers and interpreters.

"So you can use them in source code that appears innocuous to a human reviewer [that] can actually do something nasty," said a professor of computer security at Cambridge. "That's bad news for projects like Linux and Webkit that accept contributions from random people, subject them to manual review, then incorporate them into critical code. This vulnerability is, as far as I know, the first one to affect almost everything. By injecting Unicode Bidi override characters into comments and strings, an adversary can produce syntactically-valid source code in most modern languages for which the display order of characters presents logic that diverges from the real logic. In effect, we hide program A into program B." Such an attack could be challenging for a human code reviewer to detect, as the rendered source code looks perfectly acceptable.

Equally concerning is that Bidi override characters persist through the copy-and-paste functions on most modern browsers, editors, and operating systems. Any developer who copies code from an untrusted source into a protected code base may inadvertently introduce an invisible vulnerability.

The good news is that the researchers conducted a widespread vulnerability scan, but were unable to find evidence that anyone was exploiting this. Yet. The bad news is that there are no defenses to it, and now that people know about it they might start exploiting it. Researchers hope that compiler and code editor developers will patch this quickly, but realize that some developers don't update their development tools regularly there will be some risk for a while.

The Cambridge paper also contains a fascinating case study on the complexities of orchestrating vulnerability disclosure with so many affected programming languages and software firms. The researchers said they offered a 99-day embargo period following their initial disclosure to allow affected products to be repaired with software updates.

"We met a variety of responses ranging from patching commitments and bug bounties to quick dismissal and references to legal policies," the researchers wrote. "Of the nineteen software suppliers with whom we engaged, seven used an outsourced platform for receiving vulnerability disclosures, six had dedicated web portals for vulnerability disclosures, four accepted disclosures via PGP-encrypted email, and two accepted disclosures only via non-PGP email. They all confirmed receipt of our disclosure, and ultimately nine of them committed to releasing a patch."

As for what needs to be done about Trojan Source, the researchers urge governments and firms that rely on critical software to identify their suppliers' posture, exert pressure on them to implement adequate defenses, and ensure that any gaps are covered by controls elsewhere in their toolchain.

"The fact that the Trojan Source vulnerability affects almost all computer languages makes it a rare opportunity for a system-wide and ecologically valid cross-platform and cross-vendor comparison of responses," the paper concludes. "As powerful supply-chain attacks can be launched easily using these techniques, it is essential for organizations that participate in a software supply chain to implement defenses."

Security experts called the research really good work at stopping something before it becomes a problem. However, there is concern that this vulnerability has already been discovered by nation-state entities and they have biding their time waiting to use this exploit at a strategic time. In any event, the disclosure of this possible Trojan will hopefully allow developers to take corrective actions promptly and head off any attacks that might emerge.

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