SIM2K
Adapting Technology to Your Business Needs

3•22
Information you can use

SIMformation

Government Steps into Digital Currency Regs

President Joe Biden has issued an executive order outlining a host of new potential regulatory policies for cryptocurrency and digital goods. The order urges a centralization of regulatory enforcement, in an attempt to move away from the current patchwork approach, and lays out twin goals of protecting consumers and mitigating the fiscal and human costs of crypto misuse.

Cryptocurrency's major promise – the ability to securely conduct business without reliance on the financial sector – is widely viewed as a positive thing, but critics have pointed out that it's a severely underregulated market, and that crypto is all too frequently used for transactions in illegal drugs, weapons, and more.

One of the proposals in the order would see the creation of a Central Bank Digital Currency (CBDC), backed by the Federal Reserve, which has been mulling over the possibility of creating a cash-backed cryptocurrency for a number of years. The administration says that it sees several upsides to the creation of a US CBDC, including greater inclusion in the financial system (since it could potentially help the unbanked move money around) and facilitate cross-border payments.

This is a so-called "stablecoin," which has been trialed by major financial institutions like JP Morgan and Wells Fargo – it has the same portability as more typical cryptocurrencies like Bitcoin and Dogecoin, but it's indexed to the value of real-world cash, rather than subject to wild price fluctuations.
Another proposal calls for multiple agencies to provide in-depth research into the effect of new regulations designed to curtail the use of cryptocurrency for illicit purposes, as well as the potential effects on financial markets, competition policy and cybersecurity.

"Today, it can take a few days to get access to your funds. A real-time retail payments infrastructure would ensure the funds are available immediately – to pay utility bills or split the rent with roommates, or for small business owners to pay their suppliers," said a Treasury spokesman.

Immediate access to funds could be especially important for households on fixed incomes or living paycheck-to-paycheck, when waiting for funds to be available to pay a bill can mean overdraft fees or late fees that compound. Similarly, for small businesses, immediate access to funds from a sale to pay for supplies can be a game-changer, the Treasury official added. Treasury Secretary Janet Yellen said "This approach will support responsible innovation that could result in substantial benefits for the nation, consumers, and businesses."

Crypto regulation in the U.S. has suffered, according to Forrester, from a lack of centralization – the IRS treats digital assets as property to be taxed, while the SEC treats them like securities. Greater clarity will be very useful, and what is read between the lines in this order is really the encouragement for various regulators to work together, according to a Forrester spokesperson. In addition, the advent of a US-backed stablecoin could be beneficial for both consumers and businesses, giving them a new, streamlined system for payments and fund transfers.

What crypto currencies have highlighted is a global systemic problem in banking: in a world that now operates on a 24/7/365 mindset, how can business stay current when they are forced to use an 8-hour banking day? The advent of Bitcoin as a de facto currency is forcing the global banking community to realize that they are still working on an infrastructure that is hundreds of years old.

However, the contrarian view of this move to insert government into digital coinage is viewed as a move away from traditional "money" (paper, coins and checking) and to a government-controlled system where all transactions can be monitored and controlled, and appropriate taxation taken (i.e. eliminating "all cash" unreported income and barter exchanges.) This side of the argument points out that Bitcoin was created expressly to circumvent government-applied banking restrictions and therefore the administration's announcement defeats the original intent of digital currency. As one blogger stated:

> "It may well be that the federal government wants to stifle the growth of cryptocurrency before it gets even more widely adopted and influential. The fundamental value proposition of Bitcoin is that it is beyond the government's control. This isn't the case with the U.S. dollar, which the federal government can print and inflate. In many ways, the government controls the dollar and who can use it. But no government, or any central entity, can control or inflate Bitcoin. Bitcoin's independence is due to its decentralization and complicated blockchain technology. Understanding the nuances of that technology isn't important for those outside the industry, but it's just important to know that, when properly stored, Bitcoin is non-confiscatable. In other words, the government can't seize it or take it away from you. It can't ban "problematic" people from Bitcoin. It can't seize your assets if they are held in Bitcoin. Is it any wonder the federal government is moving to crack down on crypto?"

It will be interesting to see what the future of digital currency will really hold.

Firewalls Defend Against Attacks

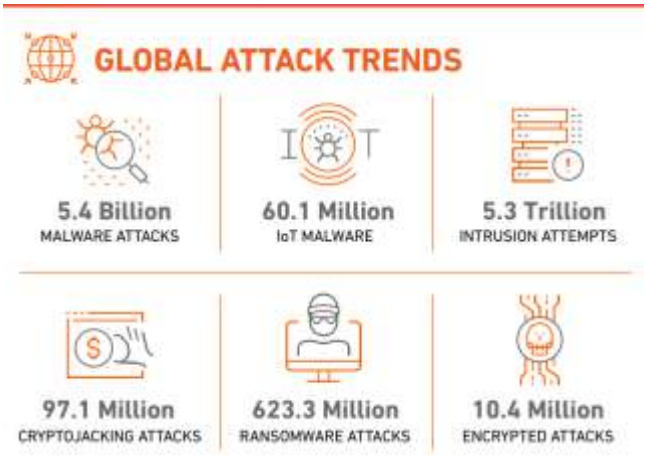
With the escalating situation in Ukraine and the increased threat of cyber attacks from Russia, its allies, as well as the countries Russia has compromised within cyberspace, it is recommended the network traffic to and from the following countries be blocked using the GeoIP filter/blocking feature on your edge devices (i.e. firewalls, proxy filters, etc.) where appropriate.

Geo-blocking traffic will help reduce your organization's overall attack surface. Furthermore, it is recommended that any additional countries with which you currently do not, or expect to have legitimate interactions with in the future, be blocked using this feature as well.

Recommended countries to block:

- Russia
- Iran
- Ukraine
- North Korea
- China
- Turkey
- Belarus
- Venezuela
- Netherlands

Below is a summary of malware attacks reported by Sonicwall, a firewall manufacturer, based on what their product has intercepted in the past year.



This shows how massive the volume of threats has been, and that this trend shows no sign of letting up as we go into 2022. In fact, Sonicwall reported a 167% spike in malware attacks just in the second half of 2021, more than 2019 and 2020 combined.

SIM2K can review your firewall settings and be sure that appropriate geo-blocking is in place. The equipment that we install is capable of this, so it is important to limit where traffic might be able to reach your network. If you don't do a lot of international business, it is a best practice to block other nations as discussed above, so please contact us and we can work with you to review and update any settings on your firewall to enhance your protection.

An "Inside Job"

The FBI has published a fresh warning about LockBit 2.0. recommending that companies enable multi-factor authentication (MFA) and use strong, unique passwords for all admin and high-value accounts to thwart the strain of ransomware that is used by one of the busiest attack groups on the internet today. MFA is vital to protecting against compromised user and admin passwords, but Microsoft has found that 78% of organizations using Azure Active Directory don't enable MFA.

LockBit's operators use any method available to compromise a network, as long as it works. These include, but are not limited to, buying access to an already compromised network from "access brokers"", exploiting unpatched software bugs, and even paying for insider access, as well as using exploits for previously unknown zero-day flaws, according to the FBI's report.

The group's techniques continue to evolve. The FBI says LockBit's operators have started advertising for insiders at a target company to help them establish initial access into the network. Insiders were promised a cut of the proceeds from a successful attack. A month earlier it began automatically encrypting devices across Windows domains by abusing group policies in Active Directory.

After compromising a network, LockBit uses multiple tools to exfiltrate data (to threaten victims with a leak if they don't pay) before encrypting files. LockBit always leaves a ransom note with instructions for how to obtain the decryption key.

Like other Russia-based ransomware operations, LockBit 2.0 determines the system and user language settings and excludes an organization from attack if the languages are one of 13 Eastern European languages. "If an Eastern European language is detected, the program exits without infection," the FBI notes.

Besides requiring strong, unique passwords and MFA for webmail, VPNs and accounts for critical systems, the FBI also recommends a series of mitigations, including keeping operating systems and software up to date and removing unnecessary access to administrative shares. It also recommends using a host-based firewall and enabling "protected files" in Windows, referring to Microsoft's controlled folder access. It also recommends that companies segment their networks, investigate any abnormal activity, implement time-based access for accounts set at the admin level and higher, disable command-line and scripting activities and permissions, and – of course – maintain offline backups of data.

Call SIM2K for assistance in implementing these protective measures on your network.

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.

Consumer Price Index Jumps

U.S. consumer prices have been rising monthly, leading to the biggest annual increase in inflation in 40 years, fueling financial markets speculation for a hefty 50 basis points interest rate hike from the Federal Reserve.

The broad increase in prices reported by the Labor Department was led by soaring costs for rents, electricity and food. High inflation, which has overshot the Fed's 2% target, could imperil the Biden economic agenda. "For the Fed, this report provides another wake-up call. Inflation is here and it continues to make its presence known everywhere," said an economist at Bank of America Securities in New York.

The consumer price index gained 0.6% last month, and food prices rose 0.9%, with the cost of food consumed at home increasing 1.0%. There were strong increases in the prices of cereals and bakery products, dairy, fruits and vegetables. Meat prices rose moderately. Electricity prices jumped 4.2%. In the 12 months through February, the CPI jumped 7.9%, the biggest year-on-year increase since February 1982.

That followed a 7.5% advance in January and marked the fifth straight month of annual increases in excess of 6%. Economists polled by Reuters had forecast the CPI rising 0.5% on month and accelerating 7.3% on a year-on-year basis. Effective with the January report, the CPI was re-weighted based on consumer expenditure data from 2019-2020. That increased the goods weight and trimmed services, accounting for some of the above-expectations increase in the CPI.

Why is this important to SIM2K? We are seeing price increases across most vendors as well, notably Microsoft and their announcement of increased pricing for Office 365 as well as other products. And, other vendors, like communications vendors, have increased pricing. And we are seeing security tools going up, not only from inflation but increased demand for these products given the Ukraine crisis and Russian and Chinese hacking threats. 2021 is a watershed year on the security front and nearly all of our clients have been impacted by the need for more tools, training and processes.

On the hardware side, SIM2K is seeing increases but especially in "high demand" items like docking stations and monitors. In looking back over past invoicing, our standard monitors are running over 20% higher than they were 5 years ago. Plus, hardware vendors are still crippled as the chip shortage still in effect.

All is not bleak – improvements to the underlying technologies are constantly being made. Locking into long term contracts is another way to combat price increases with vendors, but also risky taking on that obligation. But SIM2K is committed to seeking the best products at competitive pricing for our customers. We are sure you are seeing the impact from your business connections, and we are not immune either, but together we will work to keep the value in our relationships as these turbulent economic times continue.

"Random Tid-Bytes"

Browsers Moving Towards Consistency

Apple is working with browser developers Google, Microsoft, and Mozilla to make web design technologies more consistent no matter which browser a user relies on. The problem is that some browsers handle web technologies in different ways. This could gives rise to the adage, "When is a standard not a standard? When it's a web standard." But when it comes to developers, particularly enterprise developers attempting to create consistent web interfaces across platforms, products, and browsers, it becomes a painful friction point. It looks like browser developers have a growing understanding of this, hence the new collaboration. The aim of thise project is to try to ensure web applications based on these standards work and look the same across the myriad of different devices, platforms, and operating systems. With a little luck, one day, web developers will be able to have some confidence that the experiences they deliver are consistent to all users.

Add-On Program Sets Malware Trap

Windows 10 and 11 have built-in functions that stop malware or programs from doing harmful actions to your PC, to some extent. But Sandboxie can provide a more direct method if you need to be extra vigilant, especially if you are installing or running a program that you're not quite comfortable with. Sandboxie sets up a "sandbox" – separate from the rest of your data and programs – for that suspect program to run inside. If the program tries to run malware, or if your web browser downloads something bad, Sandboxie keeps all these harmful actions confined in the sandbox. That way, the malicious program won't mess with the normal operations of your PC, by deleting, locking up, or rewriting files. Sandboxie also places a handy shortcut on your desktop, which you can click at any time to run your default browser inside a sandbox.

Can Your PC Run Windows 11?

Over a third of devices in the enterprise today can't run Windows 11 because they don't meet Microsoft's minimum hardware requirements for the OS, according to enterprise network performance firm Riverbed. The firm's data scientists say in a new report that 34% of devices currently being used aren't capable of running Windows 11 because of Microsoft's minimum hardware requirements. However, they also found that only 12% of existing devices will need to be replaced if CIOs want them on Windows 11 while 22% of devices can be upgraded to meet the requirements. To comply with Windows 11 requirements, a PC needs at least 4GB of memory and 64GB of storage; UEFI secure boot must be enabled; the graphics card must be compatible with DirectX 12 or later, with a WDDM 2.0 driver; and a Trusted Platform Module (TPM) 2.0 must be included. On hardware upgrades, Riverbed found that 21% of machines will need an upgrade or replacement due to the TPM requirements and 15% for UEFI. Riverbed found that 19.45% of devices would need a storage upgrade, while 11% need to upgrade to TPM 2.0 and 8% will need to be upgraded with UEFI. SIM2K can evaluate your hardware for ability to be upgraded if you feel a need to move to Windows 11.

The Tech Perspective on Russia/Ukraine

The Russia invasion of its neighbor and former Soviet Union member Ukraine has drawn a broad rebuke from international leaders, along with significant protest from the Russian public. SIM2K has issued several warnings about suspected malware and other cyber risks based on government statements on increased state-sponsored attacks. Russia's assault has produced a range of cybersecurity-related risks that organizations and people will need to protect themselves against. Here are some of the ways in which Russia's invasion of Ukraine have impacted cybersecurity, and why SIM2K is urging organizations to take steps to stay safe in a continually evolving crisis.

In tandem with the physical strikes against Ukraine, a piece of wiper malware first detected by researchers at Symantec and ESET had already begun targeting organizations in Ukraine. This wiper malware has been given the name HermeticWiper and it differentiates itself from typical malware in one, important way: Those responsible for it aren't looking for any payment – they just want to do damage. Current analyses of HermeticWiper reveal that the malware is being delivered in highly-targeted attacks in Ukraine, Latvia, and Lithuania. Its operators seem to leverage vulnerabilities in external-facing servers while utilizing compromised account credentials to gain access and spread the malware further.

These tactics are nothing new, and familiar cybersecurity best practices around privileged access hold true. But here, the stakes have changed. Even in the worst-case-scenario of any ransomware attack, there's at least a promise (which could admittedly be false) of a decryption key that can be purchased for a price. With a wiper malware, there is no such opportunity.

Russia's proclivity for cyber warfare is well recorded. In the past, the country has been credibly blamed or proven responsible for several cyberattacks against Ukraine and its surrounding neighbors, including DDoS attacks in Estonia in 2007, Georgia in 2008, and Kyrgyzstan in 2009. Russia is also believed to have been responsible for an email spam campaign against Georgia in 2008, and also for the delivery of the "Snake" malware against Ukraine's government in 2014. And in 2015 and 2017, when Ukraine's power grid suffered two separate shutdowns because of the malware variants BlackEnergy and Industroyer/CrashOverride, much of the evidence reportedly pointed back to Russia. Though these attacks, like the current attacks involving HermeticWiper, were highly targeted, the idea of "tidy" cyber warfare is a farce.

In June 2017, Russia – as concluded by the CIA just months later – unleashed a cyberattack on Ukraine that spilled out into the world. The cyberattack involved a piece of malware reportedly developed by Russia's military intelligence agency the GRU, called NotPetya. Though it presented itself as a common piece of ransomware, it actually worked more like a wiper, destroying the data of its victims, which included banks, energy firms, and government officials. But the attack, which was reportedly carried out to harm Ukraine's financial system, spread out, hitting networks in Denmark, India, and the United States. It was at the time the most devastating cyberattack in history, costing the shipping company Maersk a reported $300 million, and the pharmaceutical giant Merck a reported $870 million.

As Ukraine defends itself against Russian forces, world leaders are faced with a difficult decision. Should they deliver support to Ukraine in any material way, Russia may then retaliate against them with its own cyber-attacks, and these attacks are unlikely to be borne by world leaders. Instead, the "crossfire" between national cyber-fronts will likely inflict harm on everyday individuals and businesses. Already, this decision has produced a wrinkle, as world leaders are not just defending themselves against Russia's cyber-offensive regimes, but also against known ransomware gangs that have quickly sworn allegiance to Russia's cause. Despite a clarification about an hour later, which attempted to reframe the group's "full support of Russian government" into "we do not ally with any government", there can be no doubt about the threat the group poses.

Unfortunately, the risk of escalation seems likely, as countries ramp up economic sanctions against Russia, and as the US is walking a delicate balance about its own cyber initiatives. On February 24, multiple White House officials denied, as NBC News had earlier reported, that the Biden Administration was considering multiple "options" of cyber engagement "on a scale never before contemplated." According to White House Press Secretary Jen Psaki, who wrote on Twitter, NBC's "report on cyber options being presented to @POTUS is off base and does not reflect what is actually being discussed in any shape or form."

Already, countless videos have begun circulating online that either make unproven claims or make claims that have specifically been debunked. According to recent reporting from Politico: "Russia-backed media reports falsely claiming that the Ukrainian government is conducting genocide of civilians ran unchecked and unchallenged on Twitter and on Facebook. Videos from the Russian government – including speeches from Vladimir Putin – on YouTube received dollars from Western advertisers. Unverified TikTok videos of alleged real-time battles were instead historical footage, including doctored conflict-zone images and sounds."

Users should digest any viral videos and news with caution, particularly during this conflict, as the primary aggressor has a proven history with information warfare. It is also worth remembering that during wartime even reporting from reputable sources may be based on inaccurate, incomplete or out-of-date information.

While Ukraine is in crisis, several online threat actors have continued their own assault campaigns. On February 24, multiple outlets reported that a ransomware gang was exploiting vulnerabilities in Microsoft Exchange to deliver its preferred ransomware, colloquially dubbed "Cuba." On the same day, the US Cybersecurity and Infrastructure Security Agency (CISA) announced that it had spotted "malicious cyber operations by Iranian government-sponsored advanced persistent threat (APT) actors known as MuddyWater." Those attacks were targeting both government and private-sector organizations in Asia, Africa, Europe, and North America. As CISA Director Jen Easterly warned on Twitter: "Even as we remain laser-focused on Russian malicious cyber activity, we cannot fail to see around the corners."

This conflict has raised the stakes on malware and the need to be vigilant against incursions against your network. SIM2K gets information from various cybersecurity sources and is implementing the best practices recommended to help protect you. We will continue to update you and may, from time to time, encourage you to take additional steps for increased protection on your network in light of evolving attacks that may come from state-sponsored and criminal cyberthreats.

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