Sarbanes Oxley Compliance Professionals Association (SOXCPA)
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA
Tel: 202-449-9750 Web: www.sarbanes-oxley-association.com

Sarbanes Oxley News, July 2022

Dear members and friends,

Jerome Powell, Chair of the Board of Governors of the Federal Reserve System, gave an interesting presentation at the "International Roles of the US Dollar", a research conference sponsored by the Federal Reserve Board, in Washington DC.

International Roles of the US Dollar conference

Good morning, and welcome to the inaugural conference on the International Roles of the U.S. Dollar. Thank you all for participating and for lending your expertise on this important topic. This conference marks the first use of our new Martin Conference Center, which I hope you enjoy.

The international financial and monetary system that emerged after World War II has been defined by the centrality of the dollar.

It is the world's reserve currency and the most widely used for payments and investments.

As outlined in recent work by Board staff, this global preeminence has been supported by the depth and liquidity of U.S. financial markets, the size and strength of the U.S. economy, its stability and openness to trade and capital flows, and international trust in U.S. institutions and the rule of law.

Professor Barry Eichengreen will expand on some of these themes later this morning.

The dollar's international role holds multiple benefits. For the United States, it lowers transaction fees and borrowing costs for U.S. households, businesses, and the government.

Its ubiquity helps contain uncertainty and, relatedly, the cost of hedging for domestic households and businesses. For foreign economies, the wide use of the dollar allows borrowers to have access to a broad pool of lenders and investors, which reduces their funding and transaction costs.

The benefits of the dollar as the dominant reserve currency have generated an extensive academic literature. Yesterday's paper on the Treasury market by Alexandra Tabova and Frank Warnock extends that work in meaningful ways.

The Federal Reserve's strong commitment to our price stability mandate contributes to the widespread confidence in the dollar as a store of value. To that end, my colleagues and I are acutely focused on returning inflation to our 2 percent objective.

Meeting our dual mandate also depends on maintaining financial stability. The Fed's commitment to both our dual mandate and financial stability encourages the international community to hold and use dollars.

The wide use of the dollar globally can also pose financial stability challenges that can materially affect households, businesses, and markets.

For that reason, the Federal Reserve has played a key role in promoting financial stability and supporting the use of dollars internationally through our liquidity facilities.

The central bank liquidity swap lines provide foreign central banks with the capacity to deliver U.S. dollar funding to institutions in their jurisdictions.

And the Foreign and International Monetary Authorities (FIMA) Repo Facility allows approved FIMA account holders the option to temporarily exchange their U.S. Treasury securities held by the Federal Reserve for U.S. dollars.

These facilities serve as liquidity backstops so that holders of dollar assets and participants in dollar funding markets can be confident that strains will be eased when these markets come under stress.

That assurance, in turn, mitigates the effect of such strains on the flow of credit to U.S. households and businesses. Both facilities enhance the standing of the dollar as the dominant global currency.

The swap lines were extensively used during the Global Financial Crisis, the 2011 euro-area debt crisis, and the financial turmoil at the outset of the COVID-19 pandemic in 2020.

The paper on central bank swap lines presented yesterday by Gerardo Ferrara, Philippe Mueller, Ganesh Viswanath-Natraj, and Junxuan Wang provides novel micro-level evidence on the usefulness of swap lines in providing cross-border liquidity to support the real economy.

Looking forward, rapid changes are taking place in the global monetary system that may affect the international role of the dollar in the future. Most major economies already have or are in the process of developing instant, 24/7 payments.

Our own FedNow service will be coming online in 2023. And in light of the tremendous growth in crypto-assets and stablecoins, the Federal Reserve is examining whether a U.S. central bank digital currency (CBDC) would improve on an already safe and efficient domestic payments system.

As the Fed's white paper on this topic notes, a U.S. CBDC could also potentially help maintain the dollar's international standing.

As we consider feedback from the paper, we will be thinking not just about the current state of the world, but also how the global financial system might evolve over the next 5 to 10 years.

The paper by Jiakai Chen and Asani Sarkar, which is on today's program, and our distinguished panelists on this topic this afternoon, will provide important insights on this issue.

To summarize, I would like to stress the importance of the dollar to the U.S. and global economies and financial markets. It is critical that we understand the channels, connections, and effects of the role of the dollar.

In closing, I want to thank you all for taking the time to join our discussion on the dollar's international roles. This conference brings together world-class researchers, practitioners, and policymakers dedicated to understanding and addressing these vital issues.

I look forward to their insights and I hope you enjoy the conference.

To read more: https://www.bis.org/review/r220620i.htm

Botnet Disrupted in International Cyber Operation

THE UNITED STATES ATTORNEY'S OFFICE
SOUTHERN DISTRICT of CALIFORNIA

The U.S. Department of Justice, together with law enforcement partners in Germany, the Netherlands and the United Kingdom, have dismantled the infrastructure of a Russian botnet known as RSOCKS which hacked millions of computers and other electronic devices around the world.

A botnet is a group of hacked internet-connected devices that are controlled as a group without the owner's knowledge and typically used for malicious purposes. Every device that is connected to the internet is assigned an Internet Protocol (IP) address.

According to a search warrant affidavit, unsealed today in the Southern District of California, and the operators' own claims, the RSOCKS botnet, operated by Russian cybercriminals, comprised millions of hacked devices worldwide.

The RSOCKS botnet initially targeted Internet of Things (IoT) devices. IoT devices include a broad range of devices—including industrial control systems, time clocks, routers, audio/video streaming devices, and smart garage door openers, which are connected to, and can communicate over, the internet, and therefore, are assigned IP addresses.

The RSOCKS botnet expanded into compromising additional types of devices, including Android devices and conventional computers.

"The RSOCKS botnet compromised millions of devices throughout the world," said U.S. Attorney Randy Grossman. "Cyber criminals will not escape justice regardless of where they operate. Working with public and private partners around the globe, we will relentlessly pursue them while using all the tools at our disposal to disrupt their threats and prosecute those responsible." Grossman thanked the prosecution team, the FBI and the Department of Justice Criminal Division's Computer Crimes and Intellectual Property Section for their excellent work on this case.

"This operation disrupted a highly sophisticated Russia-based cybercrime organization that conducted cyber intrusions in the United States and abroad," said FBI Special Agent in Charge Stacey Moy. "Our fight against cybercriminal platforms is a critical component in ensuring cybersecurity and safety in the United States. The actions we are announcing today are a testament to the FBI's ongoing commitment to pursuing foreign threat actors in collaboration with our international and private sector partners." A legitimate proxy service provides IP addresses to its clients for a fee. Typically, the proxy service provides access to IP addresses that it leases from internet service providers (ISPs). Rather than offer proxies that

RSOCKS had leased, the RSOCKS botnet offered its clients access to IP addresses assigned to devices that had been hacked.

The owners of these devices did not give the RSOCKS operator(s) authority to access their devices in order to use their IP addresses and route internet traffic.

A cybercriminal who wanted to utilize the RSOCKS platform could use a web browser to navigate to a web-based "storefront" (i.e., a public web site that allows users to purchase access to the botnet), which allowed the customer to pay to rent access to a pool of proxies for a specified daily, weekly, or monthly time period.

The cost for access to a pool of RSOCKS proxies ranged from $30 per day for access to 2,000 proxies to $200 per day for access to 90,000 proxies.

Once purchased, the customer could download a list of IP addresses and ports associated with one or more of the botnet's backend servers. The customer could then route malicious internet traffic through the compromised victim devices to mask or hide the true source of the traffic.

It is believed that the users of this type of proxy service were conducting large scale attacks against authentication services, also known as credential stuffing, and anonymizing themselves when accessing compromised social media accounts, or sending malicious email, such as phishing messages.

As alleged in the unsealed warrant, FBI investigators used undercover purchases to obtain access to the RSOCKS botnet in order to identify its backend infrastructure and its victims.

The initial undercover purchase in early 2017 identified approximately 325,000 compromised victim devices throughout the world with numerous devices located within San Diego County.

Through analysis of the victim devices, investigators determined that the RSOCKS botnet compromised the victim device by conducting brute force attacks.

The RSOCKS backend servers maintained a persistent connection to the compromised device. Several large public and private entities have been victims of the RSOCKS botnet, including a university, a hotel, a television studio, and an electronics manufacturer, as well as home businesses and individuals. At three of the victim locations, with consent, investigators replaced the compromised devices with government-controlled computers (i.e., honeypots), and all three were subsequently compromised by RSOCKS. The FBI identified at least six victims in San Diego.

This case was investigated by the FBI and is being prosecuted by Assistant U.S. Attorney Jonathan I. Shapiro of the Southern District of California and Ryan K.J. Dickey, Senior Counsel for the Department of Justice Criminal Division's Computer Crimes and Intellectual Property Section. The Department of Justice extends its appreciation to the authorities of Germany, the Netherlands, and the United Kingdom, the Justice Department's Office of International Affairs and private sector cybersecurity company Black Echo, LLC for their assistance provided throughout the investigation.

In September 2020, FBI Director Christopher Wray announced the FBI's new strategy for countering cyber threats. The strategy focuses on imposing risk and consequences on cyber adversaries through the FBI's unique authorities, world-class capabilities, and enduring partnerships. Victims are encouraged to report the incident online with the Internet Crime Complaint Center (IC3) www.ic3.gov

To read more: https://www.justice.gov/usao-sdca/pr/russian-botnet-disrupted-international-cyber-operation

FBI Las Vegas Federal Fact Friday:

Social Media Money Flipping Scam

The FBI Las Vegas Field Office wants to educate the public about a scam taking place using social media platforms and banking apps to solicit large sums of cash from victims.

Money Flipping

The FBI has alerted social media companies of a series of legitimate accounts being hijacked by scammers advertising unrealistic money flipping opportunities.

These scammers claim they will exponentially increase a victim's funds once provided via Cash App. These scammers will often have legitimate-looking profiles displaying strangers with large sums of cash resulting from their participation in the fraudulent investment.

How It is Implemented

Scammers contact the victim directly via private messenger, often using accounts stolen from the victim's friends.

The scammers will offer returns larger than the victim's investment at no interest and no risk.

If the victim sends money, communications are either ceased or scammers will send fake Cash App screenshots indicating the victim's money has already increased.

They then request more money with the promise of more returns that the victim will never see.

If the victim sent money or not, the scammers often suggest money is pending in the victim's Cash App account but requires replacing the email address connected to the victim's social media account with one provided by the scammers.

Once done, the scammers reset the password and take control of the account. Once they have control, the cycle continues, now against the victim's followers.

Means Of Defense

Use dual-factor authentication (DFA) when available. Though many find this inconvenient, having DFA prevents accounts from being hijacked simply by email reset. This helps prevent many forms of account hijacking and can also alert users of hijack attempts.

Do not change your account information based on outside requests. There is no legitimate reason to change your account information to that of someone else's. Cash App is not locked by social media settings and anyone that attempts to convince you otherwise is likely attempting to gain access to your information. Be cautious.

Do not click on links and verify who you're conversing with. If you are having an unusual conversation with someone on social media and they attempt to solicit money or account information, question this and give them a phone call.

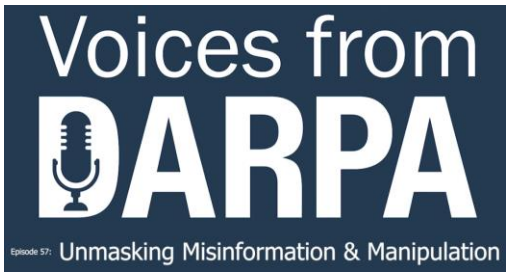
Talk to your friends live, ask questions, be skeptical, and do not click on links as they may be directing you to a malicious webpage.

Online, anyone can be anyone else. Trust, but verify. If the money transfer application has a security pin feature that requires PIN entry before authorizing a transfer, use it!

Voices from DARPA Podcast Episode 57

Unmasking Misinformation & Manipulation

In this 20-minute episode of the Voices from DARPA podcast, we discuss DARPA's Influence Campaign Awareness and Sensemaking (INCAS) program.



Adversaries exploit misinformation and true information through compelling narratives propagated on social media and online content.

INCAS seeks new tools to help analysts quickly identify geopolitical influence campaigns amidst today's noisy information environment and find better ways to determine the impacts of such propaganda.

We talk with leaders of teams working on aspects of the INCAS program – including identifying narratives using lessons from the entertainment industry and exploring how different people react to the same messages – in addition to INCAS Program Manager Brian Kettler.

As Kettler says: "Propaganda is not new, but the speed and scale of it is new. The information ecosystem is rapidly evolving. Our adversaries are getting better all the time."

You may visit: https://youtu.be/g9aoZiP48Fc

https://itunes.apple.com/us/podcast/voices-from-darpa/id1163190520

Crypto-Assets and Decentralized Finance through a Financial Stability Lens

Vice Chair Lael Brainard, At Bank of England Conference, London, UK

Recent volatility has exposed serious vulnerabilities in the crypto financial system. While touted as a fundamental break from traditional finance, the crypto financial system turns out to be susceptible to the same risks that are all too familiar from traditional finance, such as leverage, settlement, opacity, and maturity and liquidity transformation. As we work to future-proof our financial stability agenda, it is important to ensure the regulatory perimeter encompasses crypto finance.

Distinguishing Responsible Innovation from Regulatory Evasion

New technology often holds the promise of increasing competition in the financial system, reducing transaction costs and settlement times, and channeling investment to productive new uses.

But early on, new products and platforms are often fraught with risks, including fraud and manipulation, and it is important and sometimes difficult to distinguish between hype and value.

If past innovation cycles are any guide, in order for distributed ledgers, smart contracts, programmability, and digital assets to fulfill their potential to bring competition, efficiency, and speed, it will be essential to address the basic risks that beset all forms of finance.

These risks include runs, fire sales, deleveraging, interconnectedness, and contagion, along with fraud, manipulation, and evasion. In addition, it is important to be on the lookout for the possibility of new forms of risks, since many of the technological innovations underpinning the crypto ecosystem are relatively novel.

Far from stifling innovation, strong regulatory guardrails will help enable investors and developers to build a resilient digital native financial infrastructure.

Strong regulatory guardrails will help banks, payments providers, and financial technology companies (FinTechs) improve the customer experience, make settlement faster, reduce costs, and allow for rapid product improvement and customization.

We are closely monitoring recent events where risks in the system have crystallized and many crypto investors have suffered losses.

Despite significant investor losses, the crypto financial system does not yet appear to be so large or so interconnected with the traditional financial system as to pose a systemic risk.

So this is the right time to ensure that like risks are subject to like regulatory outcomes and like disclosure so as to help investors distinguish between genuine, responsible innovation and the false allure of seemingly easy returns that obscures significant risk.

This is the right time to establish which crypto activities are permissible for regulated entities and under what constraints so that spillovers to the core financial system remain well contained.

Insights from Recent Turbulence

Several important insights have emerged from the recent turbulence in the crypto-finance ecosystem.

First, volatility in financial markets has provided important information about crypto's performance as an asset class. It was already clear that crypto-assets are volatile, and we continue to see wild swings in crypto-asset values.

The price of Bitcoin has dropped by as much as 75 percent from its all-time high over the past seven months, and it has declined almost 60 percent in the three months from April through June. Most other prominent crypto-assets have experienced even steeper declines over the same period.

Contrary to claims that crypto-assets are a hedge to inflation or an uncorrelated asset class, crypto-assets have plummeted in value and have proven to be highly correlated with riskier equities and with risk appetite more generally.

Second, the Terra crash reminds us how quickly an asset that purports to maintain a stable value relative to fiat currency can become subject to a run.

The collapse of Terra and the previous failures of several other unbacked algorithmic stablecoins are reminiscent of classic runs throughout history. New technology and financial engineering cannot by themselves convert risky assets into safe ones.

Third, crypto platforms are highly vulnerable to deleveraging, fire sales, and contagion—risks that are well known from traditional finance—as

illustrated by the freeze on withdrawals at some crypto lending platforms and exchanges and the bankruptcy of a prominent crypto hedge fund. Some retail investors have found their accounts frozen and suffered large losses.

Large crypto players that used leverage to boost returns are scrambling to monetize their holdings, missing margin calls, and facing possible insolvency.

As their distress intensifies, it has become clear that the crypto ecosystem is tightly interconnected, as many smaller traders, lenders, and DeFi (decentralized finance) protocols have concentrated exposures to these big players.

Finally, we have seen how decentralized lending, which relies on overcollateralization to substitute for intermediation, can serve as a stress amplifier by creating waves of liquidations as prices fall.

Same Risk, Same Regulatory Outcome

The recent turbulence and losses among retail investors in crypto highlight the urgent need to ensure compliance with existing regulations and to fill any gaps where regulations or enforcement may need to be tailored—for instance, for decentralized protocols and platforms.

As we consider how to address the potential future financial stability risks of the evolving crypto financial system, it is important to start with strong basic regulatory foundations.

A good macroprudential framework builds on a solid foundation of microprudential regulation.

Future financial resilience will be greatly enhanced if we ensure the regulatory perimeter encompasses the crypto financial system and reflects the principle of same risk, same disclosure, same regulatory outcome.

By extending the perimeter and applying like regulatory outcomes and like transparency to like risks, it will enable regulators to more effectively address risks within crypto markets and potential risks posed by crypto markets to the broader financial system.

Strong guardrails for safety and soundness, market integrity, and investor and consumer protection will help ensure that new digital finance products, platforms, and activities are based on genuine economic value and not on regulatory evasion, which ultimately leaves investors more exposed than they may appreciate.

Due to the cross-sectoral and cross-border scope of crypto platforms, exchanges, and activities, it is important that regulators work together domestically and internationally to maintain a stable financial system and address regulatory evasion.

The same-risk-same-regulatory-outcome principle guides the Financial Stability Board's work on stablecoins, crypto-assets, and DeFi; the Basel consultation on the prudential treatment of crypto-assets; the work by the International Organization of Securities Commissions' FinTech network; the work by federal bank regulatory agencies on the appropriate treatment of crypto activities at U.S. banks; and a host of other international and domestic work.

In implementing a same-risk-same-regulatory-outcome principle, we should start by ensuring basic protections are in place for consumers and investors.

Retail users should be protected against exploitation, undisclosed conflicts of interest, and market manipulation—risks to which they are particularly vulnerable, according to a host of research. If investors lack these basic protections, these markets will be vulnerable to runs.

Second, since trading platforms play a critical role in crypto-asset markets, it is important to address noncompliance and any gaps that may exist.

We have seen crypto-trading platforms and crypto-lending firms not only engage in activities similar to those in traditional finance without comparable regulatory compliance, but also combine activities that are required to be separated in traditional financial markets.

For example, some platforms combine market infrastructure and client facilitation with risk-taking businesses like asset creation, proprietary trading, venture capital, and lending.

Third, all financial institutions, whether in traditional finance or crypto finance, must comply with the rules designed to combat money laundering and financing of terrorism and to support economic sanctions.

Platforms and exchanges should be designed in a manner that facilitates and supports compliance with these laws.

The permissionless exchange of assets and tools that obscure the source of funds not only facilitate evasion, but also increase the risk of theft, hacks, and ransom attacks.

These risks are particularly prominent in decentralized exchanges that are designed to avoid the use of intermediaries responsible for know-your-

customer identification and that may require adaptations to ensure compliance at this most foundational layer.

Finally, it is important to address any regulatory gaps and to adapt existing approaches to novel technologies. While regulatory frameworks clearly apply to DeFi activities no less than to centralized crypto activities and traditional finance, DeFi protocols may present novel challenges that may require adapting existing approaches.

The peer-to-peer nature of these activities, their automated nature, the immutability of code once deployed to the blockchain, the exercise of governance functions through tokens in decentralized autonomous organizations, the absence of validated identities, and the dispersion or obfuscation of control may make it challenging to hold intermediaries accountable.

It is not yet clear that digital native approaches, such as building in automated incentives for undertaking governance responsibilities, are adequate alternatives.

Connections to the Core Financial Institutions

There are two specific areas that merit heightened attention because of heightened risks of spillovers to the core financial system: bank involvement in crypto activities and stablecoins.

To date, crypto has not become sufficiently interconnected with the core financial system to pose broad systemic risk. But it is likely regulators will continue to face calls for supervised banking institutions to play a role in these markets.

Bank regulators will need to weigh competing considerations in assessing bank involvement in crypto activities ranging from custody to issuance to customer facilitation.

Bank involvement provides an interface where regulators have strong sightlines and can help ensure strong protections. Similarly, regulators are drawn to approaches that effectively subject the crypto intermediaries that resemble complex bank organizations to bank-like regulation.

But bringing risks from crypto into the heart of the financial system without the appropriate guardrails could increase the potential for spillovers and has uncertain implications for the stability of the system.

It is important for banks to engage with beneficial innovation and upgrade capabilities in digital finance, but until there is a strong regulatory

framework for crypto finance, bank involvement might further entrench a riskier and less compliant ecosystem.

Private Digital Currencies and Central Bank Digital Currencies

Stablecoins represent a second area with a heightened risk of spillovers. Currently, stablecoins are positioned as the digital native asset that bridges from the crypto financial system to fiat. This role is important because fiat currency is referenced as the unit of account for the crypto financial system.

Stablecoins are currently the settlement asset of choice on and across crypto platforms, often serving as collateral for lending and trading activity. As highlighted by large recent outflows from the largest stablecoin, stablecoins pegged to fiat currency are highly vulnerable to runs.

For these reasons, it is vital that stablecoins that purport to be redeemable at par in fiat currency on demand are subject to the types of prudential regulation that limit the risk of runs and payment system vulnerabilities that such private monies have exhibited historically.

Well-regulated stablecoins might bring additional competition to payments, but they introduce other risks. There is a risk of fragmentation of stablecoin networks into walled gardens.

Conversely, there is a risk that a single dominant stablecoin might emerge, given the winner-takes-all dynamics in such activities.
Indeed, the market is currently highly concentrated among three dominant stablecoins, and it risks becoming even more concentrated in the future.

The top three stablecoins account for almost 90 percent of transactions, and the top two of these account for 80 percent of market capitalization.

Given the foundational role of fiat currency, there may be an advantage for future financial stability to having a digital native form of safe central bank money—a central bank digital currency. A digital native form of safe central bank money could enhance stability by providing the neutral trusted settlement layer in the future crypto financial system.

A settlement layer with a digital native central bank money could, for instance, facilitate interoperability among well-regulated stablecoins designed for a variety of use cases and enable private-sector provision of decentralized, customized, and automated financial products.

This development would be a natural evolution of the complementarity between the public and private sectors in payments, ensuring strong public

trust in the one-for-one redeemability of commercial bank money and stablecoins for safe central bank money.

Building in Risk Management and Compliance

Crypto and fintech have introduced competition and put the focus on how innovation can help increase inclusion and address other vexing problems in finance today.

Slow and costly payments particularly affect lower-income households with precarious cash flows who rely on remittances or miss bills waiting on paychecks. Many hard-working individuals cannot obtain credit to start businesses or to respond to an emergency.

But while innovation and competition can reduce costs in finance, some costs are necessary to keep the system safe.

Intermediaries earn revenues in exchange for safely providing important services. Someone must bear the costs of evaluating risk, maintaining resources to support those risks through good times and bad, complying with laws that prevent crime and terrorism, and serving less sophisticated customers fairly and without exploitation.

In the current crypto ecosystem, often no one is bearing these costs. So when a service appears cheaper or more efficient, it is important to understand whether this benefit is due to genuine innovation or regulatory noncompliance.

So as these activities evolve, it is worth considering whether there are new ways to achieve regulatory objectives in the context of new technology. Distributed ledgers, smart contracts, and digital identities may allow new forms of risk management that shift the distribution of costs.

Perhaps in a more decentralized financial system, new approaches can be designed to make protocol developers and transaction validators accountable for ensuring financial products are safe and compliant.

Conclusion

Innovation has the potential to make financial services faster, cheaper, and more inclusive and to do so in ways that are native to the digital ecosystem.

Enabling responsible innovation to flourish will require that the regulatory perimeter encompass the crypto financial system according to the principle of like risk, like regulatory outcome, and that novel risks associated with the new technologies be appropriately addressed.

It is important that the foundations for sound regulation of the crypto financial system be established now before the crypto ecosystem becomes so large or interconnected that it might pose risks to the stability of the broader financial system.

To read more:
https://www.federalreserve.gov/newsevents/speech/brainard20220708a.htm

NIST Announces First Four Quantum-Resistant Cryptographic Algorithms

Federal agency reveals the first group of winners from its six-year competition.

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) has chosen the first group of encryption tools that are designed to withstand the assault of a future quantum computer, which could potentially crack the security used to protect privacy in the digital systems we rely on every day — such as online banking and email software.

The four selected encryption algorithms will become part of NIST's post-quantum cryptographic standard, expected to be finalized in about two years.

"Today's announcement is an important milestone in securing our sensitive data against the possibility of future cyberattacks from quantum computers," said Secretary of Commerce Gina M. Raimondo. "Thanks to NIST's expertise and commitment to cutting-edge technology, we are able to take the necessary steps to secure electronic information so U.S. businesses can continue innovating while maintaining the trust and confidence of their customers."

The announcement follows a six-year effort managed by NIST, which in 2016 called upon the world's cryptographers to devise and then vet encryption methods that could resist an attack from a future quantum computer that is more powerful than the comparatively limited machines available today. The selection constitutes the beginning of the finale of the agency's post-quantum cryptography standardization project.

"NIST constantly looks to the future to anticipate the needs of U.S. industry and society as a whole, and when they are built, quantum computers powerful enough to break present-day encryption will pose a serious threat to our information systems," said Under Secretary of Commerce for Standards and Technology and NIST Director Laurie E. Locascio. "Our post-quantum cryptography program has leveraged the top minds in cryptography — worldwide — to produce this first group of quantum-resistant algorithms that will lead to a standard and significantly increase the security of our digital information."

Four additional algorithms are under consideration for inclusion in the standard, and NIST plans to announce the finalists from that round at a future date. NIST is announcing its choices in two stages because of the need for a robust variety of defense tools.

As cryptographers have recognized from the beginning of NIST's effort, there are different systems and tasks that use encryption, and a useful standard would offer solutions designed for different situations, use varied approaches for encryption, and offer more than one algorithm for each use case in the event one proves vulnerable.

Encryption uses math to protect sensitive electronic information, including the secure websites we surf and the emails we send. Widely used public-key encryption systems, which rely on math problems that even the fastest conventional computers find intractable, ensure these websites and messages are inaccessible to unwelcome third parties.

However, a sufficiently capable quantum computer, which would be based on different technology than the conventional computers we have today, could solve these math problems quickly, defeating encryption systems. To counter this threat, the four quantum-resistant algorithms rely on math problems that both conventional and quantum computers should have difficulty solving, thereby defending privacy both now and down the road.

The algorithms are designed for two main tasks for which encryption is typically used: general encryption, used to protect information exchanged across a public network; and digital signatures, used for identity authentication. All four of the algorithms were created by experts collaborating from multiple countries and institutions.

For general encryption, used when we access secure websites, NIST has selected the CRYSTALS-Kyber algorithm. Among its advantages are comparatively small encryption keys that two parties can exchange easily, as well as its speed of operation.

For digital signatures, often used when we need to verify identities during a digital transaction or to sign a document remotely, NIST has selected the three algorithms CRYSTALS-Dilithium, FALCON and SPHINCS+ (read as "Sphincs plus").

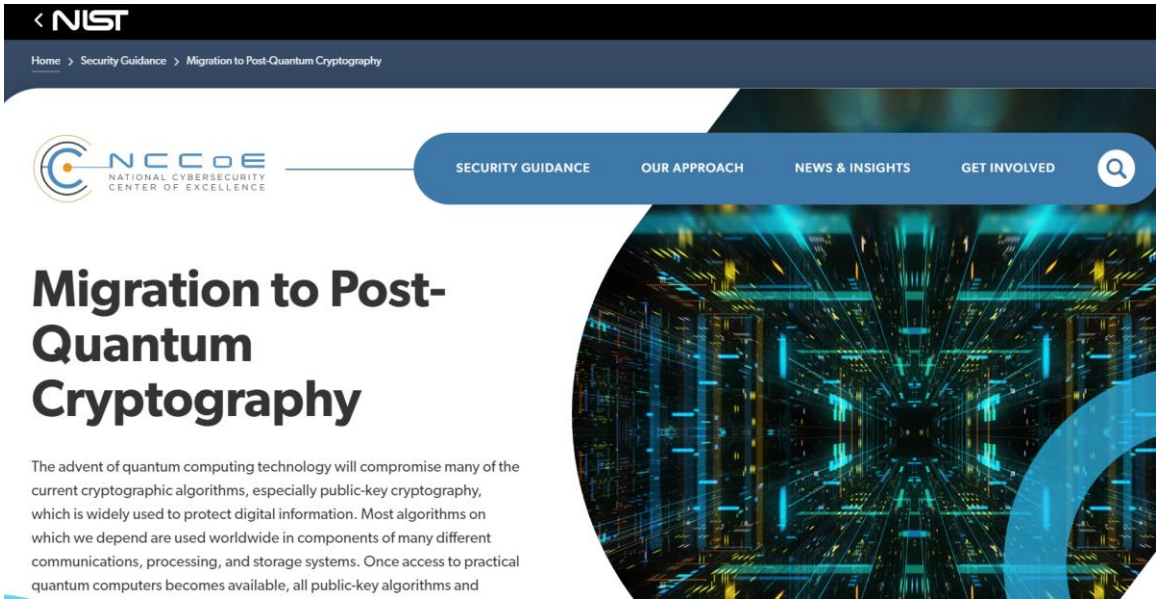
Reviewers noted the high efficiency of the first two, and NIST recommends CRYSTALS-Dilithium as the primary algorithm, with FALCON for applications that need smaller signatures than Dilithium can provide. The third, SPHINCS+, is somewhat larger and slower than the other two, but it is valuable as a backup for one chief reason: It is based on a different math approach than all three of NIST's other selections.

Three of the selected algorithms are based on a family of math problems called structured lattices, while SPHINCS+ uses hash functions. The additional four algorithms still under consideration are designed for general encryption and do not use structured lattices or hash functions in their approaches.

While the standard is in development, NIST encourages security experts to explore the new algorithms and consider how their applications will use them, but not to bake them into their systems yet, as the algorithms could change slightly before the standard is finalized.

To prepare, users can inventory their systems for applications that use public-key cryptography, which will need to be replaced before cryptographically relevant quantum computers appear.

They can also alert their IT departments and vendors about the upcoming change. To get involved in developing guidance for migrating to post-quantum cryptography, see NIST's National Cybersecurity Center of Excellence project page at: https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms



All of the algorithms are available on the NIST website at: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions

Post-Quantum Cryptography PQC

Round 3 Submissions

Official comments on the Third Round Candidate Algorithms should be submitted using the "Submit Comment" link for the appropriate algorithm. Comments from the pqc-forum Google group subscribers will also be forwarded to the pqc-forum Google group list. We will periodically post and update the comments received to the appropriate algorithm.

All relevant comments will be posted in their entirety and should not include PII information in the body of the email message.

Please refrain from using OFFICIAL COMMENT to ask administrative questions, which should be sent to pqc-comments@nist.gov

Guidelines for Submitting Tweaks for Third Round Finalists and Candidates (pdf)

To read more: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

Executive Order on Protecting Access to Reproductive Healthcare Services

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. Nearly 50 years ago, Roe v. Wade, 410 U.S. 113 (1973), articulated the United States Constitution's protection of women's fundamental right to make reproductive healthcare decisions. These deeply private decisions should not be subject to government interference. Yet today, fundamental rights — to privacy, autonomy, freedom, and equality — have been denied to millions of women across the country.

Eliminating the right recognized in Roe has already had and will continue to have devastating implications for women's health and public health more broadly. Access to reproductive healthcare services is now threatened for millions of Americans, and especially for those who live in States that are banning or severely restricting abortion care. Women's health clinics are being forced to close — including clinics that offer other preventive healthcare services such as contraception — leaving many communities without access to critical reproductive healthcare services. Women seeking abortion care — especially those in low-income, rural, and other underserved communities — now have to travel to jurisdictions where services remain legal notwithstanding the cost or risks.

In the face of this health crisis, the Federal Government is taking action to protect healthcare service delivery and promote access to critical reproductive healthcare services, including abortion. It remains the policy of my Administration to support women's right to choose and to protect and defend reproductive rights. Doing so is essential to justice, equality, and our health, safety, and progress as a Nation.

Sec. 2. Definitions. (a) The term "agency" means any authority of the United States that is an "agency" under 44 U.S.C. 3502(1), other than one considered to be an independent regulatory agency, as defined in 44 U.S.C. 3502(5).

(b) The term "reproductive healthcare services" means medical, surgical, counseling, or referral services relating to the human reproductive system, including services relating to pregnancy or the termination of a pregnancy. Sec. 3. Protecting Access to Reproductive Healthcare Services. (a) Within 30 days of the date of this order, the Secretary of Health and Human Services shall submit a report to the President:

(i) identifying potential actions:

(A) to protect and expand access to abortion care, including medication abortion; and

(B) to otherwise protect and expand access to the full range of reproductive healthcare services, including actions to enhance family planning services such as access to emergency contraception;

(ii) identifying ways to increase outreach and education about access to reproductive healthcare services, including by launching a public awareness initiative to provide timely and accurate information about such access, which shall:

(A) share information about how to obtain free or reduced cost reproductive healthcare services through Health Resources and Services Administration-Funded Health Centers, Title X clinics, and other providers; and

(B) include promoting awareness of and access to the full range of contraceptive services, as well as know-your-rights information for those seeking or providing reproductive healthcare services; and

(iii) identifying steps to ensure that all patients -- including pregnant women and those experiencing pregnancy loss, such as miscarriages and ectopic pregnancies — receive the full protections for emergency medical care afforded under the law, including by considering updates to current guidance on obligations specific to emergency conditions and stabilizing care under the Emergency Medical Treatment and Labor Act, 42 U.S.C. 1395dd, and providing data from the Department of Health and Human Services concerning implementation of these efforts.

(b) To promote access to reproductive healthcare services, the Attorney General and the Counsel to the President shall convene a meeting of private pro bono attorneys, bar associations, and public interest organizations in order to encourage lawyers to represent and assist patients, providers, and third parties lawfully seeking these services throughout the country.

Sec. 4. Protecting Privacy, Safety, and Security. (a) To address potential heightened safety and security risks related to the provision of reproductive healthcare services, the Attorney General and the Secretary of Homeland Security shall consider actions, as appropriate and consistent with applicable law, to ensure the safety of patients, providers, and third parties, and to protect the security of clinics (including mobile clinics), pharmacies,

and other entities providing, dispensing, or delivering reproductive and related healthcare services.

(b) To address the potential threat to patient privacy caused by the transfer and sale of sensitive health-related data and by digital surveillance related to reproductive healthcare services, and to protect people seeking reproductive health services from fraudulent schemes or deceptive practices:

(i) The Chair of the Federal Trade Commission (FTC) is encouraged to consider actions, as appropriate and consistent with applicable law (including the Federal Trade Commission Act, 15 U.S.C. 41 et seq.), to protect consumers' privacy when seeking information about and provision of reproductive healthcare services.

(ii) The Secretary of Health and Human Services shall consider actions, including providing guidance under the Health Insurance Portability and Accountability Act, Public Law 104-191, 110 Stat. 1936 (1996) as amended by Public Law 111-5, 123 Stat. 115 (2009), and any other statutes as appropriate, to strengthen the protection of sensitive information related to reproductive healthcare services and bolster patient-provider confidentiality.

(iii) The Secretary of Health and Human Services shall, in consultation with the Attorney General, consider actions to educate consumers on how best to protect their health privacy and limit the collection and sharing of their sensitive health-related information.

(iv) The Secretary of Health and Human Services shall, in consultation with the Attorney General and the Chair of the FTC, consider options to address deceptive or fraudulent practices related to reproductive healthcare services, including online, and to protect access to accurate information.

Sec. 5. Coordinating Implementation Efforts. (a) The Secretary of Health and Human Services and the Director of the Gender Policy Council shall establish and co-chair an Interagency Task Force on Reproductive Healthcare Access (Task Force). Additional members shall include the Attorney General and the heads of other agencies as determined by the Secretary of Health and Human Services and the Director of the Gender Policy Council. The Task Force shall work to identify and coordinate activities to protect and strengthen access to essential reproductive healthcare services. In addition, the Task Force shall coordinate Federal interagency policymaking, program development, and outreach efforts to address barriers that individuals and entities may face in seeking and providing reproductive healthcare services. The Department of Health and

Human Services shall provide funding and administrative support as may be necessary for the performance and functions of the Task Force.

(b) The Attorney General shall provide technical assistance, as appropriate and consistent with applicable law, concerning Federal constitutional protections to States seeking to afford legal protection to out-of-State patients and providers who offer legal reproductive healthcare.

Sec. 6. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

JOSEPH R. BIDEN JR.
THE WHITE HOUSE,
July 8, 2022.

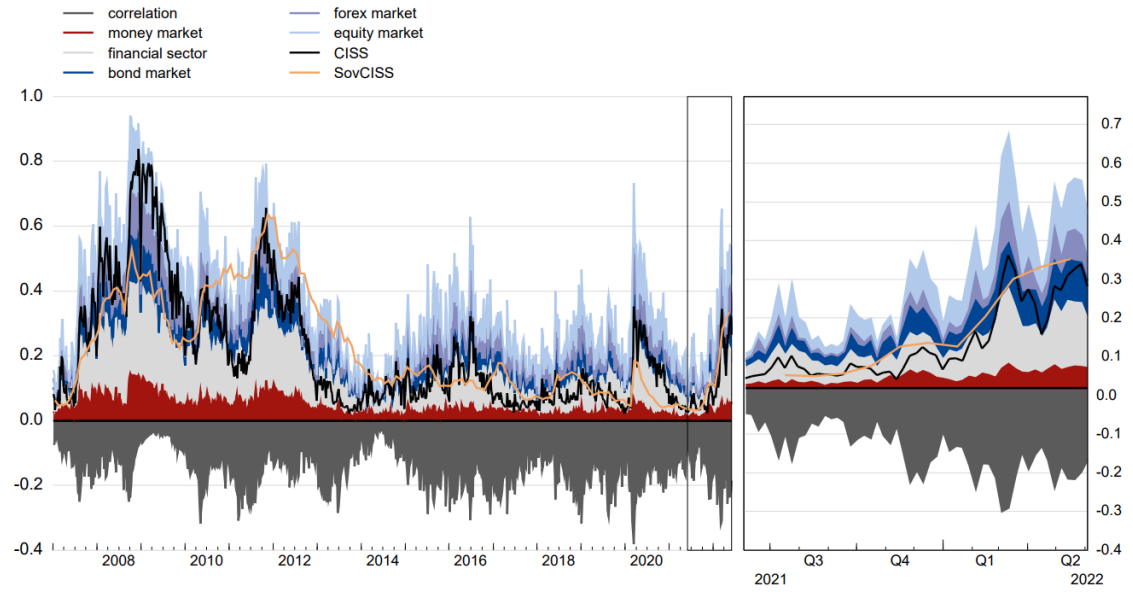
ESRB risk dashboard

ESRB European Systemic Risk Board
European System of Financial Supervision

EUROPEAN CENTRAL BANK
EUROSYSTEM

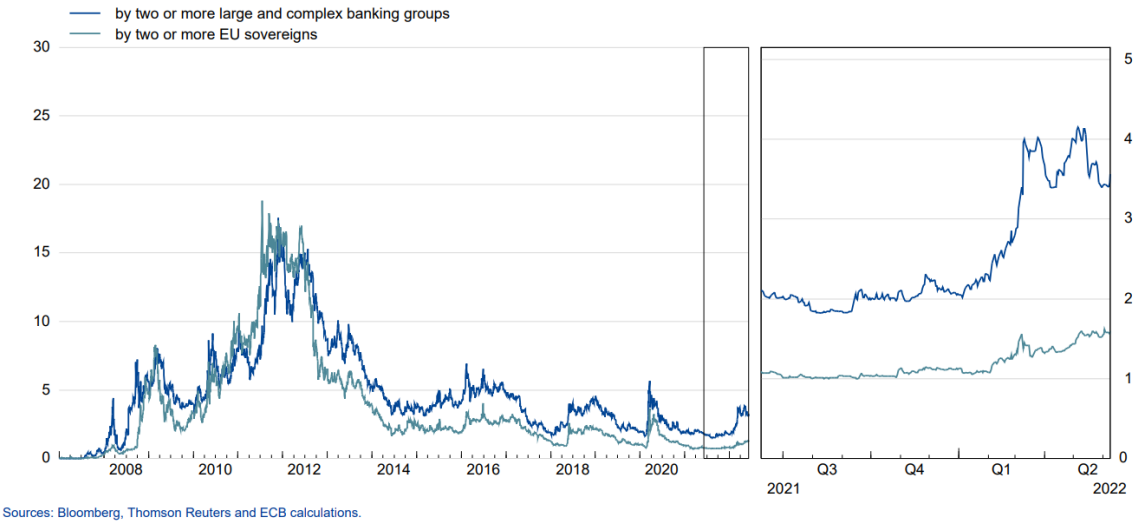
Interlinkages and composite measures of systemic risk

1.1 Composite indicator of systemic stress
(Last observation: 3 Jun. 2022)



Sources: Thomson Reuters, ECB and ECB calculations.

Probability of a simultaneous default

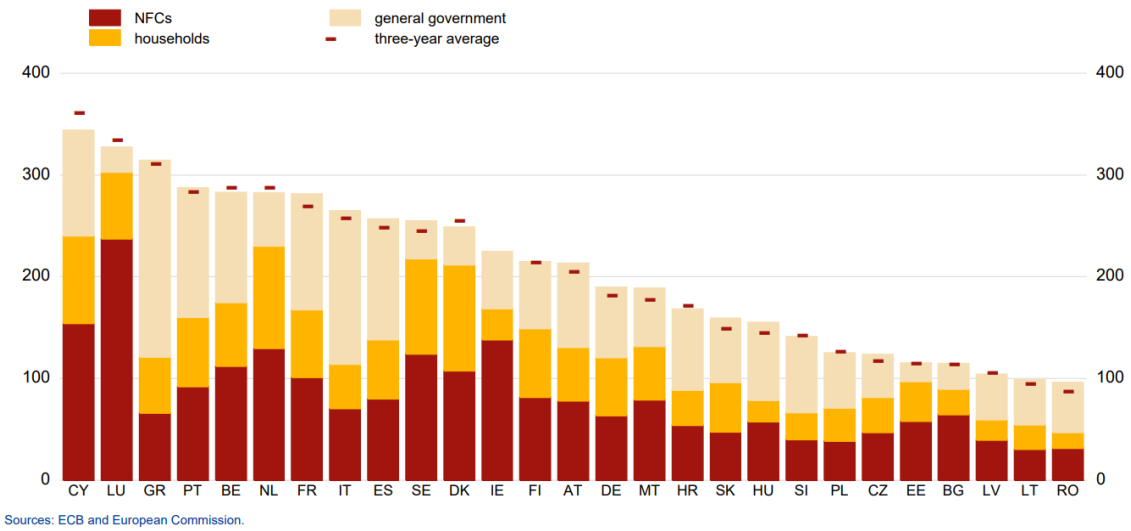


Sources: Bloomberg, Thomson Reuters and ECB calculations.

2.5 Aggregate debt-to-GDP ratio

a. Level

(EU; percentages; last observation: Q4 2021)



Sources: ECB and European Commission.

To read more:
https://www.esrb.europa.eu/pub/pdf/dashboard/20220906_rdb_external~ead8a1175c..pdf

Helping users stay safe: Blocking internet macros by default in Office (and recent developments)

Update 7/8/2022:

Following user feedback, we have rolled back this change temporarily while we make some additional changes to enhance usability. This is a temporary change, and we are fully committed to making the default change for all users.

*Regardless of the default setting, customers can block internet macros through the Group Policy settings described in **this article**.*

We will provide additional details on timeline in the upcoming weeks.

It's a challenging time in software security; migration to the modern cloud, the largest number of remote workers ever, and a global pandemic impacting staffing and supply chains all contribute to changes in organizations. Unfortunately, these changes also give bad actors opportunities to exploit organizations:

For years Microsoft Office has shipped powerful automation capabilities called active content, the most common kind are macros. While we provided a notification bar to warn users about these macros, users could still decide to enable the macros by clicking a button.

Bad actors send macros in Office files to end users who unknowingly enable them, malicious payloads are delivered, and the impact can be severe including malware, compromised identity, data loss, and remote access.

Changing Default Behavior

We're introducing a default change for five Office apps that run macros:

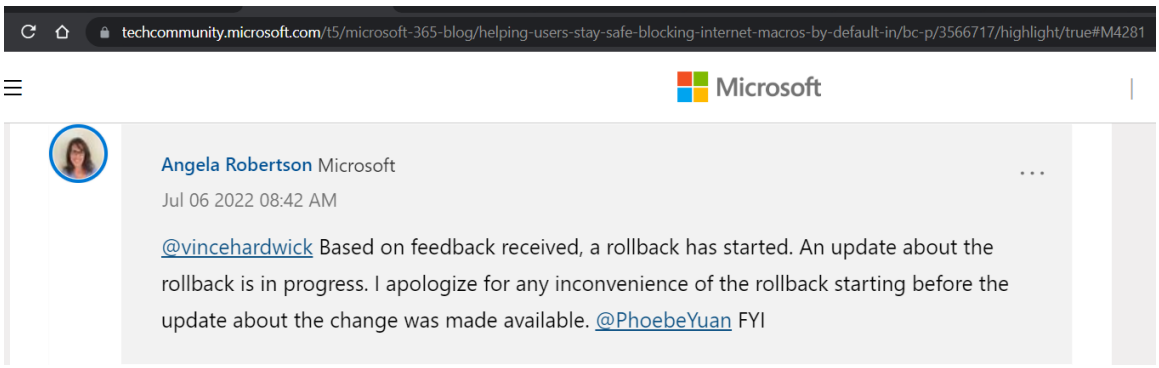
VBA macros obtained from the internet will now be blocked by default.

For macros in files obtained from the internet, users will no longer be able to enable content with a click of a button. A message bar will appear for users notifying them with a button to learn more.

The default is more secure and is expected to keep more users safe including home users and information workers in managed organizations.

This change only affects Office on devices running Windows and only affects the following applications: Access, Excel, PowerPoint, Visio, and Word. The change will begin rolling out in Version 2203, starting with Current Channel (Preview) in early April 2022. Later, the change will be available in the other update channels, such as Current Channel, Monthly Enterprise Channel, and Semi-Annual Enterprise Channel.

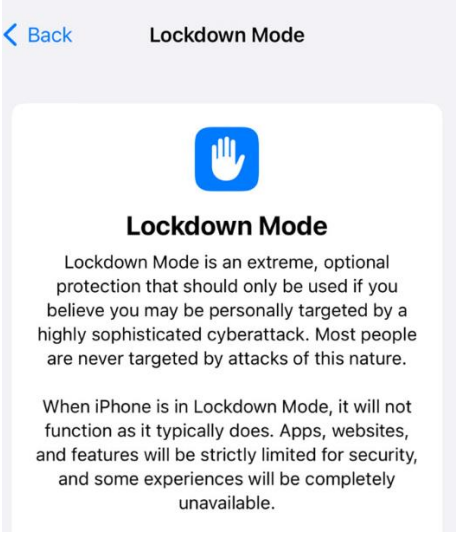
At a future date to be determined, we also plan to make this change to Office LTSC, Office 2021, Office 2019, Office 2016, and Office 2013.



To read more: https://techcommunity.microsoft.com/t5/microsoft-365-blog/helping-users-stay-safe-blocking-internet-macros-by-default-in/bc-p/3566717/highlight/true#M4281

Apple expands industry-leading commitment to protect users from highly targeted mercenary spyware

Apple is previewing a groundbreaking security capability that offers specialized additional protection to users who may be at risk of highly targeted cyberattacks from private companies developing state-sponsored mercenary spyware. Apple is also providing details of its $10 million grant to bolster research exposing such threats.



Apple detailed two initiatives to help protect users who may be personally targeted by some of the most sophisticated digital threats, such as those from private companies developing state-sponsored mercenary spyware.

Lockdown Mode — the first major capability of its kind, coming this fall with **iOS 16, iPadOS 16, and macOS Ventura** — is an extreme, optional protection for the very small number of users who face grave, targeted threats to their digital security.

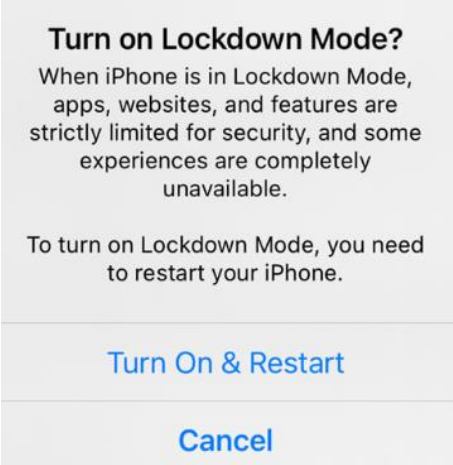
Apple also shared details about the $10 million cybersecurity grant it announced last November to support civil society organizations that conduct mercenary spyware threat research and advocacy.

“Apple makes the most secure mobile devices on the market. Lockdown Mode is a groundbreaking capability that reflects our unwavering commitment to protecting users from even the rarest, most sophisticated attacks,” said Ivan Krstić, Apple’s head of Security Engineering and Architecture. “While the vast majority of users will never be the victims of highly targeted cyberattacks, we will work tirelessly to protect the small number of users who are. That includes continuing to design defenses

specifically for these users, as well as supporting researchers and organizations around the world doing critically important work in exposing mercenary companies that create these digital attacks."

Lockdown Mode offers an extreme, optional level of security for the very few users who, because of who they are or what they do, may be personally targeted by some of the most sophisticated digital threats, such as those from NSO Group and other private companies developing state-sponsored mercenary spyware.

Turning on Lockdown Mode in iOS 16, iPadOS 16, and macOS Ventura further hardens device defenses and strictly limits certain functionalities, sharply reducing the attack surface that potentially could be exploited by highly targeted mercenary spyware.



At launch, Lockdown Mode includes the following protections:

- Messages: Most message attachment types other than images are blocked. Some features, like link previews, are disabled.

- Web browsing: Certain complex web technologies, like just-in-time (JIT) JavaScript compilation, are disabled unless the user excludes a trusted site from Lockdown Mode.

- Apple services: Incoming invitations and service requests, including FaceTime calls, are blocked if the user has not previously sent the initiator a call or request.

- Wired connections with a computer or accessory are blocked when iPhone is locked.

- Configuration profiles cannot be installed, and the device cannot enroll into mobile device management (MDM), while Lockdown Mode is turned on.

Apple will continue to strengthen Lockdown Mode and add new protections to it over time. To invite feedback and collaboration from the security research community, Apple has also established a new category within the Apple Security Bounty program to reward researchers who find Lockdown Mode bypasses and help improve its protections. Bounties are doubled for qualifying findings in Lockdown Mode, up to a maximum of $2,000,000 — the highest maximum bounty payout in the industry.

Apple is also making a $10 million grant, in addition to any damages awarded from the lawsuit filed against NSO Group, to support organizations that investigate, expose, and prevent highly targeted cyberattacks, including those created by private companies developing state-sponsored mercenary spyware.

The grant will be made to the Dignity and Justice Fund established and advised by the Ford Foundation — a private foundation dedicated to advancing equity worldwide — and designed to pool philanthropic resources to advance social justice globally. The Dignity and Justice Fund is a fiscally sponsored project of the New Venture Fund, a 501(c)(3) public charity.

“The global spyware trade targets human rights defenders, journalists, and dissidents; it facilitates violence, reinforces authoritarianism, and supports political repression,” said Lori McGlinchey, the Ford Foundation’s director of its Technology and Society program. “The Ford Foundation is proud to support this extraordinary initiative to bolster civil society research and advocacy to resist mercenary spyware. We must build on Apple’s commitment, and we invite companies and donors to join the Dignity and Justice Fund and bring additional resources to this collective fight.”

The Dignity and Justice Fund expects to make its first grants in late 2022 or early 2023, initially funding approaches to help expose mercenary spyware and protect potential targets that include:

- Building organizational capacity and increasing field coordination of new and existing civil society cybersecurity research and advocacy groups.

- Supporting the development of standardized forensic methods to detect and confirm spyware infiltration that meet evidentiary standards.

- Enabling civil society to more effectively partner with device manufacturers, software developers, commercial security firms, and other relevant companies to identify and address vulnerabilities.

- Increasing awareness among investors, journalists, and policymakers about the global mercenary spyware industry.

- Building the capacity of human rights defenders to identify and respond to spyware attacks, including security audits for organizations that face heightened threats to their networks.

To read more: https://www.apple.com/newsroom/2022/07/apple-expands-commitment-to-protect-users-from-mercenary-spyware/

FSB proposes key performance indicators for measuring progress toward the G20 cross-border payments targets

The Financial Stability Board (FSB) published for public feedback an interim report on the approach for monitoring progress toward meeting the targets for the G20 Roadmap for Enhancing Cross-border Payments.

The report provides preliminary recommendations about key performance indicators (KPIs) that could be used to monitor progress over time and identifies existing and potential sources of data for calculating those KPIs.

In October 2021, the FSB set quantitative global targets for addressing the four challenges faced by cross-border payments (cost, speed, access, transparency) as a key foundational step in the G20 Roadmap.

These targets were set for each of the three main segments of the market (wholesale, retail and remittances). The targets define the Roadmap's ambition and create accountability. However, measuring progress toward these targets will not be straightforward because no comprehensive data sources currently exist.

For the wholesale segment, the FSB views private-sector network providers as the most promising data sources for monitoring speed and access, while the use of surveys and proxies are being evaluated for monitoring progress towards meeting the transparency target.

The retail payments segment is highly varied in terms of end-users, service providers, and payment mechanisms. The FSB proposes differentiated KPIs for the various use-cases, which would allow a better understanding of how progress toward meeting the targets differs among those use-cases.

The enormous variety of end-users and payment service providers in this segment make collecting comprehensive data infeasible. The FSB is, therefore, evaluating the feasibility of collecting representative samples, for instance from private-sector data aggregators.

For the remittances segment, the public sector's long-standing goal of improving conditions in this segment has led to the establishment of multiple high-quality databases, most notably the World Bank's Remittance Prices Worldwide database and Global Findex database. The FSB is proposing to leverage these, and similar, public-sector databases to calculate KPIs.

The FSB invites feedback from the public on the preliminary proposals in this report. In particular, feedback is appreciated on the following questions:

Has the FSB identified appropriate potential sources of data for efficiently monitoring progress toward the Roadmap's targets? What, if any, additional or alternative public or private data sources should the FSB also consider and for what KPIs?

Has the FSB defined the KPIs appropriately, such that they are closely and meaningfully tied to the relevant target? What, if any, additional considerations should inform the calculation of the KPIs so that they provide sufficiently representative measurements of progress toward the targets without being overly burdensome?

The FSB is evaluating the use of proxies for monitoring progress toward some of the targets. Are the proxies proposed appropriate? What, if any, additional or alternative proxies should the FSB consider that are sufficiently representative and simplify monitoring?

The responses will help to inform the FSB's report in October 2022 to the G20 setting out further details of the implementation approach and the KPIs. Feedback should be sent to fsb@fsb.org by 31 July 2022 with the title "Monitoring progress toward cross-border payments targets".

To read more: https://www.fsb.org/2022/07/fsb-proposes-key-performance-indicators-for-measuring-progress-toward-the-g20-cross-border-payments-targets/

Countering hack-for-hire groups

Shane Huntley, Director, Threat Analysis Group

Google

As part of TAG's mission to counter serious threats to Google and our users, we've published analysis on a range of persistent threats including government-backed attackers, commercial surveillance vendors, and serious criminal operators.

Today, we're sharing intelligence on a segment of attackers we call hack-for-hire, whose niche focuses on compromising accounts and exfiltrating data as a service.

In contrast to commercial surveillance vendors, who we generally observe selling a capability for the end user to operate, hack-for-hire firms conduct attacks themselves.

They target a wide range of users and opportunistically take advantage of known security flaws when undertaking their campaigns. Both, however, enable attacks by those who would otherwise lack the capabilities to do so.

We have seen hack-for-hire groups target human rights and political activists, journalists, and other high-risk users around the world, putting their privacy, safety and security at risk. They also conduct corporate espionage, handily obscuring their clients' role.

To help users and defenders, we will provide examples of the hack-for-hire ecosystem from India, Russia, and the United Arab Emirates and context around their capabilities and persistence mechanisms.

How Hack-For-Hire Operations Work

The hack-for-hire landscape is fluid, both in how the attackers organize themselves and in the wide range of targets they pursue in a single campaign at the behest of disparate clients.

Some hack-for-hire attackers openly advertise their products and services to anyone willing to pay, while others operate more discreetly selling to a limited audience.

For example, TAG has observed Indian hack-for-hire firms work with third party private investigative services — intermediaries that reach out for services when a client requires them — and provide data exfiltrated from a successful operation.

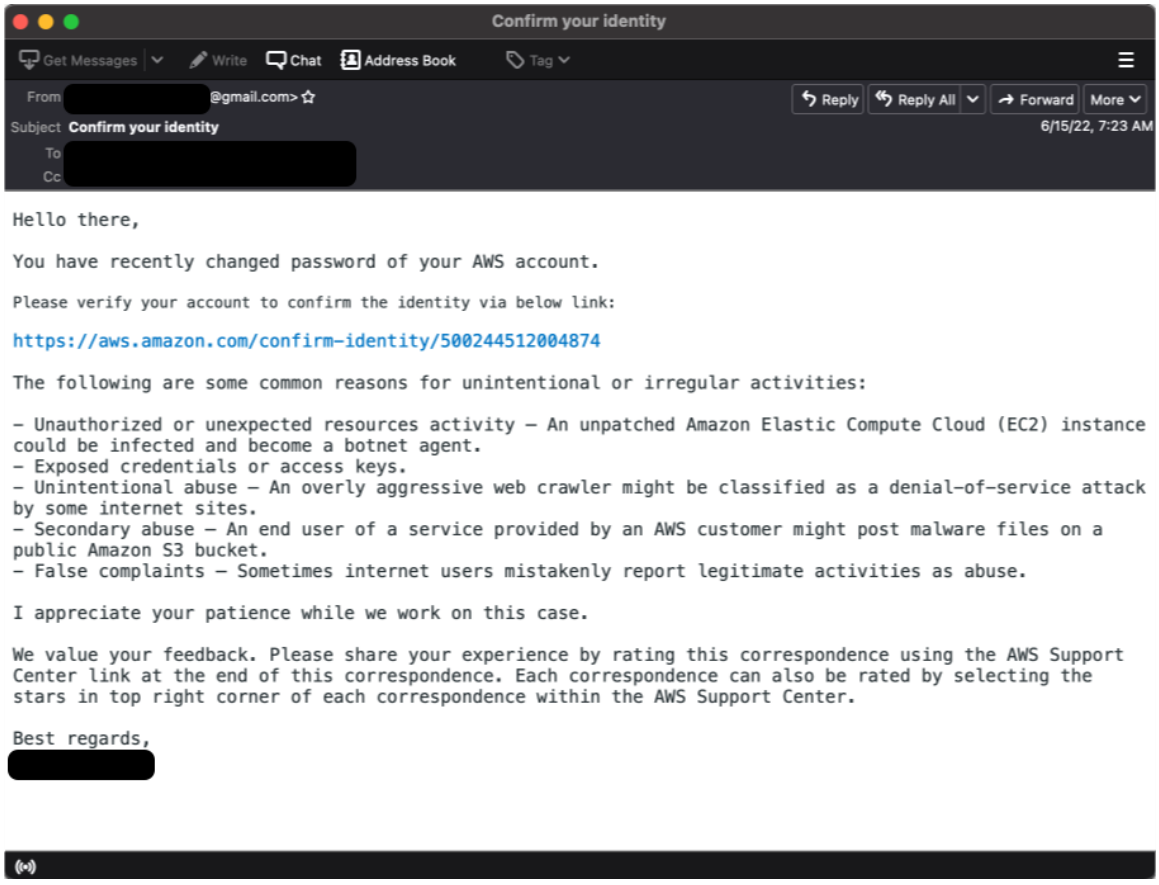
This is detailed in depth in today's Reuters investigation into the Indian hack-for-hire ecosystem. We have also observed Indian hack-for-hire firms work with freelance actors not directly employed by the firms themselves.

The breadth of targets in hack-for-hire campaigns stands in contrast to many government-backed operations, which often have a clearer delineation of mission and targets.

A recent campaign from an Indian hack-for-hire operator was observed targeting an IT company in Cyprus, an education institution in Nigeria, a fintech company in the Balkans and a shopping company in Israel.

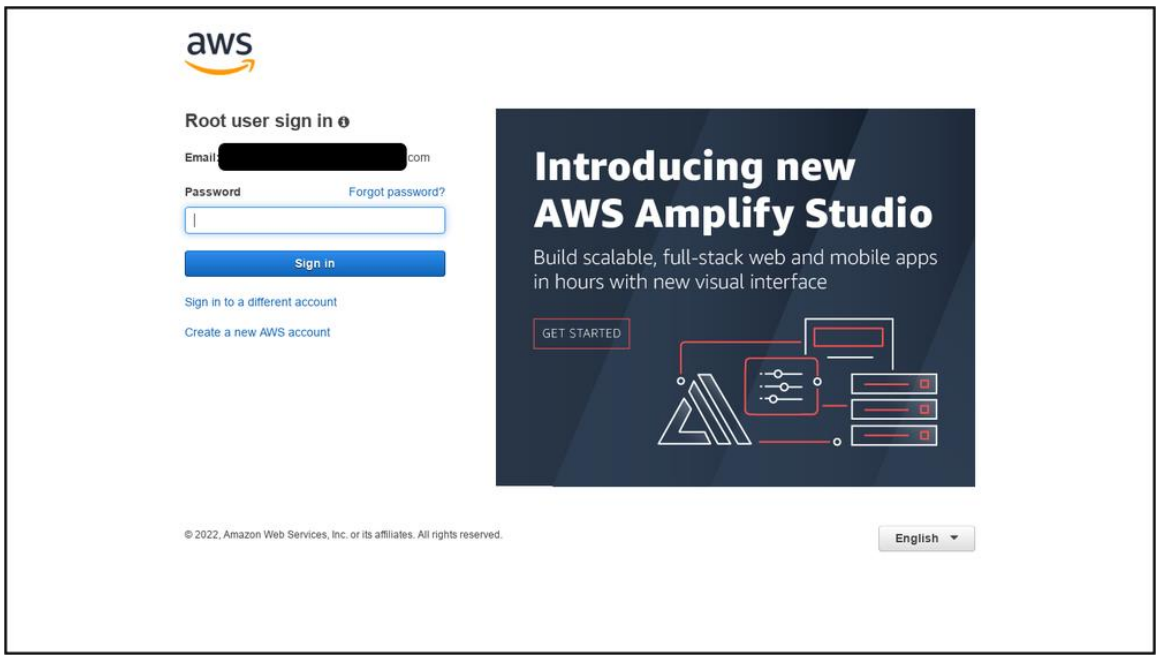
Recent Hack-for-Hire Campaigns

India

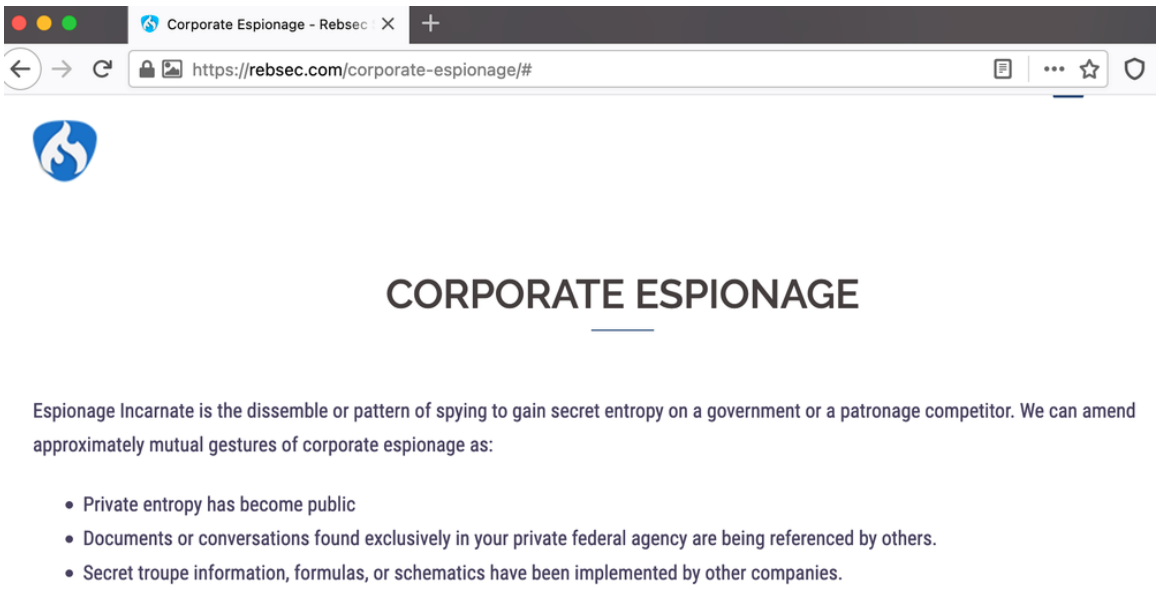


Since 2012, TAG has been tracking an interwoven set of Indian hack-for-hire actors, with many having previously worked for Indian offensive security providers Appin and Belltrox.
One cluster of this activity frequently targets government, healthcare, and telecom sectors in Saudi Arabia, the United Arab Emirates, and Bahrain with credential phishing campaigns. These credential phishing campaigns

have ranged from targeting specific government organizations to AWS accounts to Gmail accounts.



TAG has linked former employees of both Appin and Belltrox to Rebsec, a new firm that openly advertises corporate espionage as an offering on its company website.



Russia

While investigating a 2017 credential phishing campaign that targeted a prominent Russian anti-corruption journalist, we discovered the Russian attacker targeting other journalists, politicians across Europe, and various NGOs and non-profit organizations.

But what stuck out during this investigation was the breadth of targeting, which also included individuals that had no affiliation with the selected organizations, and appeared to be regular, everyday citizens in Russia and surrounding countries. This hack-for-hire actor has been publicly referred to as 'Void Balaur'.

These campaigns were similar regardless of target, consisting of a credential phishing email with a link to an attacker-controlled phishing page. The lures ranged from fake Gmail and other webmail provider notifications to messages spoofing Russian government organizations.

After the target account was compromised, the attacker generally maintained persistence by granting an OAuth token to a legitimate email application like Thunderbird or generating an App Password to access the account via IMAP. Both OAuth tokens and App Passwords are revoked when a user changes their password.

During our early investigation, TAG discovered the attacker's public website (no longer available) advertising account hacking capabilities for email and social media services. The site claimed to have received positive reviews on Russian underground forums such as Dublikat and Probiv.cc. Over the past five years, TAG has observed the group targeting accounts at major webmail providers like Gmail, Hotmail, and Yahoo! and regional webmail providers like abv.bg, mail.ru, inbox.lv, and UKR.net.

To read more: https://blog.google/threat-analysis-group/countering-hack-for-hire-groups/

Keeping PowerShell: Security Measures to Use and Embrace

Cybersecurity authorities from the United States, New Zealand, and the United Kingdom recommend proper configuration and monitoring of PowerShell, as opposed to removing or disabling PowerShell entirely.

This will provide benefits from the security capabilities PowerShell can enable while reducing the likelihood of malicious actors using it undetected after gaining access into victim networks.

The following recommendations will help defenders detect and prevent abuse by malicious cyber actors, while enabling legitimate use by administrators and defenders.

This Cybersecurity Information Sheet from the National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), the New Zealand National Cyber Security Centre (NZ NCSC), and the United Kingdom National Cyber Security Centre (NCSC-UK) provides details on using PowerShell® and its security measures.

PowerShell® is a scripting language and command line tool included with Microsoft Windows®. Similar to Bash for open-source operating systems (e.g., Linux®), PowerShell extends the user experience as an interface into the operating system.

PowerShell was introduced in Windows Vista® and has evolved with each Windows version. PowerShell can help defenders manage the Windows operating system, by:

- Enabling forensics efforts,
- Improving incident response, and
- Allowing automation of common or repetitive tasks.

In Microsoft's cloud platform Azure®, PowerShell can help to manage Azure resources, permitting administrators and defenders to build automated tools and security measures.

However, the extensibility, ease of use, and availability of PowerShell also presents an opportunity for malicious cyber actors.

Many publicly-acknowledged cyber intrusions, including those by ransomware actors, have used PowerShell as a postexploitation tool.

This technique is not new, as malicious actors often find ways to target or use legitimate system software.

The authors' recommendations mitigate cyber threats without obstructing PowerShell's functionality, which aligns to Microsoft's guidance on maintaining operational PowerShell use.

Blocking PowerShell hinders defensive capabilities that current versions of PowerShell can provide, and prevents components of the Windows operating system from running properly.

Recent versions of PowerShell with improved capabilities and options can assist defenders in countering abuse of PowerShell. The Australian Cyber Security Centre (ACSC) has also offered comprehensive configuration guidance on securing PowerShell.

To read more: https://media.defense.gov/2022/Jun/22/2003021689/-1/-1/1/CSI_KEEPING_POWERSHELL_SECURITY_MEASURES_TO_USE_AND_EMBRACE_20220622.PDF

Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;

- should not be relied on in the particular context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of an interpretative document;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors. However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

The Association accepts no responsibility with regard to such problems incurred as a result of using this site or any linked external sites.

Sarbanes-Oxley Compliance Professionals Association (SOXCPA)

Welcome to the Sarbanes-Oxley Compliance Professionals Association (SOXCPA), the largest Association of Sarbanes-Oxley professionals in the world.

Join us. Stay current. Read our monthly newsletter with news, alerts, challenges and opportunities. Get certified and provide independent evidence that you are a Sarbanes-Oxley expert.

You can explore what we offer to our members:

1. Membership - Become a standard, premium or lifetime member.

You may visit: https://www.sarbanes-oxley-association.com/How_to_become_member.htm

2. Monthly Updates - Visit the Reading Room of the SOXCPA at: https://www.sarbanes-oxley-association.com/Reading_Room.htm

3. Training and Certification - You may visit: https://www.sarbanes-oxley-association.com/Distance_Learning_and_Certification.htm

https://www.sarbanes-oxley-association.com/CJSOXE_Distance_Learning_and_Certification.htm

For instructor-led training, you may contact us. We tailor all programs to meet specific requirements.