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, May 2022

Dear members and friends,

We will start with the 2021 Annual Report of the PCAOB.

Message from the Chair

I am pleased to present this report, which summarizes our operations and financial results for the fiscal year ended December 31, 2021.

In 2021, the PCAOB faced changes and transition, including the continuing challenges of the COVID-19 pandemic, high-profile developments in the capital markets, and ongoing technological evolution in auditing.

The leadership of our organization also changed with the appointment of four new Board members in November. Amid these shifts, our organization stayed focused on performing at a high level. It did so thanks in large part to things that don't change.

The first of these constants is the PCAOB's mission. As we take steps to adapt to a changing environment, we strive to fulfill our purpose: to protect

investors and further the public interest in the preparation of informative, accurate, and independent audit reports.

The second of these constants is our extraordinary team. Guided by our mission, PCAOB staffers each day draw on their diverse backgrounds and talents to promote high-quality auditing through oversight that is both rigorous and responsive.

The PCAOB achieved a number of significant accomplishments in 2021. I look forward to working with my fellow Board members and our talented staff to build on these accomplishments as we develop and work to fulfill the organization's strategic priorities for 2022 and beyond.

Respectfully

Erica Y. Williams
Chair, Public Company Accounting Oversight Board

Driving Improvement in the Quality of Audit Services to Protect Investors

Adapting our inspection program in a shifting crisis: We designed our 2021 inspection program to respond to the effects of the COVID-19 pandemic on financial reporting and audit risks.

We adapted our program in several key ways, as discussed in two staff publications: an April 2021 Spotlight publication and a companion resource for audit committees.

First, we selected more audits for review in industries experiencing significant disruptions or elevated risks during the pandemic, such as transportation, entertainment, hospitality, manufacturing, certain aspects of the retail segment, and commercial real estate (including real estate investment trusts).

Second, we focused on certain financial statement items and other reporting matters that were affected by the pandemic, including going concern assessments, allowances for loan losses, impairments, and the increased risk of fraud.

Finally, we enhanced the unpredictability of our inspections by:

(1) significantly increasing the percentage of audits we select randomly, especially for the largest audit firms, and

(2) selecting more nontraditional financial statement focus areas (e.g., cash) for inspection.

Shedding light on recurring audit deficiencies, quality control, and good practices: As we proceeded with our 2021 inspection plan, we worked to educate auditors, audit committees, investors, and others on what we learned through our 2020 reviews of audits of public companies.

Our October 2021 Spotlight publication summarized our observations related to common or recurring deficiencies, the effectiveness of quality control systems at audit firms, good practices that can enhance audit quality, and how auditors are responding to major technological developments.

Enhancing our broker-dealer inspection information: Released in August 2021, the Board's "Annual Report on the Interim Inspection Program Related to Audits of Brokers and Dealers" came with several enhancements aimed at making this information clearer and more actionable.

These enhancements included providing more specific information in the areas of revenue and internal control over compliance, both of which continue to drive high deficiency rates in audit and examination engagements.

Enforcing compliance with our standards and rules: In 2021, our enforcement actions included sanctioning 14 firms and 15 individuals in settled matters. Our Division of Enforcement and Investigations (DEI) continued to prioritize:

(1) investigations involving significant audit violations, which typically present the greatest risks to investors,

(2) non-cooperation with PCAOB inspections and other matters threatening or eroding the integrity of the Board's regulatory oversight process, and

(3) audit matters relating to significant auditor independence violations.

DEI also focused on matters relating to deficiencies in firm quality control policies and procedures.

Maintaining our strong commitment to international cooperation: In the spring of 2021, we announced a new cooperative agreement with the Belgian Audit Oversight College and the renewal of our cooperative agreement with the Haut Conseil du Commissariat aux Comptes of France.

Allowing for cooperation in audit oversight and the exchange of confidential information in accordance with applicable law, these agreements extended the PCAOB's long track record of working cooperatively with oversight bodies outside the United States.

With these agreements in place, we have the ability to inspect and investigate all PCAOB-registered accounting firms that are located in a European country and that issue audit reports for public companies that have a reporting obligation with the SEC.

Promoting transparency and consistency in the fulfillment of the Board's HFCAA responsibilities: Following a proposal and request for comment issued in May 2021, we adopted a new rule in September 2021 related to the PCAOB's responsibilities under the Holding Foreign Companies Accountable Act (HFCAA).

The rule provides a framework for the PCAOB to use when determining, as contemplated under the HFCAA, whether the Board is unable to inspect or investigate completely registered public accounting firms located in a foreign jurisdiction because of a position taken by one or more authorities in that jurisdiction.

Following the SEC's approval of the rule in November 2021, the Board made its first HFCAA determinations in December 2021, finding that the PCAOB is unable to inspect or investigate completely registered firms headquartered in mainland China and Hong Kong.

Anticipating and Responding to the Changing Environment

Crafting new PCAOB requirements to reflect the evolving audit landscape: In 2021, we updated PCAOB rules, notably with our HFCAA rulemaking, and made progress on the items on our research and standard-setting agenda.

Our staff worked to develop a proposed standard on quality control for the Board's consideration and continued its monitoring of other areas for addition to the standard-setting agenda.

Another standard-setting initiative that advanced in 2021 was our project on lead auditors' use of other auditors. The roles of other auditors have become more significant as companies' global operations have grown.

Working with other auditors can differ from working with people in the same audit firm, creating coordination and communication challenges that can have significant implications for audit quality and investor protection.

The PCAOB has issued a proposal that would strengthen existing requirements and impose a more uniform approach to a lead auditor's supervision of other auditors.

In September 2021, we issued a supplemental request for comment seeking further public input on revisions to the proposal, with an eye towards

adopting final amendments and completing this standard-setting project in 2022.

Staying abreast of developments in data and technology: Advancements in technology continue to affect the nature, timing, and preparation of financial information, including preparers' controls around financial information, and the planning and performance of audits.

Our Office of the Chief Auditor devoted further attention to our research project on data and technology, informed in part by input from a Data and Technology Task Force, to assess whether there is a need for guidance, changes to PCAOB standards, or other regulatory actions.

In May 2021, we issued a Spotlight to share insights from our research and outreach.

Providing guidance related to the use of external audit evidence: A major technological development for both public companies and their auditors is the ever-increasing volume and availability of information from external sources such as regulatory agencies and industry data providers.

Some external sources, for example, have developed interactive applications that can provide real-time industry data to companies (e.g., hotel occupancy rates).

In October 2021, we released staff guidance on considerations regarding the relevance and reliability of information from external sources that the auditor plans to use as audit evidence.

The guidance also addresses the relationship between the quality and quantity of audit evidence.

Enhancing Transparency and Accessibility Through Proactive Engagement With Investors and Other Stakeholders

Briefing investors on international issues: In June 2021, we held an investor webinar focused on international issues, an area of significant investor interest given the global and interconnected nature of the capital markets. (In 2021, PCAOB-registered firms located outside the U.S. issued over 1,000 audit reports for companies whose securities are listed on U.S. exchanges.)

During the event, Board members and PCAOB staff briefed webinar attendees on the scale of our international oversight, the operation and coordination of our inspections of non-U.S. firms, and access challenges.

Engaging with audit committee chairs: Each year, we reach out to audit committee chairs at U.S. public companies whose audits we inspect that year, inviting them to connect with staff from our Division of Registration and Inspections for a substantive conversation covering a range of topics related to oversight of external auditors.

In 2021, more than 240 audit committee chairs accepted our invitation to talk. Highlights from this engagement are contained in a March 2022 publication, "2021 Conversations With Audit Committee Chairs".

Innovating in our stakeholder engagement: In the continuing virtual environment of 2021, we looked for ways to counter remote "fatigue" and to keep our dialogue with stakeholders engaged and dynamic. In honor of Women's History Month and International Women's Day in March 2021 — and in a first for the PCAOB — we hosted two roundtables composed entirely of women audit committee members. In addition to topics related to audit quality, the conversation covered how boards and/or companies are striving to improve diversity, as well as issues associated with record numbers of women leaving the workforce as a result of the pandemic.

Sharing our insights: As part of executing our mission and strategy, we seek continually to provide key stakeholder groups with timely resources and updates that can promote improvements in audit quality.

To that end, we were pleased in October 2021 to again host our annual Forum for Auditors of Small Businesses and Broker-Dealers.

Although still in virtual format given COVID-19 precautions, the forum provided presentations from the PCAOB and the Financial Industry Regulatory Authority.

We also provided insights through publications, such as our February 2021 summary of what we learned from the nearly 300 conversations that we had with audit committee chairs during 2020.

Exercising leadership in global engagement: An important multilateral venue for the PCAOB's global engagement is the International Forum of Independent Audit Regulators (IFIAR), an organization where PCAOB Board Members and staff play active roles.

In April 2021, Board Member Duane M. DesParte was elected IFIAR Chair for a two-year term expiring in April 2023. "IFIAR brings together audit regulators from across the globe to share experiences, knowledge and perspectives, helping to improve the effectiveness of audit oversight globally and thereby raising the bar on audit quality," said Board Member DesParte in a statement.

Bringing together academics and other key stakeholders: In 2021, we saw an increase in interest for our annual Conference on Auditing and Capital Markets, which aims to foster economic research on topics such as the economic impact of auditing and audit regulation on the capital markets.

FINANCIAL STATEMENTS

Statements of Financial Position

December 31, 2021 and 2020

($ in millions)	2021	2020
Assets		
Cash and cash equivalents	$146.0	$166.3
Restricted cash and cash equivalents	11.8	12.9
Short-term investments	17.6	-
Accounts and other receivables, net	5.9	2.3
Prepaid expenses and other assets	15.8	12.9
Furniture and equipment, leasehold improvements, and technology, net	13.1	15.2
TOTAL ASSETS	**$210.2**	**$209.6**
Liabilities and net assets without donor restrictions		
Liabilities		
Accrued payroll and related benefits	$27.4	$27.1
Accounts payable and accrued expenses	1.4	1.5
Deferred rent	18.8	20.6
Total liabilities	**47.6**	**49.2**
Net assets without donor restrictions		
Undesignated	134.5	130.6
Statutorily designated for scholarships in Section 109(c)(2) of the Sarbanes-Oxley Act	11.7	13.0
Statutorily designated for sequestration	16.4	16.8
Total net assets without donor restrictions	**162.6**	**160.4**
TOTAL LIABILITIES AND NET ASSETS WITHOUT DONOR RESTRICTIONS	**$210.2**	**$209.6**

More than 300 people attended the virtual event – a record for the PCAOB. With an audience of academics, economists, auditors, and investors, the conference focused on audit quality and quality control; the impact of the COVID-19 pandemic; trends in environmental, social, and governance reporting and assurance; and the use of technology in audits.

Supporting the next generation of leaders in accounting and auditing: The Sarbanes-Oxley Act of 2002 ("the Sarbanes-Oxley Act"), requires that funds generated from the collection of PCAOB monetary penalties be used to fund a merit scholarship program for students in accredited accounting degree programs.

In 2021, we awarded $2.53 million in scholarships to 253 students from 229 institutions, bringing the total number up to $16.23 million in scholarships offered by the PCAOB since the program's inception in 2011.

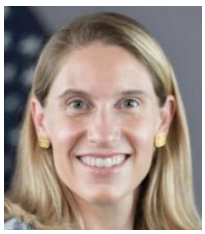
Among our 2021 PCAOB Scholars who participated in a voluntary survey, 51% self-identified as non-white, 67% identified as female, and 56% come from households with annual incomes under $48,000.

To build our rapport with these talented individuals, we invited scholarship recipients to join us for a series of online get togethers, allowing PCAOB Scholars to connect with us and each other.

To read more: https://pcaob-assets.azureedge.net/pcaob-dev/docs/default-source/about/administration/documents/annual_reports/2021-annual-report.pdf?sfvrsn=6379c829_5

Remarks at Virtual Roundtable on the Future of Going Public and Expanding Investor Opportunities: A Comparative Discussion on IPOs and the Rise of SPACs

SEC Commissioner Caroline A. Crenshaw



Thank you Hal [Scott] for that kind introduction and for inviting me to speak today. I am honored to precede such an esteemed panel of practitioners and academics. As always, I must give my standard disclaimer that my remarks are my own and do not necessarily represent the views of the Commission or its staff.

I cannot emphasize enough how important discussions such as today's are – thinking through some of the most pressing questions in our markets. And, one of those areas is Special Purpose Acquisition Companies, or SPACs.

Now, of course, this was an issue that we were paying attention to well before the notice and comment period for the SPAC rulemaking proposal. But nothing takes place in a vacuum, and the meteoric rise in SPACs and the Commission's proposed rulemaking must be considered in the context of changes in both the public and private markets.

So today's topic is particularly apt. I hope the roundtable will be one of many, and that such discussions will lead to academic work, public input, and engagement from all stakeholders and interested parties.

As you are all aware, the U.S. public markets provide many benefits, including disclosures and safeguards at the offering stage followed by periodic reporting, public trading venues that offer high degrees of liquidity, and an ecosystem of laws and regulations that provide investors with protections and remedies when needed. In 2020, 165 operating companies went public via a traditional initial public offering (IPO).

There were a total of 248 SPAC IPOs that same year, meaning roughly 60% of all IPOs were conducted through SPACs. While that level of SPAC activity may not be sustained over the long-term, it is clear SPACs provide an alternative to the traditional IPO model, and may offer some competitive challenges.

That's a good thing. But, perhaps, we need to be careful not facilitate a race to the bottom in terms of public market protections. And since the boom,

the Commission and its staff identified several areas of concern with SPACs.

Such concerns include misaligned incentives, several points of dilution that may disproportionately impact retail investors, and a lack of liability that may be creating an unjustified advantage in this path to the public markets over the traditional IPO.

The questions and challenges of how to adequately address these concerns in a balanced way remain. And I, of course, look forward to your thoughts and engagement on the SPACs proposed rulemaking.

I noted this a couple of weeks ago during prior remarks, but I think it is a point that bears repeating: there is an ongoing debate about what the right balance is between the public and private markets, and what that means for retail investors. For today's symposium, we are focused on the balance within the public markets, between the two primary paths to becoming a publicly traded company – SPACs and traditional IPOs.

However, these questions of balance within the public markets are really a part of a broader debate about the balance between public and private markets. The private markets are growing, with more companies remaining private for longer, while enjoying more access to private capital than at any time in recent memory.

I look forward to the panel, and to the future discussions and research that the panel may generate. But I would encourage the panel to contextualize their discussion about SPACs in light of the growing divide between public and private markets. I will try to do the same, as I highlight some additional observations about SPACs.

Shareholder Voting

In elections for political office, the ideal has been "one person, one vote." In corporate governance, the ideal that some cite is "one share, one vote."

The shareholder vote is meant to be a key check on management, on whom investors rely to generate returns and manage risks.

Shareholders exchange their capital for ownership shares, and depend on a board of directors and management to represent their interests in the operation and decision-making of a corporation.

Shareholders generally only vote on a few fundamental events in a corporation's life, including certain proposed mergers and acquisitions. However, shareholder ownership is often dispersed, which may diffuse the

incentives for individual investors to meaningfully participate in corporate governance, and diligence proposed mergers and acquisitions.
In SPACs, that lack of incentive to meaningfully participate in governance of the shell company and the selection of a target for de-SPAC may be especially acute.

As you know, early investors in a SPAC IPO are issued "units," which typically include redeemable shares and a fraction of a warrant. Such units are nominally priced at $10, and a full warrant entitles the shareholder to buy a share at an exercise price at a future date.

The shares and warrants usually begin trading separately after a certain period and, typically, investors may only exercise whole warrants, not fractions of warrants.

Once the SPAC sponsors identify a target for de-SPAC, there is a shareholder vote.

If a de-SPAC is approved by the requisite majority vote, shareholders have the option to hold onto their shares and become shareholders of the de-SPAC'd entity – or, they can redeem their shares.

Interestingly, the choice to redeem one's shares does not impact the ability to vote in favor of completing the de-SPAC.

So a shareholder can vote to approve the de-SPAC transaction and redeem their shares to recoup their initial investment plus any interest earned while funds were in the SPAC's trust, and retain their warrant.

In effect, a redemption but vote to approve insulates from downsides, but retains some exposure to upsides through warrants.

This seemingly eliminates the incentive for shareholders to consider whether the proposed de-SPAC is actually worthwhile, and perhaps erodes incentives for sponsors to make a thorough, well-reasoned, well-supported case for the transaction to the shareholders.

Data collected indicates that an average of 58% of SPAC IPO shareholders redeemed in 2020-2021, and reporting indicates that redemptions from the first quarter of 2022 are higher.

So what is the problem here? SPACs involve sophisticated sponsors, underwriters, shareholders, PIPE investors, and private operating companies.

Some may argue that, even if the voting mechanism is a rubber stamp, diligence of the proposed transaction still occurs at a couple of levels.

First by the sponsors and other SPAC related advisors, and then by the PIPE investors who come in at a later-stage. And the SEC has a proposal out that seeks to address these concerns.

So why am I talking about SPAC voting today? One reason is that SPACs were not always structured to allow for unlimited redemptions, and observers have noted that allowing SPACs to consummate a de-SPAC even when a substantial majority of shareholders redeems its shares creates and contributes to poor incentives, increases potential for dilution, and raises investor protection concerns.

Stock exchanges are self-regulatory organizations and gatekeepers that provide investor and corporate governance protections. As part of that gatekeeping function, the exchanges establish listing standards designed to protect financial markets and the investing public.

With regard to SPACs, one exchange formerly had listing standards that required certain redemption thresholds, or really non-redemption thresholds, to be met in order for a de-SPAC'd company to be publicly listed.

In other words, a certain amount of shareholders had to stay in order for the de-SPAC'd company to be listed as a public company.

At that time, this was industry practice, and it was codified as a listing standard.

However, that industry practice, and the listing standard that enshrined it, has changed.

While there may have been valid reasons for allowing the redemption threshold requirement to lapse, it may be appropriate to reconsider the balance of equities in light of the recent experience with SPACs, the high-rates of redemption, and a de-SPAC merger approval vote that increasingly seems pro-forma rather than an actual check that helps ensure only well-considered acquisitions proceed.

To be clear, the option to redeem is an important investor safeguard, it is one safety valve against potential misaligned incentives between sponsors and shareholders; and illiquidity in shell company shares.

The right to redeem should likely be protected. However, it is another question as to whether redeeming shareholders should retain the ability to vote to approve the de-SPAC after recouping their capital.

As the Commission's proposal notes, "cases where…the shareholders are able to vote in favor of a merger but also redeem their shares…could

present a moral hazard problem, in economic terms, because these redeeming shareholders would not bear the full cost of a less than optimal choice of target."

Further, in a scenario of high redemptions, the SPAC affiliates,[21] may still be incentivized to consummate a merger and may rely upon new PIPE investors to offer later-stage funding, potentially at the cost to those shareholders that did not redeem.

As the SEC's Office of the Investor Advocate recently noted in public recommendations, current listing standards contribute to "an inherent conflict of interest in the consummation of the SPAC's proposed business combination…permit[ing] these [de-SPACs] to occur even when assets are depleted by significant exercise of conversion rights, and early investors have economic incentives to allow deals of questionable quality to occur."

Importantly, the Investor Advocate has urged all exchanges that list SPACs to implement a conversion threshold of at least 50 percent, similar to a previous listing standard, to "ensure at least half of the outstanding shares of the SPAC" keep skin in the game.

This would help protect against a redemption of the majority of shares depleting the SPAC trust and raising the potential for dilution for those investors that do not redeem.

So as you discuss these issues today, I am curious about your thoughts. What impact do redeemable shares without limitations on conversion thresholds have on the different investors in the SPAC? And what impact does this have on the integrity of the public markets and investors' confidence in those markets?

When PIPE investors step-in to replace the financing that exits when there are high-redemptions – how does that shape the negotiations, and to what extent are remaining investors harmed by dilution because PIPE investors demand better terms? Do these combined circumstances contribute to momentum for sub-optimal or inefficient de-SPAC transactions? Further, I'm interested in understanding who the shareholders who choose not to redeem and convert their investment into the de-SPAC'd operating company are.

Do those shareholders represent a minority view that the proxy disclosures represent an outlook that outweighs the risk of non-redemption? Or are those investors remaining for other reasons?

SPACs – The Equity "Complex Product"

Investing in a SPAC IPO share is fundamentally different from investing in equity shares of publicly listed operating companies.

The optionality of the redemption, second layer of diligence about the private company that the shell company targets, and potential for dilution, among other factors, add complexities.

Calculating the potential for dilution is not straightforward and may be impacted by multiple considerations, including the amount of redemptions, the sponsor's promote, the equity overhang from warrants, and the negotiating dynamics of the PIPE investors.

As one of today's panelists recently stated, it initially took his colleagues and him eight hours to calculate dilution, which indicates the opaqueness of the dilutive effect and how difficult it may be for investors who choose not to redeem their shares to understand the extent of dilution.

A SPAC shareholder must decide whether or not to redeem, in part, given the potential for dilution and the prospects of the future de-SPAC'd company.

The Commission's proposal seeks to address concerns around dilution through enhanced disclosures, including a table showing the potential for dilution based upon percent of redemption, a requirement to disclose each material potential source of additional dilution that non-redeeming shareholders may experience, and greater information about financing arrangements.

Simply stated, SPACs are complex, and some of the purported benefits, such as a cheaper and more efficient path to the public markets for private companies, have been questioned.

Studies have found that the cost of going public via SPAC costs may actually be higher than a traditional IPO.
Indicating that a detailed understanding of the costs and benefits of this avenue to the public markets is not widely agreed upon. Hopefully, the SEC's proposal, if approved, will provide certainty and disclosure where it is needed most, but I'd be interested to hear further input on how the SEC could ameliorate these concerns. And I will continue to follow the work being done on all these questions.

SPACs & Other Paths

Practitioners, academics, and policy-makers should continue to think holistically about the public markets. As many have pointed-out, an increasing trend is that fewer companies are going public, small- and mid-sized IPOs are less frequent, and companies are staying private for longer.

Ensuring that companies, particularly small- and medium-sized companies, have adequate access to the public markets is an important policy objective. It provides investors more opportunities to diversify, more entrepreneurs access to the capital they need, and promotes market integrity and investor protections.

The recent SPAC boom raised concerns about the rigor of forward-looking statement disclosures, potential conflicts of interests, and whether adequate liability attached to the key second-phase of a SPAC, the de-SPAC. In some cases, SPACs may have elevated companies to the public markets sub-optimally.

One question I will be thinking through is whether this alternative path to the public markets provides unjustified opportunities for legal or regulatory arbitrage when compared to the traditional IPO. In other words, whether the form, an IPO through merger rather than offering, has been elevated over substance.

All of this being said, the traditional IPO process is not free from critique. While there are certain safeguards built into that process, it is well-documented that there are areas of friction and inefficiency with a traditional IPO, including high fees imposed on issuers.

As counsel to former Commissioner Robert Jackson, I worked with him on a speech about the middle-market IPO "tax," describing fees for middle-market companies to go public, which have remained stagnant at 7% for decades. We worked with one of the panelists today to revisit whether the middle-market IPO 7% fee was still observable, and found that from 2001-2016, over 96% of mid-sized IPOs had a spread of 7%.

Another area of friction in the traditional IPO is the pricing of the stock. Recent academic work has noted that "IPOs tend to be underpriced, relative to aftermarket prices, and that the underpricing phenomenon is persistent over time and across countries."

So I am also interested in understanding how we can provide competitive pressure to reduce such frictions. Whether that is through improvements to the traditional IPO or ensuring well-calibrated disclosures and investor protection safeguards are incorporated into alternative avenues such as SPACs and primary direct listings.

Finally, I encourage everyone at this symposium to think about the ever-growing divide between the public and private markets and how the paths to public markets can be improved and made more efficient while preserving key investor and market integrity protections.

Part of the underlying problem in many, if not all, discussions about public market paths such as SPACs, is that the public securities markets are declining in terms of overall market share. Increased exemptions to public offering registration requirements have put into place strong incentives to remain private for longer than ever before, and more capital is raised in the private markets than in the public markets.

But at what cost? As I noted a couple of weeks ago, the unicorn is no longer a unique or novel creature found in the woods of the private market. Rather, they have become larger and more common, with the largest unicorn valuation exceeding $400 billion.

I think we cannot have a conversation about integrity of the public markets, without acknowledging that more capital is raised in the private markets every day, and there are fewer public companies than in recent memory.

I know all of these are difficult, big, questions with no easy answers. But I also know that today's panelists, and the symposium attendees, are among the individuals that can help us answer these questions. Thank you.

To read more: https://www.sec.gov/news/speech/crenshaw-remarks-spac-symposium-042822

2021 Top Routinely Exploited Vulnerabilities

Summary

This joint Cybersecurity Advisory (CSA) was coauthored by cybersecurity authorities of the *United States, Australia, Canada, New Zealand, and the United Kingdom:* the Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), New Zealand National Cyber Security Centre (NZ NCSC), and United Kingdom's National Cyber Security Centre (NCSC-UK).

This advisory provides details on the top 15 Common Vulnerabilities and Exposures (CVEs) routinely exploited by malicious cyber actors in 2021, as well as other CVEs frequently exploited.

U.S., Australian, Canadian, New Zealand, and UK cybersecurity authorities assess, in 2021, malicious cyber actors aggressively targeted newly disclosed critical software vulnerabilities against broad target sets, including public and private sector organizations worldwide. To a lesser extent, malicious cyber actors continued to exploit publicly known, dated software vulnerabilities across a broad spectrum of targets.

The cybersecurity authorities encourage organizations to apply the recommendations in the Mitigations section of this CSA. These mitigations include applying timely patches to systems and implementing a centralized patch management system to reduce the risk of compromise by malicious cyber actors.

Top 15 Routinely Exploited Vulnerabilities

CVE-2021-44228. This vulnerability, known as **Log4Shell**, affects Apache's Log4j library, an open-source logging framework. An actor can exploit this vulnerability by submitting a specially crafted request to a vulnerable system that causes that system to execute arbitrary code. The request allows a cyber actor to take full control over the system.

The actor can then steal information, launch ransomware, or conduct other malicious activity. Log4j is incorporated into thousands of products worldwide. This vulnerability was disclosed in December 2021; the rapid widespread exploitation of this vulnerability demonstrates the ability of malicious actors to quickly weaponize known vulnerabilities and target organizations before they patch.

CVE-2021-26855, CVE-2021-26858, CVE-2021-26857, CVE-2021-27065. These vulnerabilities, known as **ProxyLogon**, affect Microsoft Exchange email servers. Successful exploitation of these vulnerabilities in combination (i.e., "vulnerability chaining") allows an unauthenticated cyber actor to execute arbitrary code on vulnerable Exchange Servers, which, in turn, enables the actor to gain persistent access to files and mailboxes on the servers, as well as to credentials stored on the servers.

Successful exploitation may additionally enable the cyber actor to compromise trust and identity in a vulnerable network.

CVE-2021-34523, CVE-2021-34473, CVE-2021-31207. These vulnerabilities, known as **ProxyShell,** also affect Microsoft Exchange email servers.

Successful exploitation of these vulnerabilities in combination enables a remote actor to execute arbitrary code. These vulnerabilities reside within the Microsoft Client Access Service (CAS), which typically runs on port 443 in Microsoft Internet Information Services (IIS) (e.g., Microsoft's web server).

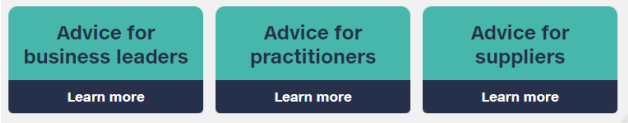
CAS is commonly exposed to the internet to enable users to access their email via mobile devices and web browsers.

CVE-2021-26084. This vulnerability, affecting Atlassian Confluence Server and Data Center, could enable an unauthenticated actor to execute arbitrary code on vulnerable systems. This vulnerability quickly became one of the most routinely exploited vulnerabilities after a POC was released within a week of its disclosure. Attempted mass exploitation of this vulnerability was observed in September 2021.

Download the Joint Cybersecurity Advisory: 2021 top Routinely Exploited Vulnerabilities at:
https://www.cisa.gov/uscert/sites/default/files/publications/AA22-117A_Joint_CSA_2021_Top_Routinely_Exploited_Vulnerabilities_Final.pdf

Supply Chain Guidance

CPNI
Centre for the Protection of National Infrastructure



Overview

Your supply chain exposes you to damaging security threats. Certain states could target you via your supply chain for their economic, political, or military gain because:

1. Your suppliers have weaker security measures in place so are easier to attack; or

2. One of your suppliers serves various organisations of interest, so targeting that supplier gives them access to several targets via a single attack

Supply chain attacks can result in the compromise of entire organisations and pose a potentially terminal risk to businesses. Hostile actors are looking for vulnerabilities in organisations of every size across a broad range of sectors.

Supply chains are not just compromised by cyber-attacks.

An insider can provide damaging access and insight, or organisations could be unwittingly handing over parts of their business to a state-controlled organisation through offshoring or foreign direct investment in their suppliers.

By giving suppliers access to information without setting expectations about how it should be protected, you are exposing your business to a range of security threats.

Act now to develop your supply chain security, avoid business disruption, and protect your business.

Governance

Implement strong and clear governance that cascades from the top downwards and ensures you are protecting your organisation as much as possible.

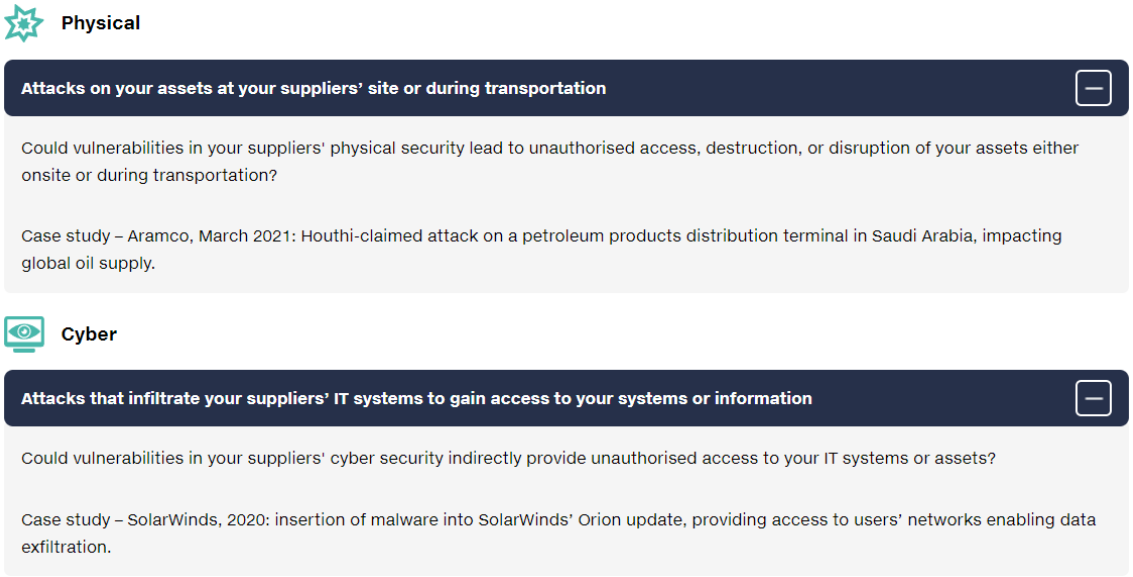
- Appoint a senior lead to take responsibility for supply chain security. Integrate procurement teams into the security management process, alongside those responsible for physical, personnel and information security. Representation from teams with the tools to defend your business from both direct and indirect attacks will ensure you have holistic protection from malicious threats. Ensure supply chain risks are captured on your organisation's risk register

- Ensure senior-level visibility of the security of your procurement processes and supply chain. This should include visibility of high-risk suppliers, and those with access to sensitive information or systems

- Create a clear policy to help staff identify and highlight high-risk suppliers and procurement activities to senior leaders. Regularly review all security policies and procedures with a clearly identified lead to take responsibility for them. Develop a strong security culture across your organisation

Threats

Attacks on your supply chain security can come from a range of sources. Ensure you are aware of the variety of potential attacks.



Insider

Attacks by your suppliers' employees or sub-contractors to gain access to your assets or systems

What access do your suppliers' employees have to your assets, and what level of personnel security checks are in place to detect and disrupt insider threats?

Scenario: Company A holds sensitive commercial data regarding a technology with military and civilian applications. A subcontractor of Company A downloads the data and sells it to competitors in the defence sector of another state.

Geographical

Foreign state access to your information due to the location of your suppliers' business or operations

Do you understand the laws by which suppliers' outside the UK might be bound regarding access and storage of your assets?

Scenario: Company A holds sensitive data in a data centre owned by Company B. Company B decides to relocate the data to a data centre in Country X, which is then able to access that data.

International suppliers' must comply with their home country's laws. Ensure your processes and oversight consider the local legal frameworks in which international organisations operate. This could include laws and regulations that require organisations to share information and data with their state. Take this into account when considering offshoring.

Hostile ownership

Foreign ownership, control, or influence over part of your supply chain

Could suppliers' owned, controlled or influenced by a foreign state lead to unintended exposure of your assets?

Scenario: Law Firm A holds sensitive data as part of due diligence for early stage investment by VC Company B. Law Firm A is purchased by an entity in Country X, offering potential access to that data by Country X.

Technology

Dependencies on technologies with inherent vulnerabilities

Could you be exposing your critical assets by relying on technology with inherent vulnerabilities that could be exploited by hostile actors?

Scenario: a range of sensitive sites procure CCTV equipment with a cloud-based recording capability run from servers in Country X, which requires any company within its jurisdiction to provide access to all data and communications.

Exposure

If a future supplier is compromised, how much damage would they be able to inflict?

- Will they have access to commercially sensitive information that could undermine your commercial success?
- Will they have access to your organisation's IT systems and sensitive information?
- How easily would you be able to detect a compromise of the supplier?

- Would a compromise be easily detected and acted upon, or if unnoticed could it be exploited over a significant period?

Consider how to reduce unnecessary or high-risk sharing of sensitive data or access to sensitive systems.

- Eliminate - If a specific activity you planned to outsource provides suppliers with an unacceptable level of access to business-critical assets, deliver the activity in-house

- Mitigate - If a specific activity you planned to outsource exposes more of your business-critical assets than you are comfortable with, reduce the assets shared to minimise your exposure

- Accept - In some circumstances, businesses may find it difficult to set security expectations for suppliers that dominate the market. You should still embed as much security as possible across your procurement processes

To read more: https://www.cpni.gov.uk/protected-procurement-business-leaders

SEC Nearly Doubles Size of Enforcement's Crypto Assets and Cyber Unit

The Securities and Exchange Commission announced the allocation of 20 additional positions to the unit responsible for protecting investors in crypto markets and from cyber-related threats.

The newly renamed Crypto Assets and Cyber Unit (formerly known as the Cyber Unit) in the Division of Enforcement will grow to 50 dedicated positions.

"The U.S. has the greatest capital markets because investors have faith in them, and as more investors access the crypto markets, it is increasingly important to dedicate more resources to protecting them," said SEC Chair Gary Gensler. "The Division of Enforcement's Crypto Assets and Cyber Unit has successfully brought dozens of cases against those seeking to take advantage of investors in crypto markets. By nearly doubling the size of this key unit, the SEC will be better equipped to police wrongdoing in the crypto markets while continuing to identify disclosure and controls issues with respect to cybersecurity."

Since its creation in 2017, the unit has brought more than 80 enforcement actions related to fraudulent and unregistered crypto asset offerings and platforms, resulting in monetary relief totaling more than $2 billion.

The expanded Crypto Assets and Cyber Unit will leverage the agency's expertise to ensure investors are protected in the crypto markets, with a focus on investigating securities law violations related to:

- Crypto asset offerings;
- Crypto asset exchanges;
- Crypto asset lending and staking products;
- Decentralized finance ("DeFi") platforms;
- Non-fungible tokens ("NFTs"); and
- Stablecoins.

In addition, the unit has brought numerous actions against SEC registrants and public companies for failing to maintain adequate cybersecurity controls and for failing to appropriately disclose cyber-related risks and incidents.

The Crypto Assets and Cyber Unit will continue to tackle the omnipresent cyber-related threats to the nation's markets.

"Crypto markets have exploded in recent years, with retail investors bearing the brunt of abuses in this space. Meanwhile, cyber-related threats continue to pose existential risks to our financial markets and participants," said Gurbir S. Grewal, Director of the SEC's Division of Enforcement. "The bolstered Crypto Assets and Cyber Unit will be at the forefront of protecting investors and ensuring fair and orderly markets in the face of these critical challenges."

The infusion of 20 additional positions into the Crypto Assets and Cyber Unit will bolster the ranks of its supervisors, investigative staff attorneys, trial counsels, and fraud analysts in the agency's headquarters in Washington, DC, as well as several regional offices.

To read more: https://www.sec.gov/news/press-release/2022-78

U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned virtual currency mixer Blender.io (Blender), which is used by the Democratic People's Republic of Korea (DPRK) to support its malicious cyber activities and money-laundering of stolen virtual currency.

On March 23, 2022, Lazarus Group, a DPRK state-sponsored cyber hacking group, carried out the largest virtual currency heist to date, worth almost $620 million, from a blockchain project linked to the online game Axie Infinity; Blender was used in processing over $20.5 million of the illicit proceeds.

Under the pressure of robust U.S. and UN sanctions, the DPRK has resorted to illicit activities, including cyber-enabled heists from cryptocurrency exchanges and financial institutions, to generate revenue for its unlawful weapons of mass destruction (WMD) and ballistic missile programs.

"Today, for the first time ever, Treasury is sanctioning a virtual currency mixer," said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson. "Virtual currency mixers that assist illicit transactions pose a threat to U.S. national security interests. We are taking action against illicit financial activity by the DPRK and will not allow state-sponsored thievery and its money-laundering enablers to go unanswered."

Treasury is also updating the List of Specially Designated Nationals and Blocked Persons (SDN List) to identify additional virtual currency addresses used by the Lazarus Group to launder illicit proceeds.

Treasury is committed to exposing components of the virtual currency ecosystem, like Blender, that are critical to the obfuscation of the trail of stolen proceeds from illicit cyber activity.

OFAC sanctioned the Lazarus Group on September 13, 2019, pursuant to Executive Order (E.O.) 13722, and identified it as an agency, instrumentality, or controlled entity of the Government of the DPRK, based on its relationship to the U.S.- and UN-designated Reconnaissance General Bureau, the DPRK's premiere intelligence organization, which is also involved in conventional arms trade.

Blender.io (Blender) is a virtual currency mixer that operates on the Bitcoin blockchain and indiscriminately facilitates illicit transactions by obfuscating their origin, destination, and counterparties.

Blender receives a variety of transactions and mixes them together before transmitting them to their ultimate destinations. While the purported purpose is to increase privacy, mixers like Blender are commonly used by illicit actors.

Blender has helped transfer more than $500 million worth of Bitcoin since its creation in 2017. Blender was used in the laundering process for DPRK's Axie Infinity heist, processing over $20.5 million in illicit proceeds.

OFAC's investigation also identified Blender's facilitation of money-laundering for, among others, Russian-linked malign ransomware groups including Trickbot, Conti, Ryuk, Sodinokibi, and Gandcrab.

Blender is being designated pursuant to E.O. 13694, as amended, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, a cyber-enabled activity originating from, or directed by persons located, in whole or in substantial part, outside the United States that is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that has the purpose or effect of causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.

While most virtual currency activity is licit, it can be used for illicit activity, including sanctions evasion, through mixers, peer-to-peer exchangers, darknet markets, and exchanges. This includes the facilitation of heists, ransomware schemes, and other cybercrimes.

Treasury continues to use its authorities against malicious cyber actors in concert with other U.S. departments and agencies, as well as our foreign partners, to disrupt financial nodes tied to illicit payments and cyber-attacks.

Those in the virtual currency industry play a critical role in implementing appropriate Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) and sanctions controls to prevent sanctioned persons and other illicit actors from exploiting virtual currency to undermine U.S foreign policy and national security interests.

The virtual currency mixers that assist criminals are a threat to U.S. national security interests. Treasury will continue to investigate the use of

mixers for illicit purposes and consider the range of authorities Treasury has to respond to illicit financing risks in the virtual currency ecosystem.

For example, in 2020, Treasury's Financial Crime Enforcement Network (FinCEN) assessed a $60 million civil money penalty against the owner and operator of a virtual currency mixer for violations of the Bank Secrecy Act (BSA) and its implementing regulations. You may visit: https://www.fincen.gov/sites/default/files/enforcement_action/2020-10-19/HarmonHelix%20Assessment%20and%20SoF_508_101920.pdf

UNITED STATES OF AMERICA
FINANCIAL CRIMES ENFORCEMENT NETWORK
DEPARTMENT OF THE TREASURY

IN THE MATTER OF:	)	
	)	
	)	Number 2020-2
Larry Dean Harmon	)	
d/b/a Helix	)	
	)	
Akron, Ohio	)	

ASSESSMENT OF CIVIL MONEY PENALTY

I. INTRODUCTION

The Financial Crimes Enforcement Network (FinCEN) has determined that grounds exist to assess a civil money penalty against Larry Dean Harmon, as the primary operator of Helix, and as the Chief Executive Officer (CEO) and primary operator of Coin Ninja LLC (Coin Ninja), pursuant to the Bank Secrecy Act (BSA) and regulations issued pursuant to that Act.[1]

Criminals have increased use of anonymity-enhancing technologies, including mixers, to help hide the movement or origin of funds. Additional information on illicit financing risks associated with mixers and other anonymity-enhancing technologies in the virtual asset ecosystem can be found in the 2022 National Money Laundering Risk Assessment. You may visit: https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf

National Money Laundering Risk Assessment

ADDITIONAL LAZARUS GROUP WALLET

OFAC is identifying four additional virtual currency wallet addresses used by the Lazarus Group to launder the remainder of stolen proceeds from the

March 2022 Axie Infinity heist. This builds upon OFAC's April 14, 2022, attribution of DPRK's Lazarus Group as the perpetrators of the Axie Infinity heist and identification of the original getaway wallet address. Treasury is committed to tracing illicit virtual currency and blocking associated wallets and addresses wherever found.

SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the entity above, Blender.io, that is in the United States or in the possession or control of U.S. persons is blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, 50 percent or more by one or more blocked persons are also blocked.

All transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of designated or otherwise blocked persons are prohibited unless authorized by a general or specific license issued by OFAC, or exempt. These prohibitions include the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any blocked person and the receipt of any contribution or provision of funds, goods, or services from any such person.

For identifying information on the entity sanctioned: https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220506

For information on complying with virtual currency sanctions, see OFAC's Sanctions Compliance Guidance for the Virtual Currency Industry at: https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf

Remarks at Securities Enforcement Forum West 2022

Gurbir S. Grewal, Director, SEC Division of Enforcement

Good afternoon everyone.

Thank you to Bruce Carton for the invitation to speak today and to Professor Joe Grundfest for the very kind introduction.

As is customary, my remarks today express my views, and don't necessarily reflect those of the Commission, the Commissioners, or other members of staff.

Ordinarily at an event like this one, I'd speak about all that ways in which we are working to protect investors, including our increased focus on the private fund space, the additional resources we've committed to our Crypto Assets and Cyber Unit, and other enforcement priorities.

And I'd likely close by reassuring each of you in the defense bar that we're not doing away with the White Paper and Wells processes, but rather streamlining them. But I'd like to take a different approach today given some recent experiences and observations.

An animating principle for me in this role has been to increase public confidence in our markets and in government—to counter the declining trust in our institutions that we are experiencing.

There is a perception among large segments of the population that corporate wrongdoers are not being held accountable and that there are two sets of rules: one for the big and powerful and another for everyone else. While there are many reasons for these beliefs and trends, delayed accountability does not help.

That's why, since day one, I've been asking staff to look for ways in which to push the pace of our investigations. The public needs to know when they read a news story about corporate malfeasance that we will move quickly to investigate what happened and hold wrongdoers accountable, even in the most complex cases. You saw an example of that recently in our actions against Archegos Capital Management, its founder Bill Hwang, and others.

But one thing I hear frequently from staff is how the conduct of defense counsel in some cases frustrates and delays our truth-seeking mission. For

example, I recently learned about a document production in an investigation concerning an entity with billions in assets that it would be overly generous to refer to as a rolling production.

Despite our best efforts, we've received a little over 200 documents over the course of the last six months, including a single page recently produced in response to requests for U.S. customer account and trading data. One page. Needless to say, that makes it difficult for us to assess whether there's been a violation of the securities laws.

None of this is new. About a decade ago, one of my predecessors—Rob Khuzami—gave a speech about questionable behavior by defense counsel in SEC investigations.

From slow-rolling document productions as I just described—to representing multiple witnesses with adverse interests in the same matter—to kicking witnesses during testimony to get them to answer questions a certain way, Director Khuzami catalogued many ways in which defense counsel undermined the SEC's investigative process.

Unfortunately ten years on from that speech, we continue to see some of these behaviors, as well as newer forms of the same tactics. In other words, while defense counsel may have stopped kicking witnesses under the table, they've moved to more subtle behaviors.

To be clear, I fully appreciate and welcome zealous advocacy. After all, good defense lawyers help ensure that our enforcement decisions are fair and informed. But dilatory or obstructive conduct is not zealous advocacy. It is behavior that frustrates our processes, puts investors at risk, and contributes to that declining trust I described.

Delay, for example, may enable a fraudster to dissipate assets or place them beyond our reach. A needlessly lengthy accounting fraud investigation could mean that markets lack accurate information about a public company for an extended period. And advisory clients unaware of a potential conflict may keep money invested with a firm, when, given full information, they would choose another money manager.

Protracted investigations also impose costs on the individuals and firms involved. Most obviously, there are the reputational costs that an issuer might incur after disclosing an investigation but before its delayed resolution. Those reputational costs may, in turn, impose economic costs on shareholders. There are also, of course, the legal bills incurred as a result of unduly extended negotiations or needless disputes over routine investigatory issues.

And, finally, there are the psychological or emotional costs for witnesses involved in investigations. When counsel decide to dispute plainly reasonable requests, delay productions, prolong testimony, or otherwise frustrate our investigations, it can exacerbate all of these costs.

For these reasons and others, it's in our collective interest to ensure that our investigations move quickly and efficiently.

To read more: https://www.sec.gov/news/speech/grewal-remarks-securities-enforcement-forum-west-051222

Macropru – fit for the future?

Sarah Breeden, Executive Director for Financial Stability Strategy and Risk and a member of the Financial Policy Committee (FPC), the United Kingdom's macroprudential authority.

When the financial system is in poor condition – when there is financial instability – it can be damaging to us all.

I like to compare the importance of financial stability to our collective prosperity with the importance of health to an individual. Good health may not be the only thing that matters for an individual's happiness. But it is essential. Because poor health comes with undesirable consequences.

We need only remind ourselves of the global financial crisis, more than a decade ago, to appreciate the undesirable consequences of financial instability.

UK GDP shrank by more than 6% during the first five quarters of the crisis, staying below its pre-recession size for a further five years. Unemployment increased, with an additional 1 million jobs lost by its peak at the end of 2011. And labour productivity, the best way to measure living standards in the long-run, fell sharply in 2008 and has barely recovered since.

The poor health of the global financial system was exposed in the most dramatic of fashions. We might liken it to a heart attack. And in response the authorities co-operated across borders and across institutions to design a radical 'healthcare plan' – to improve resilience, both at the micro-prudential individual institution and the economy-wide macro-prudential levels.

It is this macro-prudential perspective that I want to discuss today – specifically, to consider how macro-prudential policy will need to adapt, just as our health-care plans adapt, to be fit for the challenges of the future.

Since the global financial crisis, the financial system has not been a cause of sustained economic instability. But this is no reason for complacency. The financial system is ever changing. And experience suggests our job may not yet be complete.

So today, I will begin by setting out why financial stability is important and the role of macro-prudential policy in delivering it. In so doing I hope to set

out why it's as important for the financial system to observe macro-prudential policies as it is for patients to stick to their health-care plans.

I will then briefly set out some principles on which good macro-prudential policymaking is based. The rules of thumb that underlie our prescriptions if you like.

And I will conclude by raising some challenges that macro-prudential policy is facing now, including my thoughts on the road ahead. Through that, I hope to set out how we need constantly to adapt macro-prudential policies, as we do with our health-care plans as lifestyles evolve.

Interactions between financial stability and sustainable growth and the role for macro-prudential policy

Why is financial stability important?

To understand why we place so much emphasis on a well-grounded macro-prudential framework, it's important to understand why we care about financial stability in the first place. In brief, it is because we believe that financial stability is a precondition for sustainable economic growth.

A stable and well-functioning financial system exists to serve us all. It enables the efficient allocation of resources, so that businesses can exploit productive opportunities and households can meet their needs. And it allows the risks incurred in the course of generating economic growth to be shared.

The banking system supplies credit to households, to buy homes or spend more than they currently earn; and to businesses, so that they can hire more workers, invest in capital, and innovate and expand.

Non-bank financial firms further transform long-term savings into new investments via bond and stock purchases; and they enable both households and businesses to insure themselves against risks that could prove costly were they to crystallise.

The financial system also facilitates payments, so that households and businesses can pay safely for the goods and services they choose to receive.

A stable financial system is one that is resilient to shocks and so is able reliably to support households and businesses through the consistent supply of the vital services that they demand. Financial stability thus supports growth and prosperity, just as good health supports us in our daily lives.

The role of macro-prudential policy

Historically, there was a view among policymakers that as long as monetary policy guaranteed low and stable inflation, and micro-prudential regulation was successful in ensuring the balance sheets of individual institutions were robust to shocks, the financial system could take care of itself, and financial stability would follow.

However, the global financial crisis revealed the flaws in this view: while monetary policy sets the benchmark interest rate for financial transactions and "gets into all the cracks" in the financial system, it isn't sufficient to ensure that those transactions are undertaken efficiently and effectively.

Similarly, micro-prudential policy ensures the safety and soundness of individual institutions, but does not take a sufficiently bird's eye view to identify possible risks affecting the financial system as a whole.

The financial crisis highlighted quite how much the whole is greater than the sum of its parts. And that ensuring the parts are healthy does not guarantee that the whole is.

Macro-prudential interventions typically fill two gaps:

1. Individual agents don't necessarily take into account the bigger picture. Individual financial institutions and borrowers face private incentives which do not take into account the wider social impact of their actions. In such cases, macro-prudential policymakers can seek to better align private costs and benefits with social costs and benefits.

One example is the Financial Policy Committee's (FPC) mortgage tools, which seek to limit the number of mortgages banks can extend for loans that are high relative to income.

Individual borrowers may be keen to stretch themselves financially to buy a bigger house, expecting their earnings to grow or house prices to rise. And individual lenders may be happy to provide a larger loan to receive more income. But should a recession hit, not only will we see defaults, but overstretched borrowers will reduce their spending as they struggle to pay their mortgages. And this reduction would ultimately spillover to the rest of the economy, making the downturn worse.

Macro-prudential policy takes these spillovers into account. By ensuring borrowers in aggregate are not overstretching themselves and financial institutions in general are lending responsibly, macro-prudential regulators can ensure that the whole system is more resilient to shocks.

2. Markets are not necessarily efficient or complete. Market prices may not reflect the real value of assets, not every market is perfectly liquid and risks

may not be as well-dispersed as they might seem. These imperfections can lead to two types of risk to financial stability: cyclical and structural.

Cyclical risks arise because financial conditions can suddenly reverse. The simplest example is of financial institutions taking on too much risk in booms, in the expectation that the assets they purchase will always be in demand. When the cycle turns, asset prices can fall rapidly, leaving institutions with losses. This is why we have countercyclical tools - to ensure the system can build up resilience in good times, and use it in bad times.

Structural risks refer to fault-lines within the financial system, such as high concentrations of risk, complex interconnections, promises made that cannot necessarily be honoured, and uninsurable – or tail – risks. These risks can trigger sharp reversals in financial conditions, or amplify cyclical risks when they crystallise. As with cyclical risks, macro-prudential policy looks to build resilience to these risks, as well as eliminating fault-lines where appropriate.

The cost-benefit calculus

In seeking to fill these two gaps, it is important to acknowledge that there are two sides to the ledger – that a build-up in financial stability risk is often accompanied by higher growth.

When the financial system under-prices risks, households, companies and the economy at large may appear to benefit. As asset prices rise, perceptions of wealth become inflated and risks appear smaller. Households and companies feel more comfortable taking on debt, banks and investors feel more comfortable lending to them. We can consume more, invest more, grow the economy more and feel more prosperous.

The problem is that it cannot last. We cannot continue consuming more than we ever hope to earn; we cannot invest more than we ever intend to save; risks cannot be under-priced forever. This time it probably isn't different.

And when it all goes into reverse, when risks are found to be under-priced and not well-dispersed, when shocks arise and are amplified by the financial system, the cost in terms of lost growth can far outweigh the benefit of higher growth enjoyed while the risks were building.

It is this cost-benefit calculus that both motivates a role for macro-prudential policy, and helps us define precisely what we mean by it.

In short, macro-prudential policy aims to improve the trade-off between the financial system's contribution to the rewards expected in a growing economy and the degree of risk that we will face in the bad times.

To return to my analogy, we might liken it to the NHS and to health insurance where we pay a bit in the good times to protect ourselves should our health take a turn for the worse.

Principles of good policy making

Macro-prudential authorities, like the UK's FPC, work to ensure that financial systems are resilient to, and prepared for, the wide range of possible shocks they could face. Their aim is to ensure that when shocks occur, the financial system is able to absorb those shocks, rather than to amplify their impact on the economy.

We ground what we do in two elements of good macro-prudential policymaking:

- Macro-prudential policy should be targeted to provide a net benefit to the overall economy. Where interventions incur costs, these should only be imposed when they are outweighed by the benefits over the full cycle. This is perhaps equivalent to starting a course of new medication, where a good doctor must be aware of potential side effects as well as intended benefits.

  We must also recognise that there will be occasions when interventions are not yet needed, as emerging risks are not yet systemic in nature. To return to our analogy, a good doctor might decide not to start medication, but instead simply monitor a patient's general health to judge better how to improve it.

- Macro-prudential policy should be ready to adapt to change, allowing the economy to expand and innovate safely. Change always brings with it opportunities and risks and so our macro-prudential framework will need to evolve. To overuse the health analogy once more, doctors need to adapt. A doctor in the 1960s, for example, would never have had to think about the health effects of vaping.

Challenges that lie ahead

Ten years after establishing the FPC, we have reached the point where we have both made the case for macro-prudential policy, and built a macro-prudential framework designed to ensure the sector is resilient to stress. In other words, we have pulled together the skeleton for a healthcare plan and convinced the patient that they need it and that it needs to be updated regularly.

These are important achievements. Indeed we need to make sure we hang on to them even as memories of the global financial crisis fade.

But we need to decide the plan for the coming months and years too. Recent shocks – the Covid pandemic, and more recently, Russia's invasion of Ukraine – and structural changes to the financial system have reaffirmed that our work is not yet done.

Let me briefly mention a few of the lessons from our experience in Covid-19.

First the capital framework does not in practice support use of bank capital buffers in a stress as we intended. And that would have mattered a lot in the absence of the substantial government support for the corporate sector.

Second, we need to change our approach to stress testing in a stress if we are to avoid those stress tests further amplifying any downturn.

And third, in a shock of roughly half the size of the global financial crisis, it was only large-scale use of central bank balance sheets that calmed dysfunction in the system of market-based finance.

We are continuing to learn through the Russia-Ukraine crisis too. We are exploring concentrations in, and interconnections across, energy and other commodity markets, the financial system, and the real economy, as well as the potential for feedback loops between them. And we have observed too that commodity markets are relatively opaque.

We must now develop the macro-prudential framework to reflect the lessons from these recent stresses.

Looking beyond recent events, neither the financial system nor the economy stands still: there are clear structural changes that macro-prudential policy must confront.

1.The rise of market-based finance: vulnerabilities that are as much global as domestic

One key challenge is that many vulnerabilities are as much global as they are domestic. That includes non-bank, or market-based, finance.

Non-bank financial institutions currently represent around 50% of global (and UK) financial sector assets. They are increasingly a source of finance for UK businesses. However, the 'dash for cash' in March 2020 led to a rapid deterioration in the functioning even of advanced-economies' government bond markets and created market dynamics significant

enough to raise the cost of lending. The episode clearly demonstrated the need to build resilience in market-based finance.

Given the global nature of market-based finance, the effectiveness of any policies in the UK will depend in part on policies implemented in other major jurisdictions. We are therefore working with international counterparts in the Financial Stability Board to take coordinated action to address these issues - including on open-ended funds, margins, the liquidity structure and resilience of core markets, to name a few. In the meantime, the FPC (and other UK authorities) need to continue monitoring them, starting by ensuring there is reliable data to do so.

2.The growth of cryptoassets and decentralised finance: regulatory frameworks need to evolve

Another important challenge is seen in cryptoassets and decentralised finance (DeFi) which in recent years have grown to represent around 1% of global financial assets.

Cryptoasset technology is creating new financial assets, and new means of intermediation. Many services now facilitated by this technology mirror those available in the traditional financial sector, including lending, trading and exchange, investment management and insurance.

While that activity is currently small, if the pace of growth seen in recent years continues, interlinkages with the traditional financial sector are likely to increase. In addition, the new technology has the potential to reshape activity currently taking place in the traditional financial sector, either through the migration of that activity or the widespread adoption of the technology.

Crypto technology has the potential to bring significant benefits, for example by reducing the cost and increasing the speed of cross-border transactions, and encouraging competition in the financial system. But those benefits can only be realised and innovation be sustainable if it is undertaken safely and accompanied by effective public policy frameworks that mitigate risks and maintain broader trust and integrity in the financial system.

In this way, the growth of cryptoassets and DeFi has highlighted another of the key challenges for policymakers: the need for regulatory frameworks to adapt.

3.The transition to net zero: structural change requires coordinated action from all sectors

And finally, we face the continued need to support the orderly transition to a net zero economy. Climate change creates risks to financial stability through two channels: physical risks and transition risks. And the financial system will play a key role in financing the significant structural economic changes needed to deliver the transition to a net zero economy.

The unique challenge here is that the orderly transition to net zero will require coordinated action across private and public sector institutions, and across all sectors of finance and the real economy. The Bank's role is focussed on tackling the consequences (not the causes) of climate change. Indeed the transition to net zero is likely to be a bumpy one, particularly in light of recent events, and macro-prudential regulators have an important role to play in helping manage those bumps.

In support of this work, we are running a stress test of the UK's largest banks and insurers that will extend the time horizons over which we, and they, view climate risks. This is a good start in understanding the implications of climate change and transition for the financial system. But more work is needed to build the green market infrastructure that will support an orderly transition to net zero, and this will be an important area of focus for macro-prudential regulation over the coming years.

Conclusion: The road ahead

Where does all this leave us?

It's clear that we macro-prudential policymakers need to look forwards as well as backwards as we do our risk assessment. And we must also ground our analysis in the impact of shocks to the financial system on businesses, households and so the economy, and not just their impact on financial players.

The source of shocks and the mechanisms through which the financial system could amplify those shocks is wide – covering climate, Covid, crypto, cyber, and conflict as well as the credit cycle and the core banking system. But our understanding of many of these is still developing, reflecting differences in the maturity across our framework.

The consequence is that like any health check the list of what we need to review is long. And so the key is how we prioritise our work and what prescriptions we write on the back of it. That's a daunting task. But helpfully while for some issues only the macro-prudential policymaker can do the job, for other issues just like a GP we can call on the help of specialists.

I'm not proposing to write any prescriptions in this speech today. But the Bank and FPC are working hard on their diagnoses and will aim to

communicate further on issues that they wish to prioritise later this year, through the Bank's Financial Stability Strategy and the FPC's medium-term priorities.

And I hope that today has given you a flavour of the importance of building a macro-prudential framework that's as fit for the risks and opportunities of the future as it is for those we have faced in the past.

The views expressed here are not necessarily those of the Financial Policy Committee. I am grateful to Nicola Anderson, Kristina Bluwstein, Giovanni Covi, Tom Daniels, Emma Moriarty, Nicholas Vause, Danny Walker and Gabija Zemaityte for their assistance in drafting these remarks. I would like to thank Jon Cunliffe, Alina Barnett, Geoff Coppins, Lee Foulger, Grellan McGrath, Jon Relleen and Matt Waldron for their helpful comments.

Fake WhatsApp ‘voice message’ emails are spreading malware

National Cyber Security Centre

A phishing campaign which impersonates WhatsApp’s voice message feature has been spreading information-stealing malware.

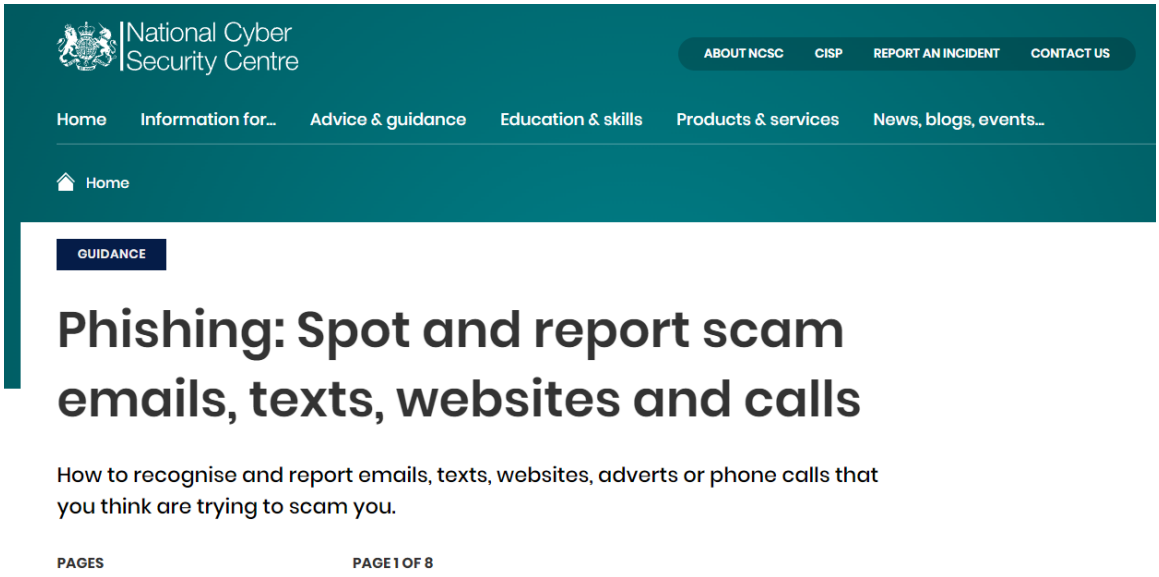
The attack starts with an email claiming to be a notification from WhatsApp of a new private voice message. The email contains a creation date and clip duration for the supposed message, and a ‘Play’ button.

The identity ‘Whatsapp Notifier’ masks a real email address belonging to a Russian road safety organisation. As the address and organisation are real, the messages aren’t flagged as spam or blocked by email security tools. Armorblox, who discovered the scam, believe the Russian organisation is playing a role without realising.

The ‘Play’ button will take the email recipient to a website which then asks them to click ‘Allow’ in an allow/block prompt to ‘confirm you are not a robot’. Once ‘allow’ is clicked, the browser will prompt to install software that turns out to be information-stealing malware.

While there are numerous ‘tells’ that this is a scam, these attacks rely on people missing the signs – perhaps because they are waiting for urgent or exciting news that could well be delivered by a voice message.

The NCSC has published guidance on how to spot and report scams, including those delivered by email and messaging. You may visit: https://www.ncsc.gov.uk/collection/phishing-scams



Our top tips for staying secure online will help you keep your devices and information secure even if you do click on a scam, and you can also learn how to recover a hacked account.

You may visit: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online

https://www.ncsc.gov.uk/guidance/recovering-a-hacked-account

CERT-In issues directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet

CERT-In
Indian Computer Emergency Response Team
Enhancing Cyber Security in India

The Indian Computer Emergency Response Team (CERT-In) serves as the national agency for performing various functions in the area of cyber security in the country as per provisions of section 70B of the Information Technology Act, 2000.

CERT-In continuously analyses cyber threats and handles cyber incidents tracked and reported to it. CERT-In regularly issues advisories to organisations and users to enable them to protect their data/information and ICT infrastructure.

In order to coordinate response activities as well as emergency measures with respect to cyber security incidents, CERT-In calls for information from service providers, intermediaries, data centres and body corporate.

During the course of handling cyber incidents and interactions with the constituency, CERT-In has identified certain gaps causing hindrance in incident analysis.

To address the identified gaps and issues so as to facilitate incident response measures, CERT-In has issued directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents under the provisions of sub-section (6) of section 70B of the Information Technology Act, 2000.

These directions will become effective after 60 days.

The directions cover aspects relating to synchronization of ICT system clocks; mandatory reporting of cyber incidents to CERT-In; maintenance of logs of ICT systems; subscriber/customer registrations details by Data centers, Virtual Private Server (VPS) providers, VPN Service providers, Cloud service providers; KYC norms and practices by virtual asset service providers, virtual asset exchange providers and custodian wallet providers.

These directions shall enhance overall cyber security posture and ensure safe & trusted Internet in the country.

The directions issued by CERT-In are available at: https://www.cert-in.org.in/Directions70B.jsp

Project Zero
A Year in Review of 0-days Used In-the-Wild in 2021

News and updates from the Project Zero team at Google
Posted by Maddie Stone, Google Project Zero

Project Zero

This is our third annual year in review of 0-days exploited in-the-wild [2020, 2019]. Each year we've looked back at all of the detected and disclosed in-the-wild 0-days as a group and synthesized what we think the trends and takeaways are.

The goal of this report is not to detail each individual exploit, but instead to analyze the exploits from the year as a group, looking for trends, gaps, lessons learned, successes, etc. If you're interested in the analysis of individual exploits, please check out our root cause analysis repository.

We perform and share this analysis in order to make 0-day hard. We want it to be more costly, more resource intensive, and overall more difficult for attackers to use 0-day capabilities. 2021 highlighted just how important it is to stay relentless in our pursuit to make it harder for attackers to exploit users with 0-days.

We heard over and over and over about how governments were targeting journalists, minoritized populations, politicians, human rights defenders, and even security researchers around the world. The decisions we make in the security and tech communities can have real impacts on society and our fellow humans' lives.

We'll provide our evidence and process for our conclusions in the body of this post, and then wrap it all up with our thoughts on next steps and hopes for 2022 in the conclusion. If digging into the bits and bytes is not your thing, then feel free to just check-out the Executive Summary and Conclusion.

Executive Summary

2021 included the detection and disclosure of 58 in-the-wild 0-days, the most ever recorded since Project Zero began tracking in mid-2014. That's more than double the previous maximum of 28 detected in 2015 and especially stark when you consider that there were only 25 detected in 2020. We've tracked publicly known in-the-wild 0-day exploits in this spreadsheet since mid-2014.

While we often talk about the number of 0-day exploits used in-the-wild, what we're actually discussing is the number of 0-day exploits detected and disclosed as in-the-wild. And that leads into our first conclusion: we believe

the large uptick in in-the-wild 0-days in 2021 is due to increased detection and disclosure of these 0-days, rather than simply increased usage of 0-day exploits.

With this record number of in-the-wild 0-days to analyze we saw that attacker methodology hasn't actually had to change much from previous years. Attackers are having success using the same bug patterns and exploitation techniques and going after the same attack surfaces.

Project Zero's mission is "make 0day hard". 0-day will be harder when, overall, attackers are not able to use public methods and techniques for developing their 0-day exploits. When we look over these 58 0-days used in 2021, what we see instead are 0-days that are similar to previous & publicly known vulnerabilities. Only two 0-days stood out as novel: one for the technical sophistication of its exploit and the other for its use of logic bugs to escape the sandbox.

So while we recognize the industry's improvement in the detection and disclosure of in-the-wild 0-days, we also acknowledge that there's a lot more improving to be done. Having access to more "ground truth" of how attackers are actually using 0-days shows us that they are able to have success by using previously known techniques and methods rather than having to invest in developing novel techniques. This is a clear area of opportunity for the tech industry.

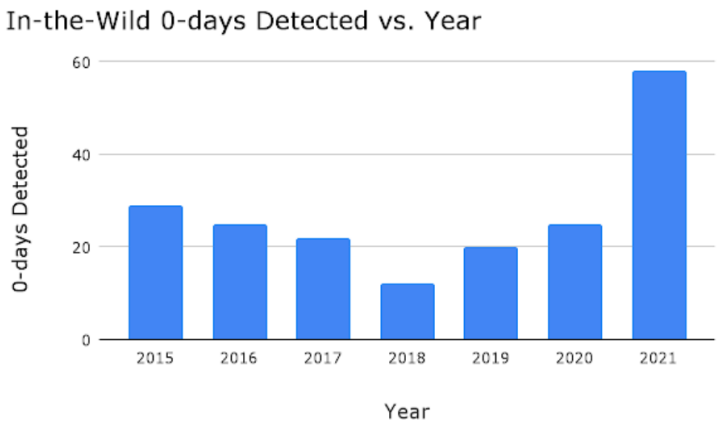
We had so many more data points in 2021 to learn about attacker behavior than we've had in the past. Having all this data, though, has left us with even more questions than we had before. Unfortunately, attackers who actively use 0-day exploits do not share the 0-days they're using or what percentage of 0-days we're missing in our tracking, so we'll never know exactly what proportion of 0-days are currently being found and disclosed publicly.

Based on our analysis of the 2021 0-days we hope to see the following progress in 2022 in order to continue taking steps towards making 0-day hard:

- All vendors agree to disclose the in-the-wild exploitation status of vulnerabilities in their security bulletins.

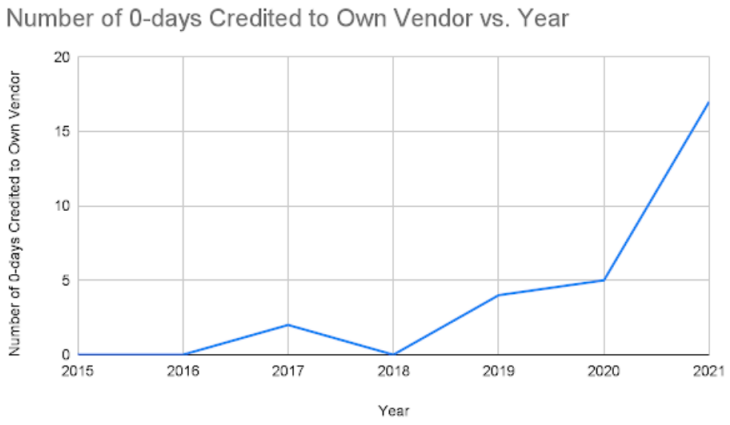
- Exploit samples or detailed technical descriptions of the exploits are shared more widely.

- Continued concerted efforts on reducing memory corruption vulnerabilities or rendering them unexploitable. Launch mitigations that will significantly impact the exploitability of memory corruption vulnerabilities.



Is it that software security is getting worse? Or is it that attackers are using 0-day exploits more? Or has our ability to detect and disclose 0-days increased? When looking at the significant uptick from 2020 to 2021, we think it's mostly explained by the latter.

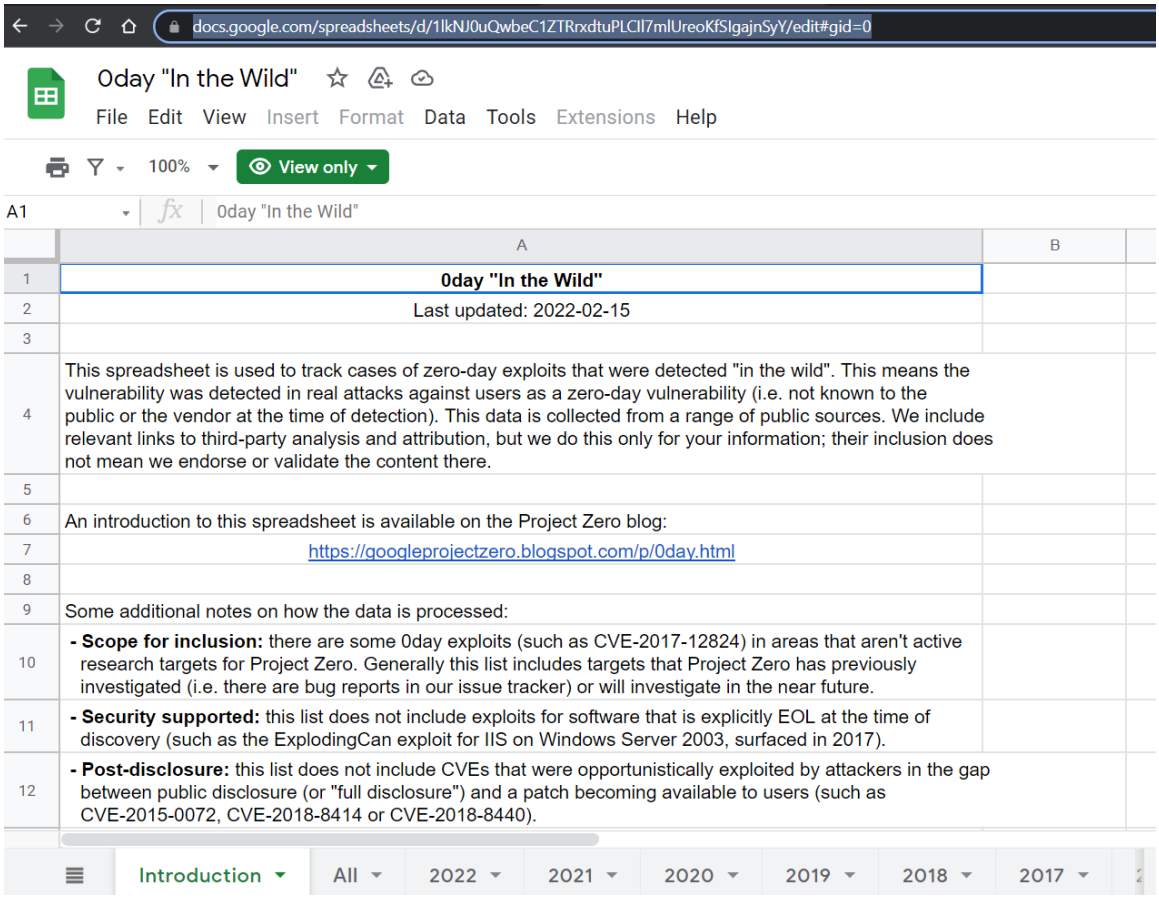
While we believe there has been a steady growth in interest and investment in 0-day exploits by attackers in the past several years, and that security still needs to urgently improve, it appears that the security industry's ability to detect and disclose in-the-wild 0-day exploits is the primary explanation for the increase in observed 0-day exploits in 2021.



While we often talk about “0-day exploits used in-the-wild”, what we’re actually tracking are “0-day exploits detected and disclosed as used in-the-wild”. There are more factors than just the use that contribute to an increase in that number, most notably: detection and disclosure. Better detection of 0-day exploits and more transparently disclosed exploited 0-day vulnerabilities is a positive indicator for security and progress in the industry.

You may visit: https://googleprojectzero.blogspot.com/2022/04/the-more-you-know-more-you-know-you.html

https://docs.google.com/spreadsheets/d/1lkNJouQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit#gid=0



Largest Mobile Chipset Manufacturers used Vulnerable Audio Decoder, 2/3 of Android users' Privacy around the World were at Risk

- Check Point Research discovered vulnerabilities in the ALAC format that could have led an attacker to remotely get access to its media and audio conversations

- MediaTek and Qualcomm, the two largest mobile chipset manufacturers in the world, used the ALAC audio coding in their widely distributed mobile handsets, putting millions of Android users' privacy at risk

- Research, dubbed "ALHACK" finds Two thirds of all smartphones sold in 2021 are vulnerable

- Qualcomm and MediaTek acknowledged the vulnerabilities flagged by CPR, putting patches and fixes in response

Background

The Apple Lossless Audio Codec (ALAC), also known as Apple Lossless, is an audio coding format, developed by Apple Inc. and first introduced in 2004 for lossless data compression of digital music.

In late 2011 Apple made the codec open source. Since then, the ALAC format has been embedded in many non-Apple audio playback devices and programs, including Android-based smartphones, Linux and Windows media players and converters.

Since then Apple has been updating the proprietary version of the decoder several times, fixing and patching security issues, but the shared code has not been patched since 2011.

Many third-party vendors use the Apple-supplied code as the basis for their own ALAC implementations, and it's fair to assume that many of them do not maintain the external code.

Check Point Research has discovered that Qualcomm and MediaTek, two of the largest mobile chipset makers in the world, ported the vulnerable ALAC code into their audio decoders, which are used in more than half of all smartphones worldwide. According to IDC, 48.1% of all Android phones sold in the US are powered by MediaTek as of Q4 2021, while Qualcomm currently holds 47% of the market.

To read more: https://blog.checkpoint.com/2022/04/21/largest-mobile-chipset-manufacturers-used-vulnerable-audio-decoder-2-3-of-android-users-privacy-around-the-world-were-at-risk/

NIST Study Shows Everyday Plastic Products Release Trillions of Microscopic Particles Into Water

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Plastics surround us, whether it's the grocery bags we use at the supermarket or household items such as shampoo and detergent bottles. Plastics don't exist only as large objects, but also as microscopic particles that are released from these larger products. These microscopic plastics can end up in the environment, and they can be ingested into our bodies.

Now, researchers at the National Institute of Standards and Technology (NIST) have analyzed a couple of widely used consumer products to better understand these microscopic plastics. They found that when the plastic products are exposed to hot water, they release trillions of nanoparticles per liter into the water.

The NIST researchers published their findings in the scientific journal Environmental Science and Technology.

"The main takeaway here is that there are plastic particles wherever we look. There are a lot of them. Trillions per liter. We don't know if those have bad health effects on people or animals. We just have a high confidence that they're there," said NIST chemist Christopher Zangmeister.

There are many different types of plastic materials, but they are all made up of polymers, natural or human-made substances composed of large molecules linked together. Scientists have found microscopic particles from these larger plastics in the oceans and many other environments. Researchers categorize them into two groups: micro- and nanoplastics.

Microplastics are generally considered smaller than 5 millimeters in length and could be seen by the naked eye, while nanoplastics are smaller than one millionth of a meter (one micrometer) and most can't even be seen with a standard microscope. Recent studies have shown some consumer products that hold liquids or interact with them, such as polypropylene (PP) baby bottles and nylon plastic tea bags, release these plastic particles into the surrounding water.

In their study, the NIST researchers looked at two types of commercial plastic products: food-grade nylon bags, such as baking liners — clear plastic sheets placed in baking pans to create a nonstick surface that prevents moisture loss — and single-use hot beverage cups, such as coffee cups. The beverage cups they analyzed were coated with low-density polyethylene (LDPE), a soft flexible plastic film often used as a liner.

The LDPE-lined beverage cups were exposed to water at 100 degrees Celsius (212 degrees Fahrenheit) for 20 minutes.

To analyze the nanoparticles released from these plastic products, the researchers first needed to determine how to detect them. “Imagine having a cup of water in a generic to-go coffee cup. It could have many billions of particles, and we would need to figure out how to find these nanoplastics. It’s like finding a needle in a haystack,” Zangmeister said.

So, he and his colleagues had to use a new approach. “We used a way of taking the water that’s in the cup, spraying it out into a fine mist, and drying the mist and all that’s left within the solution,” said Zangmeister. Through this process, the nanoparticles are isolated from the rest of the solution.

The technique itself has previously been used to detect tiny particles in the atmosphere. “So, we’re not reinventing the wheel but applying it to a new area,” said Zangmeister.

After the mist was dried, the nanoparticles in it were sorted by their size and charge. Researchers could then specify a particular size, for example nanoparticles around 100 nanometers, and pass them into a particle counter.

The nanoparticles were exposed to a hot vapor of butanol, a type of alcohol, then cooled down rapidly. As the alcohol condensed, the particles swelled from the size of nanometers to micrometers, making them much more detectable. This process is automated and run by a computer program, which counts the particles.

Researchers could also identify the chemical composition of the nanoparticles by placing them on a surface and observing them with techniques known as scanning electron microscopy, which takes high-resolution images of a sample using a beam of high-energy electrons, and Fourier-transform infrared spectroscopy, a technique that captures the infrared-light spectrum of a gas, solid or liquid.

All these techniques used together provided a fuller picture of the size and composition of the nanoparticles.

In their analysis and observations, the researchers found that the average size of the nanoparticles was between 30 nanometers and 80 nanometers, with few above 200 nanometers.

Additionally, the concentration of nanoparticles released into hot water from food-grade nylon was seven times higher compared with the single-use beverage cups.

"In the last decade scientists have found plastics wherever we looked in the environment. People have looked at snow in Antarctica, the bottom of glacial lakes, and found microplastics bigger than about 100 nanometers, meaning they were likely not small enough to enter a cell and cause physical problems," said Zangmeister.

"Our study is different because these nanoparticles are really small and a big deal because they could get inside of a cell, possibly disrupting its function," said Zangmeister, who also stressed that no one has determined that would be the case.

The U.S Food and Drug Administration (FDA) regulates the plastics that touch the food we eat or the water we drink. The agency has standards and safety measures in place to determine what's safe. The FDA's researchers run rigorous tests on these plastics and measure how much plastic mass is lost when exposed to hot water.

For example, the FDA has determined that food grade nylon (such as that used in tea bags) can safely lose up to 1% of its mass under high-temperature conditions. In the NIST study using their new technique, the researchers found one tenth of a percent of the mass was lost, which is significantly below current FDA limits for what's considered safe.

Zangmeister noted there isn't a commonly used test for measuring LDPE that is released into water from samples like coffee cups, but there are tests for nylon plastics. The findings from this study could help in efforts to develop such tests. In the meantime, Zangmeister and his team have analyzed additional consumer products and materials, such as fabrics, cotton polyester, plastic bags and water stored in plastic pipes.

The findings from this study, combined with those from the other types of materials analyzed, will open new avenues of research in this area going forward. "Most of the studies on this topic are written toward educating fellow scientists. This paper will do both: educate scientists and perform public outreach," said Zangmeister.

To read more: https://www.nist.gov/news-events/news/2022/04/nist-study-shows-everyday-plastic-products-release-trillions-microscopic

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.