Security Now! #1033 - 07-08-25

Going on the Offensive

This week on Security Now!

• Another Israeli spyware vendor surfaces. • Win11 to delete restore points more quickly. • The EU accelerates its plans to abandon Microsoft Azure. • The EU sets timelines for Post-Quantum crypto adoption. • Russia to create a massive IMEI database. • Canada and the UK create the "Common Good Cyber Fund". • U.S. states crack down on Bitcoin ATMs amid growing scams. • Congressional staffers cannot use WhatsApp on gov devices. • LibXML2 and the problems with commercial use of OSS. • A(nother) remote code execution vulnerability in WinRAR. • HaveI BeenPwned gets a cool data visualization site. • How is ransomware getting in? • Windows to offer "safe" non-kernel endpoint security? • Proactive age verification coming to porn sites. How? • Canada (also) says "bye bye" to Hikvision. • Germany will be banning DeekSeek. The whole EU may follow. • Cloudflare throttled in Russia? • What must the U.S. do to compete in global exploit acquisition?

Ad hoc signage is typically added after a need for it has occurred:

Security News

Israeli spyware maker Paragon Solutions

I have no idea why all of the major commercial spyware publishers seem to be Israeli, but it's apparent that's the case and it's really not a good look for Israel. Israel is home of Cellebrite, the famous smartphone cracker, The NSO Group which sells the Pegasus spyware, QuaDream, formed from ex-NSO Group members who offer the REIGN spyware, and Candiru, also known as Saito Tech Ltd. But what brought this to the fore today was news of yet another Israeli commercial spyware vendor known as Paragon which sells a smartphone penetration solution known as Graphite. This brings the total to five such companies that we know about.

In mid June, the Citizen Lab group's posting had the headline "Graphite: Caught First Forensic Confirmation of Paragon's iOS Mercenary Spyware, Finds Journalists Targeted" their introduction said:

> *On April 29, 2025, a select group of iOS users were notified by Apple that they were targeted with advanced spyware. Among the group were two journalists that consented for the technical analysis of their cases. The key findings from our forensic analysis of their devices are:*
>
> - *Our analysis finds forensic evidence confirming with high confidence that both a prominent European journalist (who requests anonymity), and Italian journalist Ciro Pellegrino, were targeted with Paragon's Graphite mercenary spyware.*
> - *We identify an indicator linking both cases to the same Paragon operator.*
> - *Apple confirms to us that the zero-click attack deployed in these cases was mitigated as of iOS 18.3.1 and has assigned the vulnerability CVE-2025-43200.*
>
> *Our analysis is ongoing.*

Some of the interesting revelations from their posting include:

> *We analyzed Apple devices belonging to a prominent European journalist who has requested to remain anonymous. On April 29, 2025, this journalist received an Apple notification and sought technical assistance.*
>
> *Our forensic analysis concluded that one of the journalist's devices was compromised with Paragon's Graphite spyware in January and early February 2025 while running iOS 18.2.1. We attribute the compromise to Graphite with high confidence because logs on the device indicated that it made a series of requests to a server that, during the same time period, matched our published Fingerprint P1. We linked this fingerprint to Paragon's Graphite spyware with high confidence.*
>
> *Graphite spyware server contacted by the journalist's device: https://46.183.184.91/.*
>
> *The server appears to have been rented from VPS provider EDIS Global. The server remained online and continued to match Fingerprint P1 until at least April 12, 2025.*
>
> *We identified an iMessage account present in the device logs around the same time as the phone was communicating with the Paragon server 46.183.184.91. We redact the account and refer to it as ATTACKER1. Based on our forensic analysis, we conclude that this account was used to deploy Paragon's Graphite spyware using a sophisticated iMessage zero-click attack. We believe that this infection would not have been visible to the target. Apple confirms to us*

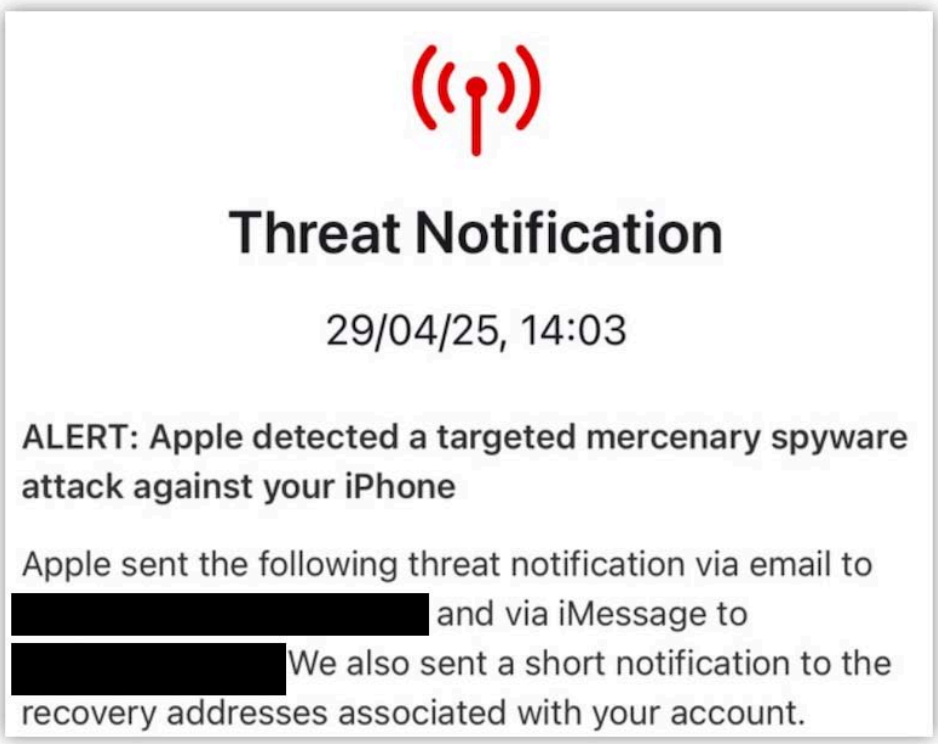
that the zero-click attack deployed here was mitigated as of iOS 18.3.1 and has assigned CVE-2025-43200 to this zero-day vulnerability.

Ciro Pellegrino is a journalist and head of the Naples newsroom at Fanpage.it, where he has reported on numerous high-profile cases. On April 29, 2025, Mr. Pellegrino received an Apple notification and sought our technical assistance.

We analyzed artifacts from Mr. Pellegrino's iPhone and determined with high confidence that it was targeted with Paragon's Graphite spyware. Our analysis of the device's logs revealed the presence of the same ATTACKER1 iMessage account used to target the journalist from Case 1, which we associate with a Graphite zero-click infection attempt.

It is standard for each customer of a mercenary spyware company to have its own dedicated infrastructure. Thus, we believe that the ATTACKER1 account would be used exclusively by a single Graphite customer / operator, and we conclude that this customer targeted both individuals.

Their use of the term "Mercenary" was interesting. It's the official term that Apple uses in their formal Threat Notifications to targeted individuals. I have a screenshot of a redacted Apple notification in the show notes:



They identify a total of seven Italian's who've received notifications either from Apple or WhatsApp. So this Paragon group is definitely now on the map and active.

A few weeks later, the publication "SecurityWeek" wrote: "Meta-owned WhatsApp told SecurityWeek that a recent FreeType vulnerability, flagged as potentially exploited at the time of disclosure, has been linked to an exploit of Israeli surveillance solutions provider Paragon."

In mid-March, Meta published an advisory on the Facebook security advisories page to inform

users about CVE-2025-27363, an out-of-bounds vulnerability in the FreeType open source library that could lead to arbitrary code execution. The advisory said the vulnerability may have been exploited in the wild. Meta knew this because the University of Toronto's Citizen Lab research group reported that a WhatsApp zero-day vulnerability had indeed been exploited in Paragon spyware attacks. WhatsApp representatives at the time told SecurityWeek that the zero-day attacks involved the use of groups and sending PDF files, and that the weakness had been patched on the server side, without the need for a client-side fix.

SecurityWeek explains:

> *FreeType is a development library designed for rendering text onto bitmaps, and provides support for other font-related operations. In the case of CVE-2025-27363, which impacts FreeType 2.13.0 and earlier, Meta said the issue is triggered when attempting to parse font subglyph structures related to TrueType GX and variable font files.*

And Meta's advisory explains:

> *Meta's advisory explains: "The vulnerable code assigns a signed short value to an unsigned long and then adds a static value causing it to wrap around and allocate an undersized heap buffer. The code then writes up to 6 signed long integers out of bounds relative to this buffer which can permit the execution of arbitrary code."*

Citizen Lab wrote that Paragon is known for developing sophisticated exploits that do not require any interaction from the targeted user, that they have found indications that the company was until recently able to hack up-to-date iPhones and that their spyware has been used in countries including Australia, Canada, Denmark, Italy, Cyprus, Singapore, and Israel.

Windows 11 system restore life reduced

Just in case anyone listening might have some reason to depend upon their Windows 11 system restore points enduring for their traditional 90 days, I wanted to note that Microsoft's most recent update to the 24H2 edition of Windows 11 has reduced restore point life to 60 days. I doubt anyone will care, but I thought it was worth noting. I don't know if they're wishing to save space, or tightening security, or what. But there it is. If you're the latest Win11 and you routinely restore, you'll now need to do so within 60 days.

The European Union accelerates its efforts to leave Azure

I noted last week when talking about the French city of Lyon, which is working to move from Microsoft solutions to Linux and other open source alternatives, that the entire European Union was also working to eliminate their dependency upon Microsoft Azure for cloud services. It's looking like the EU will be selecting the French company OVHcloud, with whom they are now in advanced talks. The reporting about this indicated that sharper point had been put on the EU's need for increased sovereignty and its distance and dependence upon U.S. solutions, after the U.S. administration imposed sanctions on four judges of the International Criminal Court in early June. One result of that was that those judges had their Microsoft accounts closed. So the EU will be working to provide alternative services that are no longer subject to the prevailing policies and politics of the U.S.

The EU and Post-Quantum Crypto
The European Union has published a PQC – a Post-Quantum Cryptography – roadmap. This roadmap instructs EU member states to begin transitioning their systems to post-quantum cryptography by the end of 2027. For all high-risk systems, such as critical infrastructure, this transition should be finished by the end of 2030. For other less mission-critical systems, States should have finished the migration of as many systems as feasible by the end of 2035.

Overall, this entire pre- and post-quantum crypto move has been handled with remarkable planning and grace. We have the new algorithms which continue to be tested and stress-tested and are now being deployed. We have updated underlying protocols that have been designed to smoothly accommodate the evolution, retirement and introduction of anything new that may be required. All indications are that just as were present during the original design and birth of the Internet, a bunch of very smart people got together to carefully define and establish these next steps in the evolution of the world's networking and security.

Wow! Talk about "Big Brother"
The old challenge of *"Why do you care about privacy if you have nothing to hide?"* is receiving a stress-test in Russia with the government's announcement of their plan to create a single national database of IMEI numbers. The Russian Ministry of Digital Affairs says the database will be used to combat financial fraud. Banning IMEI codes will allow authorities to block individual devices from mobile networks, even after fraudsters change phone numbers.

IMEI numbers indelibly identify physical mobile phone handsets. They're the approximate equivalent of the globally unique MAC addresses that are assigned to every Ethernet NIC to identify and differentiate it from any other. But IMEI numbers must be known to the user's service providing carrier since they are what identifies the mobile device handset to the cellular network. This means that they are never really secret or private. But needing to subpoena individual carriers on a per-subscriber basis would be far less convenient than requiring every carrier to provide an exhaustive dump of their entire subscriber/IMEI database, then require them to notify the Russian Ministry of Digital Affairs of any changes to that data over time.

Common Good Cyber Fund
On June 23rd the UK and Canada announced their establishment and initial funding under the heading *"New Common Good Cyber Fund Launches to Strengthen Internet Security Globally"* Their announcement said:

> *The Internet Society (ISOC) and Global Cyber Alliance (GCA), on behalf of the Common Good Cyber secretariat, today announce the launch of the Common Good Cyber Fund, an initiative to strengthen global cybersecurity by supporting nonprofits that deliver core cybersecurity services that protect civil society actors at high risk and the Internet as a whole. This first-of-its-kind effort to fund cybersecurity for the common good—for everyone, including those at the greatest risk of intimidation, harassment, harm and coercion—has the potential to fundamentally improve cybersecurity for billions of people around the world.*
>
> *The Common Good Cyber secretariat members working to address this challenge are: Global Cyber Alliance, Cyber Threat Alliance, CyberPeace Institute, Forum of Incident Response and Security Teams, Global Forum on Cyber Expertise, Institute for Security and Technology, and Shadowserver Foundation.*

In a Joint Statement Between the Prime Minister of the United Kingdom and the Prime Minister of Canada on June 15, 2025, the Prime Ministers announced that they would both invest in the Joint Canada-UK Common Good Cyber Fund. On June 17, during the G7 Leaders' Summit in Alberta, Canada, all the G7 Leaders announced that they would support initiatives like the Canada-UK Common Good Cyber Fund to aid members of civil society who are actively working to counter the threat of transnational repression.

Despite serving as a critical frontline defense for the security of the Internet, nonprofits working in cybersecurity remain severely underfunded—exposing millions of users, including journalists, human rights defenders, and other civil society groups to heightened risks of digital transnational repression involving the misuse of cyber capabilities to conduct surveillance, track individuals, and facilitate physical targeting. This underfunding also leaves the wider public exposed to increasingly frequent and sophisticated cyber threats.

Philip Reitinger, the President and CEO of the Global Cyber Alliance said: "Common Good Cyber represents a pivotal step toward a stronger, more inclusive cybersecurity ecosystem. By increasing the resilience and long-term sustainability of nonprofits working in cybersecurity, improving access to trusted services for civil society organizations and human rights defenders, and encouraging greater adoption of best practices and security-by-design principles, the Common Good Cyber Fund ultimately helps protect and empower all Internet users."

The fund will support nonprofits that:
- *Maintain and secure core digital infrastructure, including DNS, routing, and threat intelligence systems for the public good;*
- *Deliver cybersecurity assistance to high-risk actors through training, rapid incident response, and free-to-use tools*

The announcement indicated that the fund would initially receive $5.7 million to support these efforts. So this is great. The world has become utterly dependent upon a sophisticated system that just sort of blossomed organically. It needs support. So this will be very welcome. And Bravo to the UK and Canada for leading this.

States crack down on bitcoin ATMs as scams surge

Axios had some good coverage describing recent U.S. State regulations being enacted in response to the rise of Crypto-ATMs and the high levels of abuse, thereof. Here's what we learn:

States across the U.S. are rolling out tough new laws that cap deposits and tighten oversight on cryptocurrency ATMs, seeking to cut off a favorite tool of scammers and extortionists.

These Crypto-ATM kiosks are the easiest way for ordinary people to turn cash into crypto, and their use by fraudsters has surged over the last few years, especially with scams targeting older Americans. These are popular tools of scammers because cryptocurrency provides criminals with a way to receive money that a third-party can't roll back. These kiosks have popped up all over the country and over the last few years, scammers have increasingly utilized them in all manners of schemes.

Last September the FTC reported that fraud losses specifically involving crypto kiosks jumped nearly 10x from 2020 to 2023. The FBI reported $247 million in losses tied to the kiosks in 2024, with a 99% increase in complaints from the year before.

Schemes have particularly impacted older Americans, both the FTC and FBI warn. People 60 and over were more than three times as likely as younger adults to report a loss using a crypto kiosk. States taking action include Illinois. The state legislature sent a bill to Gov. JB Pritzker in early June, who had called for legislation to address the issue early in the year. Among other things, the law would require crypto ATM operators to include details on every receipt — such as the blockchain address where funds are sent — that would help law enforcement with any future fraud investigation.

Other states have taken similar actions. Vermont passed a law in May. One thing it does is put a daily limit on usage for these machines to throttle how much criminals can gouge victims.

Nebraska stamped a new law in March that establishes a licensing system for crypto ATM operators. Nebraska has been eager to bring crypto business to the state.

Arizona, which also enacted a bitcoin reserve fund, established a law in May that requires refunds on fraudulently induced transactions.

A new Oklahoma law, which survived a veto by the state's governor, will go into effect on Nov. 1, establishing similar protections.

And Rhode Island's governor signed a new law last Monday. In addition to enacting similar measures as other states, Rhode Island's law requires a warning about the irreversibility of cryptocurrency transactions to be clearly posted on the kiosk.

Cities have also homed in on the issue. On June 16th, The City of Spokane, Washington, voted to ban all crypto kiosks. [No Crypto for you!] And they've been a topic in Minnesota cities including St. Paul, Stillwater and Forest Lake.

Much of this legislation has been at the urging of the AARP – the American Association of Retired People – which has been urging state legislators to pass these bills. The AARP says they've endorsed 12 bills that have passed in different states so far.

It came as a surprising to me that there's a high fee for the use of these services. They are not free. One Crypto-ATM provider, Bitcoin Depot, reported an operating profit margin of 20%, generating $33 million in profits for the first quarter of this year.

I think that of all of this, the requirement of posting very clear physical warning messages on these machines, reminding – or informing – anyone using them that all transactions are final and that there can be no recourse or refunds, makes a lot of sense. We live in a country where individuals wish to preserve as much of their freedom and privacy as possible. So I think the best that can be done is assuring that everyone understands the nature of when they are doing. Yes, incautious people will be duped and scammed. That's always been true and always will be. It's only the means that change over time.

No use of WhatsApp among Congressional staffers

It occurs to me that the way to improve an app's security is to widely and publicly ban its use due to exactly its demonstrated lack of security. To that end…

The U.S. House's chief administrative officer recently informed congressional staffers that the messaging app WhatsApp is now banned on their government devices.

The ban centers on the vulnerability of staffers' data at rest and it comes as Congress is also taking steps to limit the use of AI programs which it deems similarly risky. In recent years the chief administrative officer has set at least partial bans on DeepSeek, ByteDance's apps and Microsoft Copilot. It has also heavily restricted staffers' use of ChatGPT, instructing offices to only use the paid version, ChatGPT Plus.

The Congressional Affairs Office wrote in an email: "The Office of Cybersecurity has deemed WhatsApp a high-risk to users due to the lack of transparency in how it protects user data, absence of stored data encryption, and potential security risks involved with its use. House staff are NOT allowed to download or keep the WhatsApp application on any House device, including any mobile, desktop, or web browser versions of its products. If you have a WhatsApp application on your House-managed device, you will be contacted to remove it."

On the other side, Andy Stone, a spokesperson for Meta said in a statement to Axios: "We disagree with the House Chief Administrative Officer's characterization in the strongest possible terms. We know members and their staffs regularly use WhatsApp and we look forward to ensuring members of the House can join their Senate counterparts in doing so officially. Messages on WhatsApp are end-to-end encrypted by default, meaning only the recipients and not even WhatsApp can see them. This is a higher level of security than most of the apps on the CAO's approved list that do not offer that protection."

However, the issue was reportedly WhatsApp's lack of on-device encryption, not whether or not it's secure in-transit. We know that WhatsApp is secure in transit since they borrowed Signal's well-designed and audited crypto technology. The CAO said that Microsoft Teams, Wickr, Signal, iMessage and FaceTime are all acceptable alternatives to WhatsApp. To me, this does sound and feel somewhat arbitrary. But as I noted earlier, if this might get WhatsApp to improve their security, everyone wins.

The state of LibXML2

I was somewhat distressed to hear what was on the mind of the German developer and maintainer of the open source Libxml2 library, especially after learning that this library being used by macOS, Windows and Linux. And of course when we hear about a lone maintainer of a library that's being used by all top three of the industry's operating systems, and thus indirectly by anyone using those features of those top OSes, we're all put in mind of the classic XKCD cartoon. Here's what Nick Wellnhofer recently posted under the topic: *"Triaging security issues reported by third parties"*

I have to spend several hours each week dealing with security issues reported by third parties. Most of these issues aren't critical but it's still a lot of work. In the long term, this is unsustainable for an unpaid volunteer like me. I'm thinking about making some changes to allow me to continue working on libxml2. The basic idea is to treat security issues like any other bug. They will be made public immediately and fixed whenever maintainers have the time. There will be no deadlines. This policy will probably make some downstream users nervous, but maybe it encourages them to contribute a little more.

The more I think about it, the more I realize that this is the only way forward. I've been doing this long enough to know that most of the secrecy surrounding security issues is just theater.

All the "best practices" like OpenSSF Scorecards are just an attempt by big tech companies to guilt trip OSS maintainers and make them work for free. My one-man company recently tried to become a OpenSSF member. You have to become a Linux Foundation member first which costs at least $10,000/year. These organizations are very exclusive clubs and anything but open. It's about time to call them and their backers out.

In the long run, putting such demands on OSS maintainers without compensating them is detrimental. I just stepped down as libxslt maintainer and it's unlikely that this project will ever be maintained again. It's even more unlikely with Google Project Zero, the best white-hat security researchers money can buy, breathing down the necks of volunteers.

Nick's issue-opening posting evoked a thoughtful reply from Red Hat's Michael Catanzaro, who is on the GNOME Release Team, the Fedora Workstation Working Group, and the desktop team at Red Hat. Michael replied:

Problem is, many of these bugs will actually be exploited in the wild if we do this, both in targeted attacks against specific disfavored individuals, and mass attacks against vulnerable populations like Uighurs.

- *I agree that reducing the disclosure deadline for libxml2 vulnerabilities might be strategic, at least for the time being, but there is a cost: downstream vendors might stop reporting bugs here, which is probably worse than the status quo. If you want to do this, then I suggest applying a short disclosure deadline of 14 days rather than 0 days. It might not even be necessary to make any changes to the disclosure deadline at all. Please take a few days to think about what you prefer; since you are the only active maintainer, I will follow whatever you decide.*

- *If you are burning out, then one option worth considering is to reduce your focus, e.g. you might consider focusing on triaging issue reports, reviewing merge requests, and, optimistically, mentoring new maintainers, rather than trying to fix security issues yourself. It's unreasonable to expect you to handle every problem alone, and it's time for downstream vendors to step up if desired. Many extremely wealthy corporations have a stake in fixing libxml2 security issues, and they should help out by becoming upstream maintainers. If nobody else wants to help maintain libxml2, then the consequence is security issues will surely reach the disclosure deadline (whatever it is set to) and become public before they are fixed. This is not your fault.*

- *I'm very grateful to Project Zero and other vulnerability research groups for reporting issues. Their reports are invariably excellent and we should encourage them to continue reporting vulnerabilities as quickly as they can find them. Warning us that problems exist is not a problem. (That said, Project Zero has notably reported zero security vulnerabilities in libxml2 since the start of this year. They have reported three vulnerabilities in libxslt.)*

And Nick answered Michael's reply, writing:

The point is that libxml2 never had the quality to be used in mainstream browsers or operating systems to begin with. It all started when Apple made libxml2 a core component of all their OSes. Then Google followed suit and now even Microsoft is using libxml2 in their OS outside of Edge. This should have never happened. Originally it was kind of a growth hack, but now these companies make billions of profits and refuse to pay back their technical debt, either by

switching to better solutions, developing their own or by trying to improve libxml2.

The behavior of these companies is irresponsible. Even if they claim otherwise, they don't care about the security and privacy of their users. They only try to fix symptoms.

I'm not playing a part in this game anymore. It would be better for the health of this project if these companies stopped using it. I'm thinking about adding the following disclaimer:

> *This is open-source software written by hobbyists, maintained by a single volunteer, badly tested, written in a memory-unsafe language and full of security bugs. It is foolish to use this software to process untrusted data. As such, we treat security issues like any other bug. Each security report we receive will be made public immediately and won't be prioritized.*

Most core parts of libxml2 should be covered by Google's or other bug bounty programs already. The rest of the code isn't as security-critical. I don't care if I don't receive security reports as early as possible. Most issues should be easily fixable by anyone. As soon as a patch is available, my job is done. I won't embargo security issues until a release is made. The only time you really want an embargo are non-trivial issues that take longer to fix. I can live with that risk.

Regarding Michael's bullet points: I'd love to mentor new maintainers but there simply aren't any candidates. I'm not burning out. Thanks for asking.

Earlier, I was admiring with some awe the graceful way the industry has been managing the growing threat of quantum computing which has the potential to overturn our well established public key crypto systems.

That's in the sharpest possible contrast to the sad and arguably pathetic mess the same industry has made of the open source model. XKCD's famous teetering tower is so poignant exactly because it's so true. The idea that Apple, Microsoft and Google are all using this code for free, then Google's Project Zero is finding and reporting flaws, while starting a disclosure deadline clock as a means of forcing the software's developers to fix the discovered mistakes is so deeply wrong on so many levels.

So I can see the logic behind Nick's solution. If all flaws, whether or not they are also security vulnerabilities, are immediately made public, Project Zero is de-fanged and deadlines cease to exist. Nick's follow-up posting made it clear that he's well over the glory and flattery of having all of the big OSes incorporating his code into their commercial offerings. Thanks very much. How about paying for the privilege of having me maintaining this code base for you to use year after year?

And that's the problem, of course. The open source software concept has always been that it's there to be freely used by anyone... for free. And that's what happened. When another hobbyist uses it for their own little project, that's different from when a massive multi-billion dollar corporation does so. In the latter case, the value proposition here seems unbalanced. Those multi-billion dollar corporations are paying their own code maintainers to keep their code working. But then they also take whatever they want from the open course community without ever returning anything other than complaints. Now, we know that there are more socially responsible large corporations that do employ developers to work on improving open source software. Certainly Google does a great deal of that.

But this open source movement, while it certainly has its heart in the right place, hasn't yet managed to figure out how to manage a fair exchange of value.

WinRAR for Windows Security RCE!
I'm a registered and paid RAR and WinRAR user. So when I hear of an exploitable remote code execution vulnerability in WinRAR I'm quick to download an update. WinRAR just moved to version 7.12 and everyone using it should update: https://www.win-rar.com/download.html. Their update notes said:

> *1. Directory Traversal Remote Code Execution Vulnerability (ZDI-CAN-27198)*
>
> *In previous versions of WinRAR, as well as RAR, UnRAR, UnRAR.dll, and the portable UnRAR source code for Windows, a specially crafted archive containing arbitrary code could be used to manipulate file paths during extraction. User interaction is required to exploit this vulnerability, which could cause files to be written outside the intended directory.*
>
> *This flaw could be exploited to place files in sensitive locations — such as the Windows Startup folder — potentially leading to unintended code execution on the next system login.*
>
> *This issue affects only Windows-based builds. Versions of RAR and UnRAR for Unix, the portable source code on Unix, and RAR for Android are not affected.*
>
> *We thank whs3-detonator, working with Trend Micro's Zero Day Initiative, for responsibly reporting this vulnerability.*

So the danger would be that miscreants would arrange to induce Windows users to download, open and extract the contents of booby-trapped RAR files. When doing so, the extraction-to directory can be overridden for special malicious files, causing them to be written elsewhere.

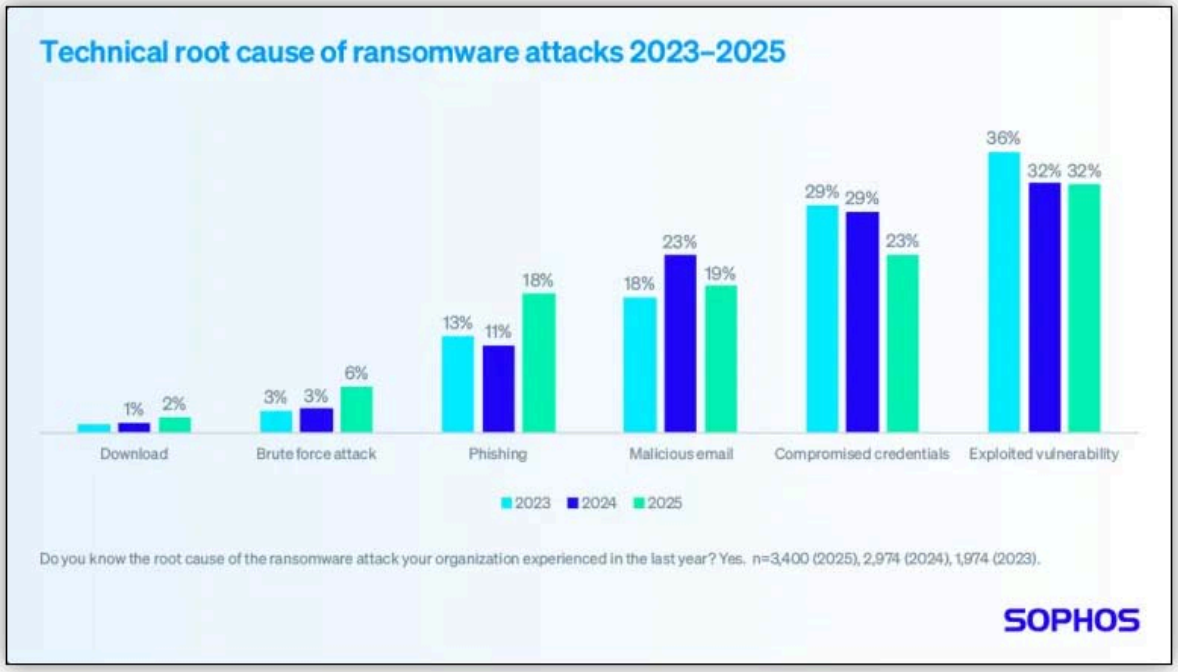
We covered a similar problem with RAR and WinRAR many years ago, and I recall that by the time we reported about it, that problem was under active exploitation so fixing it was imperative. This time, RAR users have the opportunity to get ahead of that day.

My Win10 machine had v5.18. The installer simply overwrote that with the newer version. Registration remained intact and I now have a much more current release of RAR.

https://haveibeenpwned.watch/
And speaking of infographics, I have a cool new site for everyone to check out. A security engineer named George-Andrei Iosif who's with Snap has created "haveibeenpwned.watch", a portal to display the data from the haveibeenpwned.com database in easy-to-understand graphs.

The headline of his page reads: *"Open-source, no-fluff charts showcasing haveibeenpwned.com's pwned account data."* His charts support mouse hovers, so you can further explore the charts.

Sophos ransomware attacks root causes:



Sophos produced a very nice infographic in barchart form. Among each of six possible technical root causes of eventual ransomware attack, it breaks down the percentage of each for the most recent three years, 2023, 2024, and 2025 year-to-date. The way they broke the data down, using bar charts to show percentages that total 100% is difficult to parse. So I wish they had shown this as three pie charts, one for each year. Then we could easily see the percentage for the year overall as well as how the three pies compare. But no such luck.

In any event, the six categories, in order of clearly increasing incidence, regardless of the year, are: Download, Brute force attack, Phishing, Malicious email, Compromised credentials and Exploited vulnerability. Regardless of the year, one category "Exploited vulnerability" was responsible for 1/3rd of all ransomware attacks. Compromised credentials took a strong second place. And in fact, for every year, the sum of Exploited vulnerabilities and Compromised credentials accounted for over half of all six causes, regardless of the year.

There were slight differences in the percentages, but no huge pattern. So we don't appear to be doing better. In fact, the reverse is clearly the case. Since these bars represent percentages we don't see absolute numbers. But down in the fine print of Sophos' caption we see the 'n' values for the number of ransomware attacks tracked. For 2023 that was 1,974. For 2024 it was 2,974 – exactly 1,000 more during 2024 than 2023. And for 2025 year-to-date we're already at 3,400.

I would imagine that our long-time listeners can probably feel this too. It doesn't feel as though the good guys are winning.

Windows Endpoint Security without Kernel access

We were recently remembering last July's Windows mess which was triggered by a flaw in CrowdStrike's endpoint security system. It resulted in the more than eight and a half million Windows systems crashing hard and staying crashed hard. Although we should be sensitive to the fact that this is no longer the official term for such events. I'm pretty certain Microsoft would prefer that we refer to those 8.5 million systems as taking an unplanned group vacation.

In any event, once those 8.5 million machines returned from vacation and went back to work,

Microsoft hosted in September the Windows Endpoint Security Ecosystem Summit (WESES). That summit assembled a diverse group of endpoint security vendors and global government officials to discuss strategies for improving resiliency and protecting our mutual customers. In other words, "How the 'F' do we prevent ***THAT*** from ever happening again?"

And this brings us to today's news. Microsoft is close to launching a new security platform. Next month they will begin privately previewing their new technology that will allow antivirus and security tools to run without kernel access. As we know, this has been the great challenge for Windows.
To provide truly strong endpoint security, 3rd-party vendors need to dig deep into the OS to get their hooks into all of the various APIs that malware might attempt to abuse. This is not something that any operating system kernel wants to permit – for precisely the reasons that befell all of Microsoft's and CrowdStrike's customers last summer. But Microsoft has been caught between a rock and a hard place because they have also been unwilling – until now, apparently – to provide any workable alternative solution to deep API kernel hooking. We are being told that this will finally be changing. We'll see.

Proactive age verification is coming
The U.S. Supreme Court just upheld a contentious Texas law requiring proactive age verification before accessing pornographic content on the Internet. And as I've noted before, this is fundamentally different from mom and dad setting the dates of birth into Jonny's and Sally's phones so that they will be able to use Facebook. This is Mommy and Daddy needing to prove **their own ages** to some of the web sites they have every legal right to visit.

This is made tricky by the fact that at the moment we have no technology for providing anonymous age verification, and the challenge of providing unspoofable anonymous age verification remains an unsolved problem.

WIRED's coverage of this had the headline *"US Supreme Court Upholds Texas Porn ID Law"* and the subhead *"In a 6-3 decision, the Supreme Court held that age verification for explicit sites is constitutional. In a dissent, Justice Elena Kagan warned it burdens adults and ignores First Amendment precedent."* The first 4 paragraphs of WIRED's coverage reads:

> *If you try to access Pornhub, one of the world's biggest websites, from any of 17 US states, you'll be blocked. Pornhub's parent company, Aylo Holdings, has restricted access in response to a slew of laws that says Pornhub itself should be responsible for checking that every visitor is over 18. Now, the United States Supreme Court has made a decision on a key age verification law, which could have ramifications for the entire country and the wider internet as a whole.*
>
> *On Friday, in a 6–3 decision that could reshape the landscape of online privacy and free speech, the Supreme Court upheld in full the Texas age verification law—one of the first passed in the country—requiring many websites publishing pornographic content to check that* ***all*** *visitors are over 18. The law, Texas HB1181, says sites that are "more than one-third sexual material" can face fines of up to $10,000 per day if they don't put in place age verification systems, plus extra penalties of up to $250,000. It also states websites should display health warnings about the potential health risks of pornography.*
>
> *Writing for the majority, Justice Clarence Thomas said that because the law "simply requires proof of age to access content that is obscene to minors, it does not directly regulate adults' protected speech," adding, "adults have no First Amendment right to avoid age verification."*

In her dissent, Justice Elena Kagan argued that the Texas law imposes a direct and unconstitutional burden on adults' access to protected speech. "A State may not care much about safeguarding adults' access to sexually explicit speech; a State may even prefer to curtail those materials for everyone," she wrote, "but the First Amendment protects those sexually explicit materials, for every adult."

I had no idea that Pornhub could be described as one of the world's biggest websites, but I did a bit of checking and, sure enough, it is.
It seems clear to me that this creates a market in the short term for VPN services which provide for virtual Internet relocation. And I suppose that anyone living in any of those 17 blacked-out U.S. states who wishes to obtain access to this proscribed content will have already found a way to appear to be connecting from a non-blacked-out location. But I said "in the short term" because VPN services operating within the United States are also subject to the law. And the law doesn't say "no one connecting from within Texas" it says "no one residing within Texas." So once the use of VPNs for geo-relocation becomes commonplace, we can expect our duly elected representatives to close that loophole too.

This will be interesting to watch, and it's another intractable mess we've gotten ourselves into where the cyberworld collides with the physical world.

Canada says goodbye to Hikvision
Hikvision is another controversial Chinese company. They manufacture security cameras and the Canadian government has just ordered them to close their Canadian operations. Canadian officials said that the company's business is a threat to Canada's national security and banned government agencies from purchasing new Hikvision products. As we know when we covered this previously, the US sanctioned Hikvision for aiding the Chinese government's surveillance of the Uyghur minority in Western China.

Germany seeks to ban DeepSeek
Meanwhile, Berlin Germany's data protection agency is seeking to ban DeepSeek throughout Germany over its illegal transfer of user data to China. Germany's data protection agency has reported both apps to the Apple and Google app stores for GDPR violations. According to CNBC, this initial action in Germany may lead to a European Union wide ban on DeepSeek.

Cloudflare "throttled" by Russia
Early last month Russian ISPs began throttling traffic from Cloudflare to their customers. And when I say "throttling" I don't mean forcing pages to load more slowly. Russian ISPs are only allowing 16K bytes of data to load from a page before completely blocking anything more. These days, you can't get much done in 16 Kbytes. The only rationale that I could imagine would be that it would be possible to have a Cloudflare site return an HTTP redirect to a Russian- located site. So perhaps that was the idea. Any Russian sites hosted by Cloudflare could rehost themselves in Russia and redirect any previous Cloudflare visitors to their Russian site. But just re-pointing their domain to a Russian Hosting IP would seem easier.

Sci-Fi

Having caught up with Ryk Brown's Frontiers Saga series, over the weekend I started into my re-read of "Project Hail Mary". I had forgotten how much I must have enjoyed it the first time, since I'm astonished by how much fun I'm having with this book.

My life, Lorrie, loved "The Martian" and she had been looking for something to read. I don't think she really paid much attention when I read Project Hail Mary the first time. Perhaps she was in the middle of some other book. But when I came home last week with the news of the trailer and we started to watch it, she stopped me half way through because she didn't want any spoilers. She wanted to read the book. She finished it this weekend and really enjoyed it.

So, for what it's worth, anyone listening to as geeky a podcast as this, who obtains pleasure from reading or listening to books, will likely love Andy Weir's writing, his science and his humor. I missed reading Andy's second book, Artemis, when it was released eight years ago in 2017. I must have been deep into some other series at the time. But I'm not now. So once I finish my reread of Hail Mary I plan to follow that with Artemis.

Going on the Offensive

This podcast has often wondered what's going on with the United State's cyberwar posture.

We're endlessly covering China's intrusions into U.S. networks and all the trouble that causes for us, here. We recently looked at the concerns over the discovery of undocumented radios turning up in Chinese-made power inverters used in wind and solar energy production. Chinese-made security cameras are being increasingly banned from sensitive locations and we've worried about the ubiquitous presence of DJI drones being used on military bases and other sensitive areas.

What I wonder is whether similarly cyber-aware Chinese citizens located in China – essentially our counterparts – are covering the same sorts of stories about intrusions, plotting and planning by the U.S.? Because we're here in the U.S. we don't have the same visibility into U.S. operations in China as we do into China's operations in the U.S. So I've often wondered whether the U.S. is giving as well as it's getting? Are things balanced? Is China worrying about us as much as we're worrying about them?

Before we go any further I always want to be clear that this entire subject area, necessary as it is, always makes me feel a bit queasy. I know we have Chinese listeners and there are very few things in this life that feel more unjust to me than racism. So I want to be crystal clear here that in every instance we're talking about the actions of our respective governments and their militaries – not their people – not American citizens or Chinese citizens or Chinese/American citizens. This will never have anything to do with ethnicity. Although democracies elect their leaders, those leaders don't always do what many of those they lead wish they would. So we fill out our ballots and hope for the best.

I ran across a fascinating document which was prepared by Winnona DeSombre Bernsen, a Former security engineer at Google's Threat Analysis Group, the founder of the offensive security conference DistrictCon, held in Washington DC, and she has organized policy content at DEFCON and authored multiple pieces on offensive cyber capability proliferation. She's a fellow at the "Atlantic Council", a Washington D.C. based policy think tank, and in that capacity she interviewed a sobering list of people whom she lists at the end of her piece. In many cases she's only able to use their approximate titles because of the sensitive nature of their positions within the U.S. government or military.

She titled this piece: *"Crash (exploit) and burn: Securing the offensive cyber supply chain to counter China in cyberspace"*. Note her use of the term "offensive cyber supply chain" – in other words: how can the United States reliably obtain the tools (exploits) we need to attack others.

The PDF of this report is 44 pages and I've placed a link to that PDF in the show notes for anyone who wishes to dig deeper. The report is perfectly organized for the harried policy pusher, It makes all of its points quickly then backs them up with data and specifics. So I only need to share the beginning of this well- organized, lengthy, in-depth and detailed report since it contains a ton of very interesting insights and specifics that we've never covered here before.

The report begins by posing a question as the report's thesis:

> *If the United States wants to increasingly use **offensive** cyber operations internationally, does it have the supply chain and acquisition capabilities to back it up—especially if its adversary is the People's Republic of China?*

Strategic competition between the United States and China has long played out in cyberspace, where offensive cyber capabilities, like zero-day vulnerabilities, are a strategic resource. Since 2016, China has been turning the zero-day marketplace in East Asia into a funnel of offensive cyber capabilities for its military and intelligence services, both to ensure it can break into the most secure Western technologies and to deny the United States from obtaining similar capabilities from the region. If the United States wishes to compete in cyberspace, it must compete against China to secure its offensive cyber supply chain.

This report is the first to conduct a comparative study within the international offensive cyber supply chain, comparing the United States' fragmented, risk-averse acquisition model with China's outsourced and funnel-like approach. Our key findings are:

- *Zero-day exploitation is becoming more difficult, opaque, and expensive, leading to "feast-or-famine" contract cycles.*
- *Middlemen with prior government connections further drive up costs and create inefficiency in the US and Five Eyes (FVEYs) market, while eroding trust between buyers and sellers.*
- *China's domestic cyber pipeline dwarfs that of the United States. China is also increasingly moving to recruit from the Middle East and East Asia.*
- *The United States relies on international talent for its zero-day capabilities, and its domestic talent investment is sparse – focused on defense rather than offense.*
- *The US acquisition processes favor large prime contractors, and prioritize extremely high levels of accuracy, trust, and stealth, which can create market inefficiencies and overly index on high-cost, exquisite zero-day exploit procurements.*
- *China's acquisition processes use decentralized contracting methods. The Chinese Communist Party (CCP) outsources operations, shortens contract cycles, and prolongs the life of an exploit through additional resourcing and "n-day" usage.*
- *US cybersecurity goals, coupled with "Big Tech" market dominance, are strategic counterweights to the US offensive capability program, demonstrating a strategic trade-off between economic prosperity and national security.*
- *China's offensive cyber industry is already heavily integrated with artificial intelligence (AI) institutions, and China's private sector has been proactively using AI for cyber operations.*
- *Given the opaque international market for zero-day exploits, preference among government customers for full exploit chains leveraging multiple exploit primitives, and the increase in bug collisions, governments can almost never be sure they truly have a "unique capability."*

So it feels as though there may be an inherent conflict between the traditional way the U.S. military has conducted business and the faster, more furious and significantly less certain way the 0-day cyber-marketplace functions. It also sounds as though the U.S. may still be stuck in a *"but we're the good guys"* mindset whereas China's management may evidence more of a *"just get it done"* style which more closely aligns with the realities of cyber.
Winnona next lists three recommendations, writing:

- *Strengthen the supply chain by creating Department of Defense (DOD) vulnerability research accelerators, funding domestic hacking clubs and competitions, expanding the National Security Agency's (NSA) Centers of Academic Excellence in Cyber Operations (CAE-CO) program, and providing legal protections to security researchers.*

- *Improve acquisition processes by establishing a government-sponsored vulnerability broker in a federally funded research and development center (FFRDC) to decentralize and simplify exploit purchases while increasing cyber capability budgets and expanding research on automated exploit chain generation.*

- *Adjust policy frameworks to consider counterintelligence strategies in the zero-day marketplace (burning capabilities of malicious actors while recruiting willing 'responsible' actors into a more formal pipeline), funding n-day research through US Cyber Command (USCYBERCOM) where appropriate and leveraging alliances to counter China's growing cyber dominance.*

That all appears to amount to *"we need to be getting serious right now about 0-day exploit acquisition. That's where all the action is and where it's going to be. And we're going to be in trouble if we don't rearrange our operations and priorities right away."* She concludes:

Without meaningful reforms, the United States risks ceding to China whatever strategic advantage it has left in cyberspace. By fostering a more deliberate offensive cyber supply chain and adjusting acquisition strategies, the US can retain a steady supply of offensive cyber capabilities to maintain its edge in the digital battlefield.

It's unclear to me where the assumption comes from that the U.S. currently has any "edge" at all in the digital battlefield. We don't know what we don't know. But I wonder if this isn't a bit of soft pedaling so as not to ruffle too many higher-up feathers?

Her report then provides a pair of pull-quotes to set the stage for a bit more background. The first quote is from Alexei Bulazel, incumbent special assistant to the president and National Security Council senior director for Cyber. Alexei says: *"America has incredible offensive cyber power. We need to stop being afraid to use it."* I dearly hope that America has incredible offensive cyber power and that the only reason we haven't seen more evidence of it is that we've been afraid to use it. That suggests that it might be available if and when needed.

Jeremy Fleming, former GCHQ director is quoted saying: *"Geopolitical conflicts are increasingly shifting to cyberspace, including tensions between the U.S. and China. Technology is therefore no longer just an area for opportunity, but also a battleground for control, values and influence."*

Okay. So here's the background Winnona provides to preface her more detailed analysis that follows. She writes:

China and the United States are engaged in strategic competition in cyberspace. While cyber operations are often an overlooked area of geopolitical power, both countries' militaries, intelligence communities, and law enforcement agencies conduct cyber operations. They do so to obtain intelligence crucial to national security, assist conventional military operations, and even create kinetic effects to achieve strategic goals. To make a cyber operation possible, one must have the capacity to break into a particular system: offensive cyber capabilities (and particularly zero-day vulnerabilities) are the necessary strategic resources required to conduct

such operations.

The United States clearly wishes to further leverage its cyber prowess in the international arena, particularly against the People's Republic of China (PRC). Doing so would help the United States protect its vital national security and economic interests, international partnerships, and norms. However, to operationalize a "cyber power" strategy, the United States must acquire enough high-end capabilities to ensure it can achieve such strategic goals. Moreover, the timeline for implementing these policies is urgent, given the increasing potential for conflict with China in the coming years. Thus, given the international privatized offensive cyber capability marketplace, how can the United States and its allies continue to ensure the availability of offensive cyber capabilities (focusing on zero-day vulnerabilities), while limiting China's access to those same capabilities?

Cyber operations consist of a variety of offensive cyber capabilities — many of the most crucial cyber capabilities involve the exploitation of "zero-day" vulnerabilities (also known as zero-days or 0days). Zero-day vulnerabilities are issues or weaknesses ("bugs") in software or hardware, typically unknown to the vendor and for which no fix is available— in other words, the vendor has had "zero days" to fix the issue. Some of these vulnerabilities are exploitable: an actor with knowledge of the vulnerability could write code that takes advantage of said vulnerability. This results in a "zero-day exploit"—code enabling a range of behaviors that could include establishing access into the computer system the software is installed on, escalating privileges on those systems, or remotely issuing commands.

The work of finding vulnerabilities and writing exploits, thanks to its strategic necessity to governments worldwide, has become a billion-dollar international services industry in the last 20 years. Private firms now often create cutting-edge offensive cyber capabilities for governments. Given the sensitivity around supporting government cyber operations, many of these firms do not openly advertise their services, shrouding the industry in secrecy. Between this secrecy and the variation in products offered (i.e., governments target different technology systems, and no two zero-days are identical), the supply chain for such capabilities is not only opaque to outsiders, but also to governments and even among players in the industry.

Within this highly fragmented and opaque market, large firms, like the United States' L3Harris or ManTech, frequently hold multi-million dollar valuations. Notably, Israel's NSO Group's worth reached $1 billion at its peak. Meanwhile, individual US government agencies receive millions of dollars to procure offensive tools. Such companies' tools have clearly been purchased by such government agencies and put to use in modern-day cyber operations. Notably, of all the zero-day vulnerabilities found exploited "in-the-wild" in 2023 and 2024 by Google, around 50 percent of them were attributed to commercial vendors that sell capabilities to government customers. While this statistic only encompasses detected zero-day exploits, this is still a significant set of capabilities being provided by private sector actors.

The offensive cyber capability industry itself is international and ranges in professionalization depending on the region; companies in Russia, Israel, Spain, Singapore, and the United States all have varying relationships with their home governments, other firms (including middlemen and brokers), international government customers, and even cyber-criminal groups. However, the study of offensive cyber capabilities has largely over-indexed on firms based in Israel and Europe rather than the United States' greatest geopolitical rival: China. This is surprising, as the Chinese hacking and cybersecurity ecosystem is robust. Chinese companies have, on multiple occasions, been directly linked to Chinese government-sponsored cyber operations against the United States. Moreover, the development of offensive cyber capabilities in the

United States remains largely unstudied or examined in a way that does a disservice to the domestic hacker community.

Why is this question important? At first glance, it can be difficult to see why the private sector zero-day exploit market—a series of obscure companies selling code that can enable governments to break into widely-used software—would be important in preserving national interests in cyberspace, particularly against China. A simple explanation of this relationship is as follows: the United States and its allies rely on an increasingly digital world, and China is both a savvy adversary and hardened target in cyberspace. When any country's intelligence community wishes to infiltrate high-value, hard-to-access digital targets, it likely must use zero-day exploits or other bespoke (in other words custom-made or tailored) offensive cyber capabilities. Intelligence organizations from both the United States and China, due to decreasing internal supply and rising demand for such capabilities, have increasingly relied on acquiring such exploits from the private sector zero-day exploit market. However, the private sector zero-day market is murky and more international than policymakers expect; even if the United States and China are truly entering a "New Cold War," both countries still source these capabilities from an overwhelmingly opaque international market of offensive cyber capability firms, and do not know if they are being supplied with potentially overlapping capabilities. In short, any cyber operation that relies on an acquired capability, conducted by the United States, China, or anyone else, carries a counterintelligence and operational security risk, with no guarantee that they can source a similar capability in the future.

Thus, securing the cyber supply chain – which means understanding the industry, constraining malicious actors, and ensuring availability from trusted parties – is important to address such risks.

While former President Joe Biden's administration sought to constrain private sector actors with additional regulation and placing bad actors on the entities list, these policies were framed around human rights concerns largely out of Europe and Israel. President Donald Trump's administration is moving away from this approach, focusing on China as a geostrategic threat over transnational digital repression framings, as well as signaling willingness to engage with private sector actors in the space. The Trump administration, as of 2025, has accelerated plans for a US Cyber Command (USCYBERCOM) 2.0, focusing on working better with private industry partners. This is a continuation of the first Trump administration's policies: Trump was the first president to delegate the authority for offensive cyber operations down to the secretary of defense (through National Security Presidential Memorandum–13) allowing USCYBERCOM more leeway to conduct operations without presidential approval, albeit still with a robust interagency review process.

If the United States wishes to further leverage its cyber prowess in the international arena by leveraging private sector partners, does it have the supply chain and acquisition capabilities to back it up—especially if its adversary is the People's Republic of China? Although the author does not condone general analogies between cyber and other domains, supply chain and acquisition analysis in the cyber domain can be similar to nuclear or other arms proliferation questions. For example, to answer whether a country has the capability to construct a nuclear weapon, one must understand how much enriched uranium the country can easily acquire. Similarly, to answer whether a country can become a cyber power that can access the hardest of digital targets, one must ask how easily it can source and acquire zero-days and other offensive cyber capabilities.

Winnona made many assertions in what I just read. In nearly every case those assertions were followed by a reference to their source. So none of this was just her opinion, regardless of how well informed it might be.

So we have a somewhat bizarre new world were governments need to purchase newly discovered 0-days vulnerabilities from anywhere they can be purchased. And where the "anywhere they can be purchased" is an entirely ad hoc mish-mash of entities, from someone in their mother's basement to an international weapons dealer or a public government contractor. If we were to extend Winnona's uranium acquisition analogy a bit, this would be analogous to tens of thousands of individuals, each with their own little backyard uranium enrichment operation, who then sell what they've created to the highest bidder, or to someone they trust.

She offered some interesting numbers to give us a sense of scale of what's going on today:

> *Live hacking competitions (where hackers hack into systems live on stage), and bug bounty programs (usually company-run reward programs that encourage hackers to find and report system vulnerabilities) enable hackers to develop similar skill sets as those required for government-sponsored hacking. These programs and competitions are both common recruiting pipelines for defensive cybersecurity companies and offensive vendors alike.*
>
> *The number of individuals that participate in such programs globally is staggering. In 2020, HackerOne, a well-respected bug bounty platform, reported around 600,000 contributors spanning 170 countries. A 2024 survey by Bugcrowd, one of the largest bug bounty and vulnerability disclosure companies on the internet, revealed most of Bugcrowd's over 200,000 hackers hailed from India, Egypt, Nigeria, Pakistan, Nepal, Vietnam, Australia, and the United States; 78 percent of them are self-taught, and 58 percent of them were under twenty-five years old. While not all of these individuals possess the skills to find zero-day vulnerabilities and write code to exploit them, multiple security experts interviewed estimated that there are likely thousands of international individuals able to do so, with numbers in the low hundreds that can be trained to do so well.*

So we have an informal community of hackers who are potentially able to make a bunch of money. But as the saying goes, "don't quit your day job". Winnona provides some interesting background to that, writing:

> *While selling offensive cyber capabilities (and particularly zero-day exploits) to governments is a lucrative profession, it is a risky industry. Creating a zero-day exploit to leverage against a widely used technology product may require between six and eighteen months of full-time engineering and research work. Unless an offensive cyber capability firm has multiple engineers working on different products or uses different payment schemes, this timeline can lead to long downtimes between exploit sales. This "feast-or-famine" payout schedule carries risks for companies that rely on one or two windfalls a year to pay their overhead and engineering costs.*
>
> *In addition, finding a customer to sell exploits to is more difficult than it first seems. In general, potential sellers must find an existing government contract through which to sell their exploits or know the right government individual to speak with. Unless an offensive cyber capability firm has hired employees who have recently left a government interested in such capabilities, actual buyers may be extremely hard to find. Thus, international hackers without former government connections normally sell their products to middlemen, many of whom operate internationally. Even then, the exploit may go through multiple levels of middlemen to*

get to a government customer, frustrating both buyers and sellers. Buyers know that exploits sold to them have extremely high mark-ups, given the number of middlemen involved, and often will not know who the original bug producers are. Meanwhile, sellers are likely aware of the extreme markups, but do not know whether their bugs were sold to multiple governments.

She quotes a former official with the Office of the National Cyber Director saying: *"An individual researcher who isn't informed on what bugs are selling for may sell a good bug for 100k. By the time it makes it to a customer, an individual bug could go for 750k to 1 million dollars."* And a senior DOD official working on offensive cybersecurity research programs is quoted, saying: *"The system by which zero day vulnerabilities are acquired is horrendously inefficient and broken."* So we learn that there's a system of middlemen who are not contributing anything meaningful beyond their connections and contacts within government. And they almost certainly owe their loyalty only to the dollar and not to any nation. Nothing prevents them from double- dipping.

We know that money motivates. So if a program existed to cut out the middlemen, to protect hackers legally and to allow governments to purchase those vulnerabilities directly, hackers could make ten times the money and have ten times the motivation. They would also have the assurance that their work would only go to help the country they wish to help, and not their country's enemies.

The problem is that there's a well-deserved prevalent mistrust of government within the hacking community. Winnona reminds of a bit of this past, writing:

Undermining all these efforts is the anti-government sentiment that remains strong within the US cybersecurity and hacking community, which likely contributes to difficulty in maintaining an offensive talent pipeline. Much of the original US hacking community emerged from counter- cultural activities like phone phreaking (i.e., bypassing Pacific Bell telephone lines to make long-distance phone calls without paying).

Law enforcement responses from the 1960s to the early 2000s treated many hackers as criminals rather than innovators. In 1990, the Secret Service's Operation Sundevil seized more than forty computers and 23,000 data disks from teenagers in fourteen American cities and charged individuals who managed the hacker magazine "Phrack" with interstate transport of stolen property. The charge was based on information published by Phrack that later proved to have been already publicly available.

The arrests and subsequent court cases resulted in the creation of the Electronic Frontier Foundation. While the US government has made significant strides toward repairing the relationship with domestic hackers in recent years, anti-government sentiment still persists.

So, yeah, Uncle Sam ... you've been the big bad bully in the past ... and now you want and need the brains of those people whose rights and freedoms you blithely ignored out of your own fear of the unknown.

There is so much fantastic content in this 44-page paper that I've had to skip over. So all I can do is commend this to any of our listeners who are interested to know more. The paper goes into much more depth about the many significant challenges presented by the way the U.S. is organized versus the comparative ease that China's processes face. So I'm going to settle for sharing the paper's findings. Winnona writes: *"During the literature review, data analysis, and expert interviews (as laid out in the above sections), nine key findings emerged:"*

1. ***Zero-day exploitation is becoming more difficult, opaque, and expensive.*** *The global hacking ecosystem is highly international and fragmented. The amount of time and capital required to develop an impactful capability has escalated dramatically in the last decade, leading to riskier feast-or-famine contract cycles. The growing number of publicly discovered zero-day threats does not detract from this market trend, in fact, the increase suggests a concurrent rising number of players in the international market. Multiple sources interviewed estimate the number of individuals consistently producing zero-day exploits is in the low hundreds globally.*

2. ***Middlemen create market inefficiency and erode trust in the market.*** *Given the lack of transparency in the zero-day market, middlemen with prior government connections further drive up costs and create inefficiency in the US and FVEYs market, while eroding trust between buyers and sellers.*

3. ***The United States relies on international talent, while China relies on domestic might.*** *The US offensive cyber workforce relies heavily on international talent pools in South America, Europe, and other FVEYs countries. China's domestic cyber pipeline dwarfs that of the United States, but China is also increasingly moving its supply network out to the Middle East and East Asia.*

4. ***Talent investment in US offense is lacking.*** *US government investment into the offensive talent pipeline, however sparse, has focused on defensive jobs, whereas China has well established and comprehensive feeder systems within its offensive apparatus. US talent in exploit development also experiences a "Training Valley of Death" between junior and intermediate levels.*

5. ***US acquisition favors large prime contractors, slows acquisition in pursuit of stealth, and adds additional risk through opacity.*** *US cyber capability acquisition favors large defense contractors, who take on heavy compliance burdens while shifting project requirements to smaller firms. The US government internally prioritizes extremely high levels of accuracy, trust, and stealth, which can create market inefficiencies and a reliance on high-cost, exquisite zero-day exploit procurements. Certain US government customers deliberately lengthen the contract cycle by refusing to share information about desired capabilities with firms, leading to an inefficient process where firms may work on an exploit that a customer has no intent to purchase.*

6. ***China's acquisition uses decentralized contracting methods, outsources operations, shortens contract cycles through additional resourcing, and prolongs the life of an exploit through "n-day usage."*** *While China also relies on large prime contractors, government ministries have decentralized government procurement processes, such that even provincial government offices issue contracts to firms. China's regulatory environment actively encourages vulnerability reporting to the state, often integrates corporate research with government offensive strategies, and widely enables private sector hack-for-hire operations. China has also shortened the feast-or-famine contract cycle for exploits by providing additional resources to its private sector firms, and it continues to use exploits after their discovery.*

7. ***US cybersecurity goals, coupled with Big Tech's dominance, are strategic counterweights to the US offensive capability program****. Because zero-day exploits in cyber operations take advantage of weaknesses in private sector software products, the global market dominance of the US Big Tech companies ensures that, as such, they act as a strategic obstacle to US offensive cyber goals. This demonstrates a strategic trade-off*

between economic prosperity (and global trust in US products), and national security. In contrast, China's tech firms have a far less global market share, and they are a strategic enabler of China's offensive cyber program.

8. ***International partnerships for unique offensive cyber capabilities attempt to leverage different circles, but the opaque market offers no guarantees.*** *The United States leverages international alliances, particularly within the FVEYs intelligence-sharing network, to bolster its cyber capabilities. In contrast, China focuses on cultivating regional influence and integrating offensive cyber capabilities from East Asia and the Middle East. However, given the opaque international market, preference for full chains leveraging multiple exploit primitives, and the increase in bug collisions, there is no 100 percent guarantee of unique capability.*

9. ***China leans forward on AI in cyber operations.*** *China's offensive cyber industry is already heavily integrated with AI institutions, and China's private sector has been proactively using AI for cyber operations. The US government's primary efforts with both AI and cyber have largely been defensive in nature, or within the intelligence community internally, although some DARPA programs have encouraged open offensive innovation.*

https://www.atlanticcouncil.org/in-depth-research-reports/report/crash-exploit-and-burn/

So what we come away with is a much better appreciation for what's going on out in the world of offensive cyber warfare.

Offensive cyber warfare is 100% about penetrating into one's perceived adversary's networks. And that, in turn, is all about leveraging exploitable 0-day – which is to say currently unknown – vulnerabilities in those networks.

What's really interesting is that there's an inherently level playing field when it comes to discovering those potentially ultra-valuable 0-day exploits. Anyone, anywhere, can make a discovery of a flaw in software, then work to engineer that into a working exploit. At that point the holder of that intellectual property has an asset worth, potentially, a million dollars. But only if that intellectual property can be conveyed to a deep-pocketed government that, in turn, has the means to exploit that for its own ends.

Today, opportunists – who may provide some value such as mutual anonymity for both the buyer and the seller – take the lion's share of the value for a hacker's work because only they are able to turn that highly valuable and volatile intellectual property into cash. Hackers who receive only ten cents on the dollar are much less incentivised to hunt down tomorrow's exploit, yet what we have learned is that offensive cyber warfare is all about having that next exploit. It's called a "supply chain" because it creates a supply and that's what it needs to do.

It's clear that the U.S. government itself needs to emerge from the shadows. It needs to become a well advertised high-value explicit buyer of 0-day exploits. Period. It needs to put the middlemen out of business. It needs to provide irrevocable protection to any hackers against any form of blowback for their work in discovering valuable cyber attack tooling. It needs to be widely known that it's possible to become wealthy from selling 0-day exploits to Uncle Sam. This is not the world I wish we had, but it's today's reality. If having a strong deterrent helps to keep the peace, then let's get one.