Security Now! #1014 - 02-25-25

FREEDOM Administration Login

This week on Security Now!

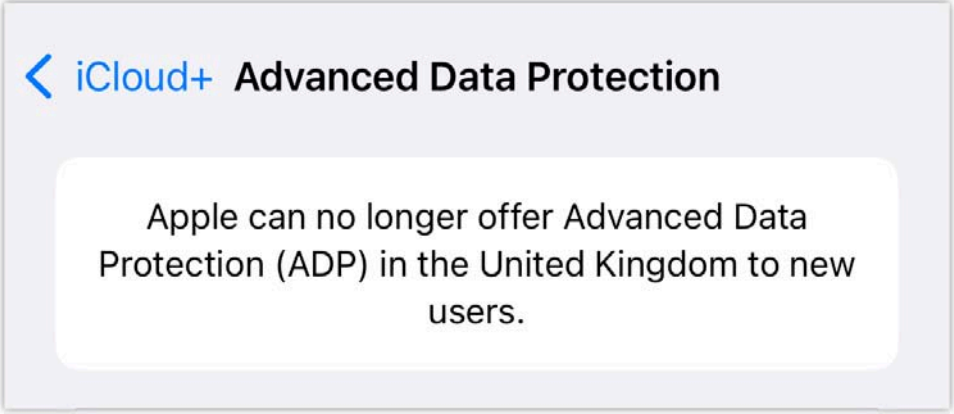
- Apple disables Advanced Data Protection for new UK users.
- Paying ransoms is not as cut and dried as we might imagine.
- Elon Musk's "X" social media blocks "Signal.me" links.
- Spain's soccer league blocks Cloudflare and causes a mess.
- Two new (and rare) vulnerabilities discovered in OpenSSH.
- The U.S. seems unable to evict Chinese attackers from its Telecom systems.
- What are those Chinese "Salt Typhoon" hackers doing to get in?
- The largest (by far) cryptocurrency heist in history occurred Friday.
- Ex-NSA head says the U.S. is falling behind on the cyber front lines.
- We have the winner (and a good one) replacement term for "backdoor".
- A look at a pathetic access control system that begs to be hacked (and will be).

We have a new entry into the ever popular
“Where there’s a will, there’s a way” contest!

Security News

Apple disables Advanced Data Protection for new UK users

This is wonderful news. Better news would have been that the UK decided to back off from their demand that Apple arrange to provide access to the encrypted stored iCloud backup data of anyone, anywhere, for whatever purpose they might have. But that hasn't happened, at least not yet. So Apple took the next step in this dance that **has** had to happen. One way or another, the world needs to work out this issue about governments believing that they have the right to breach the privacy of anyone they choose.



BBC News reported that ADP stopped being an option for new users starting at 3 p.m. U.K. time, Friday. Other outlets have subsequently confirmed that ADP is no longer an option for new users in the United Kingdom.

In response to the news, our Johns Hopkins cryptography professor, Matthew Green, posted on 'X': *"If you are not in the U.K., you should turn on ADP now. The more people who use it, the harder it will be to shut off this way."*

So what do we know? We learn a few more things from the BBC's subsequent reporting:

> *No one in the U.K. can now activate Advanced Data Protection and existing users' access will be disabled at a later date.*

My own opinion is that this is Apple intentionally not dropping the other shoe. This incremental move allows them to wait a while to see what the U.K. chooses to do next. There is little doubt that this move that's been forced upon Apple is not going to be widely embraced with great joy among the U.K.'s voting citizenry. The U.K.'s parliament now realizes that if Apple is **also** forced to take the next step of disabling all **existing** ADP-enabled encryption across the U.K., that's going to have a FAR greater negative impact with the U.K.'s politicians being directly blamed for forcing Apple to take away privacy guarantees that they previously enjoyed. And since enabling ADP is something one needs to do deliberately, it will be those who most want it who will be having it removed.

I'm sure Apple is holding out hope that that won't be necessary. If this first move by Apple is sufficient to have called the U.K.'s bluff, to very clearly demonstrate that it's not joking about this and that it will proceed with removing all remaining iCloud ADP encryption – and only for then disadvantaged U.K. citizens – then Apple can avoid backtracking on existing encryption and can simply resume allowing those who want to turn it on to do so. But I'm sure it's quite clear to everyone now that Apple holds all the cards here. The BBC's reporting said:

It is not known how many people have signed up for ADP since it became available to British Apple customers in December 2022. Professor Alan Woodward - a cyber-security expert at Surrey University - said it was a "very disappointing development" which amounted to "an act of self harm" by the government. He told the BBC: "All the UK government has achieved is to weaken online security and privacy for UK based users" and that it was "naïve" of the UK to "think they could tell a US technology company what to do globally."

Opinions on this are mixed, however. The BBC reported that online privacy expert Caro Robson said she believed it was "unprecedented" for a company "simply to withdraw a product rather than cooperate with a government." [well, that's true, it is unprecedented, which is precisely why the entire world has desperately needed this precedent to be set. Robson told the BBC:] *"It would be a very, very worrying precedent if other communications operators felt they simply could withdraw products and not be held accountable by governments."*

I don't think there's anything "worrying" about it. This is precisely what Apple needed to do. And we already know that Signal and others would follow in Apple's footsteps. The BBC said:

Meanwhile, Bruce Daisley, a former senior executive at X, then known as Twitter, told BBC Radio 4's PM programme: "Apple saw this as a point of principle - if they were going to concede this to the UK then every other government around the world would want this."

Exactly. We could not ask for a better test case setup: New users are being told they can't have it. Existing users are at risk of losing it. Your move, U.K.

There is a downside / darkside to this, however, which does temper my enthusiasm. What if the democratically elected politicians within the U.K. decide that they know better than their own citizens? What if they shrug off this first step toward Apple's removal of ADP, forcing Apple to take the next step of requiring all existing U.K. users who have ADP enabled to disable it? What then?

Some other reporting on this quoted Mike Chapple, an IT professor at the University of Notre Dame's Mendoza College of Business and a former computer scientist at the NSA, noted that this episode illustrates *"one of the fundamental flaws in government efforts to undermine encryption. Faced with having to choose between security and complying with government regulations, companies like Apple tend to remove security features entirely."* And here's the worry, Chapple noted that: *"The net effect is reduced security for everyone. If other governments follow the UK's lead, we risk a future where strong encryption is functionally outlawed, which puts all of us at risk not just to government surveillance but also to eavesdropping by other bad actors."* In other words, I've been assuming that the UK's elected parliament would lose this fight with Apple and that the rest of the world would take note. But what if I'm the one who's being naïve, we learn that people don't really care all that much about encryption so long as they're able to check how many "likes" they've received, and that they're fine with trusting their governments to do the right thing.

We need to accept that this Apple/UK standoff might very well break that way too, and that other governments would then learn exactly the **wrong** lesson, and immediately make similar demands... thus forcing a general global retreat on all encryption privacy guarantees.

Paying Ransoms

Podcast 1012's topic was "Hiding School Cyberattacks" and last week we took a look at the latest rising Ransomware-as-a-Service start, Ransomhub. One thing we didn't touch on at all during either of those discussions was the question of the legality of all these ransomware payments. An editorial about this appeared in a recent Risky Business Newsletter, which opened with a reminder regarding the legality of paying ransoms. The newsletter's editor wrote:

> *A recent CISA report, and a series of tweets from Equinix's threat intel analyst Will Thomas, clarified that quite a few infosec and adjacent cybersecurity experts are not fully aware that paying ransoms to a rising ransomware crew named RansomHub carries quite a high risk of breaking US sanctions.*
>
> *The group launched in February 2024, when it started advertising its Ransomware-as-a-Service offering in underground hacking forums. They got incredibly lucky because, just three weeks later, law enforcement agencies across the globe dismantled LockBit, which was, at the time, the largest RaaS platform on the market.*

What the editor meant about their luck was that RansomHub had established itself and it's presence in the sector just as the current number one RaaS provider, LockBit, was taken down. This left RaaS affiliates without a base of operations, but as luck would have it, the new kid on the block, RansomHub, just happened to be there to step in to fill LockBit's abandoned role. The editorial continues:

> *Throughout the year, many of LockBit's affiliates slowly found their way to RansomHub. By the end of the year, the platform rose to become 2024's most active ransomware operation, with its leak site listing more than 530 victims.*
>
> *A CISA report published last August warned of the group's rise in popularity and increased operations. But as Will Thomas noticed, RansomHub also appears to have attracted some unsavory affiliates, namely the members of a cybercrime cartel known as EvilCorp. EvilCorp appears to have begun using RansomHub as a final payload around July of last year, dropping the ransomware onto systems previously infected via the FakeUpdates (SocGholish) botnet—per reports from both Microsoft and Google.*
>
> *Between late 2017 and 2018, EvilCorp previously developed and ran its own ransomware strains, such as BitPaymer, WastedLocker, Doppelpaymer, Hades, and PhoenixLocker. The group abandoned its own tools after it was sanctioned in the US in December 2019, sanctions that forced companies to flat-out refuse to pay ransoms, fearing they'd break sanctions and face the wrath of US authorities.*
>
> *Since then, EvilCorp has been jumping between different RaaS platforms as part of a clever strategy of hiding their tracks and as a way to avoid scaring victims with possible sanctions violations. With a fresh new coat of both US and UK sanctions issued in October last year, the risk of breaking sanctions in the case of a RansomHub infection is higher than ever.*
>
> *But still! The TLDR here is that if you get hit by RansomHub, you better check with your legal team before even thinking of opening your wallet.*

We know that the rise of ransomware is entirely fueled by the prospect of ransom payments. The bad guys couldn't care less about any random enterprise's network insecurities nor their databases full of proprietary customer crap. They could not care less. The only thing they care

about is cash and the realization that vulnerable enterprises do care absolutely about their own crap-filled databases, and about them not being publicly exposed, created today's modern ransomware nightmare.

"X" blocks Signal.me links

I'm unsure why the security and privacy industries are all up in arms over last week's news that 'X' has started blocking its users from including links containing the "signal.me" domain. Signal.me links provide direct access to Signal users. To me, this seems very petty and typical of Elon's management of the platform he owns. On the other hand, he owns it now, and as we recall he didn't really want to buy it, he was forced to honor a previous purchase offer he had made. And he paid a lot of money for it. Well more than it was worth at the time. So in this country 'X' is his to do with as he chooses. Many people like and approve of the changes his stewardship has brought to 'X'. But it does seem to me that if these changes were supposed to be in support of unrestrained free speech, then blocking links to competing messaging platforms flies in the face of that.

The blocking covers public posts, private DM's and 'X' profiles. And the messages are never clear. You might see *"Sending Direct Message failed"* without further explanation. Attempting to post publicly may result in *"We can't complete this request because this link has been identified by X or our partners as being potentially harmful."* or you might see *"This request looks like it might be automated. To protect our users from spam and other malicious activity, we can't complete this action right now. Please try again later."* An attempt to add a "Signal.me" link to a profile bio resulted in an error message saying *"Account update failed. Description is considered malware."* X is also blocking users from clicking existing "Signal.me" links which were published prior to the domain's ban. Users who attempt to click on a "Signal.me" link already posted to X are met with a warning page from X that reads *"Warning: this link may be unsafe. The link you are trying to access has been identified by X or our partners as being potentially spammy or unsafe, in accordance with X's URL Policy."* However, in this case users are given the choice to ignore the warning and click an additional link on the warning page to follow the link as before.

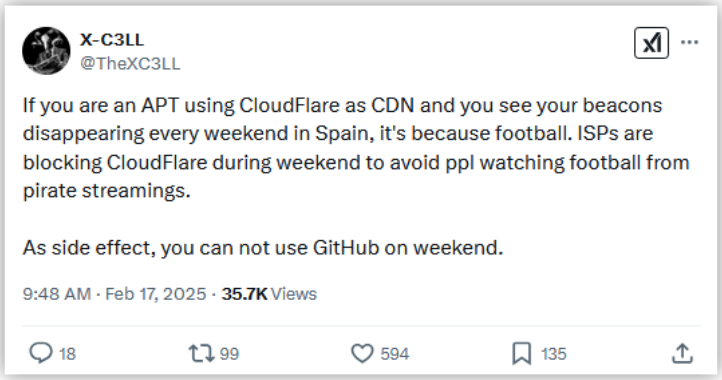
For me, the incredible inertia 'X' has is another interesting object lesson in the inertia we often observe throughout the tech sector and elsewhere. As we know, today there's been an explosion of alternative instant messaging platforms. There's Mastodon, Bluesky, Discord, Meta's Threads, WhatsApp and Instagram, Signal, Telegram and more. Unfortunately, what we have is a dispersion from the valuable single-platform concentration that Twitter originally provided. Having everyone on different platforms is far less useful to everyone – but that's the way things have evolved. This is why I decided to return to email for my own purposes. And that's why the show summary, these show notes and the picture of the week were delivered to 16,326 of our listeners yesterday, regardless of whether they remained on 'X', migrated elsewhere, or as was the often the case, were, like me, never actively participating in the social media movement.

Spanish Soccer blocks Cloudflare

I first encountered a short worrisome blurb, which read:

> *Cloudflare blocked in Spain on the weekends: Spanish internet service providers have started blocking access to some Cloudflare IP addresses on weekends. The blocks were put in place this month after Spain's soccer league won a lawsuit against* ***Cloudflare*** *for hosting pirate streaming sites. According to reports in local media, the blocks are indirectly blocking access to many legitimate websites, including GitHub, Reddit, and many private Spanish businesses.*

This news was accompanied by a Tweet:



Before I go any further let me remind everyone that the reason using a crude packet-level firewall to perform "IP-based blocking" no longer works, is SNI – Server Name Indication.

What SNI enables in practice is IP sharing at scale. For example, GRC has a handful of IPv4 IPs which I treasure. But I now have many more websites and services than I have IPs. I'm being saved by SNI, Server Name indication, which allows the incoming connecting client, as part of its TLS negotiation, to specify which remote server the client intends to access at that IP.

There might be hundreds or thousands of domain names all resolving to that single IP. So that means that access to hundreds or thousands of individual websites and services would be erroneously blocked if some court were to order the IP that's also shared by some copyright infringer be blocked. This is a mess.

Cloudflare headline read: "LaLiga Understood Dangers, Went Ahead Anyway" and Cloudflare wrote:

Cloudflare provides security and reliability services to millions of websites, helping to prevent cyberattacks and make the Internet safer. Like virtually all major cloud service providers, Cloudflare uses shared IP addresses to manage its network, meaning that thousands of domains can be accessed with a single IP address.

Cloudflare has repeatedly warned about the consequences of IP blocking that fundamentally ignores the way the Internet works. Indeed, other governments in Europe have acknowledged these concerns and concluded that IP blocking violates net neutrality. Although LaLiga clearly understood that blocking shared IP addresses would affect the rights of millions of consumers to access hundreds of thousands of websites that do not break the law, LaLiga went ahead with the blocking. This appears to reflect a mistaken belief that its commercial interests should take precedence over the rights of millions of consumers to access the open Internet.

At the same time, Cloudflare regularly speaks with rights holders and policy makers about better ways to combat illegal piracy and online abuse. While Cloudflare cannot remove content from the Internet that it does not host, we have well-developed abuse processes in place to help by connecting rights holders with service providers who can take effective action. We will continue to push for rational solutions to combat illegal piracy that do not impact the rights of millions of Europeans to browse the Internet.

Some reporting on this explained:

> *Cloudflare's statement needs no explanation, but two issues deserve highlighting:*
>
> *According to LaLiga's statement, its target behind Cloudflare was a webpage with instructions on how to download an Android app. If that app was the means of accessing the content, that raises an important question;*
>
> *When Cloudflare's IP address was blocked, did that 'deactivate' both the app and the pirated content available through it? If not, blocking many innocent websites appears to have been weighed against the benefit of blocking an instructional web page.*
>
> *Cloudflare's suggestion that this was done deliberately could make this a matter for the European Commission, at minimum.*
>
> *Perhaps even more remarkable is the unwillingness of the ISPs to do anything, despite having the power to do so. The complication, of course, is that Telefonica and Movistar have licenses to distribute LaLiga content, and very little incentive to step in.*
>
> *Ultimately, customers of Movistar have suffered the most as individuals. This means that a decision was made to block Cloudflare, in the knowledge that Movistar subscribers would face the most disruption, and then Movistar was instructed to carry out the blocking against its own customers.*
>
> *As the court envisioned, apparently.*

Again, just to be clear, it's the customers of these Spanish ISPs, that have taken to blocking websites by IP address, that are being impacted because these customers are behind their ISPs IP-based firewalls. After all of this, Spain's LaLiga soccer league replied:

> *Over the last few days, multiple websites across Spain have experienced disruptions, an issue linked to the blocking of a few IP addresses by internet service providers.*
>
> *These blocks were implemented following requests from LALIGA to combat illegal access to its content, which Cloudflare has facilitated by knowingly protecting criminal organisations for profit. Through this conduct, Cloudflare is actively enabling illegal activities such as human trafficking, prostitution, pornography, counterfeiting, fraud, and scams, among other things.*
>
> *In fact, LALIGA identified two IP addresses covered by Cloudflare, which provided access to child pornography. This evidence has been fully documented and submitted as part of a formal police report.*

Remember, what LaLiga is objecting to is a web page that provides instructions for downloading an Android app which, in turn, allows streaming of live soccer matches. And Cloudflare made clear that it has mechanisms in place for dealing with illegal content.

LaLiga's statement says: *"Cloudflare is actively enabling illegal activities such as human trafficking, prostitution, pornography, counterfeiting, fraud, and scams, among other things."* But it would be more accurate to say *"The Internet is actively enabling illegal activities such as human trafficking, prostitution, pornography, counterfeiting, fraud, and scams, among other things."* – because, yes, *"The Internet"* as a whole **does** passively enable these things, right alongside all of the positive things it also enables. And this is, of course, the Net Neutrality issue at the heart of Cloudflare's argument. They are functioning as part of the Internet's content conduit and they are determined to remain as neutral as possible.

LaLiga's statement continued:

> *This action specifically targets IP addresses used to illegally access LALIGA content, which were shielded by Cloudflare. Just like other major US tech corporations, Cloudflare enables criminal organisations to digitally launder stolen illegal content, making them a complicit party in intellectual property crimes as defined in Article 270.2 of the Spanish Penal Code.*

Wow. You know, there's a really simple solution to this. LaLiga could simply decide not to stream their soccer matches to the Internet at all. Just like in the old days. Have fans attend their games. Then there's no problem. But, no. They, of course, want all the benefits of this magical technology without any of the technologically-enabled downside. They continued:

> *It's important to emphasise that this is not a broad or indiscriminate block.*

Right. All evidence to the contrary, and despite the need to issue this explanation in the first place. They said:

> *LALIGA is absolutely certain and has proof that these IPs are being used to distribute illegal content alongside legitimate material. Legal businesses affected by these blocks are those that Cloudflare has deliberately used as a digital shield to obscure illegal activity, without their knowledge and while profiting from it.*

Wow.

> *More than 50% of pirate IPs illegally distributing LALIGA content are protected by Cloudflare. Despite multiple formal requests from LALIGA for Cloudflare to cease its collaboration with pirate sites, the company has refused to cooperate, instead continuing to profit from the criminal activity it helps to conceal.*
>
> *LALIGA has repeatedly reached out to Cloudflare, requesting voluntary cooperation. However, on Friday, February 7, the US tech company responded in a surprising manner, defending its actions with implausible and incoherent technical excuses. This left LALIGA with no other option but to take direct action. This issue is not unique to Spain; similar measures have been taken in other countries to combat piracy of sports content. LALIGA fulfilled its due diligence obligations before resorting to this step.*
>
> ***Google, Cloudflare, VPN providers, and other entities** facilitating piracy are responsible for the illegal activities they enable and profit from. LALIGA, backed by the justice system, will not relent in its efforts to protect football and the interests of its clubs against criminal action related to audiovisual fraud and digital laundering."*

"Don't shoot the messenger" is a long understood principle. To call out Google, Cloudflare, VPN providers and other entities is to say "The Internet". LaLiga wants to have all of the benefits that derive from having the Internet – which they did not create – carrying their content for effectively no cost, while also wishing to somehow prevent that no-cost carriage from being used in ways they disapprove of.

It's understandable that when served with an IP-blocking court order, those ISPs within the Court's reach had no choice other than to block access to that IP. And given LaLiga's feelings, it's also understandable that they would have made such an appeal to the court. What's missing from the equation is the legal precedent that would prevent the court from producing the ruling they did. As Cloudflare said in their statement:

> *Cloudflare has repeatedly warned about the consequences of IP blocking that fundamentally ignores the way the Internet works. Indeed, other governments in Europe have acknowledged these concerns and concluded that IP blocking violates net neutrality.*

So, hopefully, this issue will escalate to have this lower court ruling overturned by a higher Spanish court so that precedent will be created in Spain, LaLiga's and all others' current and future appeals will be thwarted, and the principles of Net Neutrality, which is clearly the only way a sane Internet can function and thrive, will prevail in the end.

We can chalk this down to "growing pains."

Two vulnerabilities discovered in OpenSSH

Through the years we've noted that vulnerabilities discovered in OpenSSH are vanishingly rare. This project is widely regarded as one of the most secure of any open source project. And this is, of course, crucial, since OpenSSH's role is to be positioned on the front line, exposing itself to the Internet while warding off all attackers. So when Qualys announces the discovery of two new and potentially weaponizable vulnerabilities in this crucially important remote access technology, everyone pays attention. Last Wednesday, Qualys disclosed:

> *The Qualys Threat Research Unit (TRU) has identified two vulnerabilities in OpenSSH. The first, tracked as CVE-2025-26465, allows an active machine-in-the-middle attack on the OpenSSH client when the **VerifyHostKeyDNS** option is enabled. The second, CVE-2025-26466, affects both the OpenSSH client and server, enabling a pre-authentication denial-of-service attack.*
>
> *The first attack, '26465, succeeds regardless of whether the VerifyHostKeyDNS option is set to "yes" or "ask" – its default is "no". This attack requires no user interaction, and does not depend on the existence of an SSHFP resource record (an SSH fingerprint) in DNS. VerifyHostKeyDNS is an OpenSSH **client** configuration option that lets the SSH **client** look up and verify a server's host key using DNS records (specifically, SSHFP records). The vulnerability was introduced in December 2014, just before the release of OpenSSH 6.8p1. Although VerifyHostKeyDNS is disabled by default, it was enabled by default on FreeBSD from September 2013 until March 2023.*

Although I don't use the OpenSSH client on my own FreeBSD instances, when I saw that date range I checked and, sure enough, FreeBSD's default OpenSSH client is, indeed, configured with VerifyHostKeyDNS enabled and set to "yes" by default. In the second vulnerability:

Both the OpenSSH client and server are vulnerable (CVE-2025-26466) to a pre-authentication denial-of-service attack, in the form of an asymmetric resource consumption of both memory and CPU, that was introduced in August 2023 (shortly before the release of OpenSSH 9.5p1).

On the server side, this attack can be mitigated by leveraging existing mechanisms in OpenSSH, such as LoginGraceTime, MaxStartups, and the more recent PerSourcePenalties.

Recommended Action: OpenSSH 9.9p2 addresses these vulnerabilities mentioned above. To ensure continued security, we strongly advise upgrading affected systems to 9.9p2 as soon as possible.

And Qualys underscored OpenSSH's terrific security, writing:

Despite these two vulnerabilities, OpenSSH's overall track record in maintaining confidentiality and integrity has made it a benchmark in software security, ensuring secure communications for organizations worldwide.

So what do these two vulnerabilities mean? Qualys writes:

In the first instance, if an attacker can perform a man-in-the-middle attack via '26465, the client may accept the attacker's key instead of the legitimate server's key. This would break the integrity of the SSH connection, enabling potential interception or tampering with the session before the user even realizes it. SSH sessions can be a prime target for attackers aiming to intercept credentials or hijack sessions. If compromised, hackers could view or manipulate sensitive data, move across multiple critical servers laterally, and exfiltrate valuable information such as database credentials. Such breaches can lead to reputational damage, violate compliance mandates (e.g., GDPR, HIPAA, PCI-DSS), and potentially disrupt critical operations by forcing system downtime to contain the threat.

In the second case, SSH is a critical service for remote system administration. If attackers can repeatedly exploit flaw '26466, being a denial of service, they may cause prolonged outages or prevent administrators from managing servers, effectively locking legitimate users out. An enterprise facing this vulnerability could see critical servers become unreachable, interrupting routine operations and stalling essential maintenance tasks.

When the Qualys research team confirmed the vulnerability, Qualys initiated a responsible disclosure process and worked with OpenSSH to coordinate its announcement.

So the bottom line is that anyone who's worried about this and who uses the OpenSSH client may wish to make sure that their client's config file has *VerifyHostKeyDNS* set to *"no"*. And anyone who relies upon OpenSSH should look for and install updates which are now available.

Finally, I need to mention that Qualys provided a truly beautiful write-up of the details of this bug. They show some small snippets of OpenSSH code and describe how they went about discovering the problem which became a vulnerability after they were able to engineer its exploitation. Anyone who considers themselves a bit of a codesmith would be well served looking at their excellent page: https://www.qualys.com/2025/02/18/openssh-mitm-dos.txt I have a link to it at the bottom of page 8 of this week's show notes. Very highly recommended!

What?! The U.S. cannot EVER FULLY evict Chinese attackers from its Telecom systems?
Some sobering news was made during last week's Munich Security Conference. As reported by Politico:

> *The State of Virginia's Senator Mark Warner is working to build support on the Hill for major changes to America's **offensive** cyber policy, amid the government's continuing failure to fully evict China's Salt Typhoon hackers from U.S. phone networks.*
>
> *Speaking to reporters on the sidelines of the Munich Security Conference last weekend, Warner said he now does not believe the U.S. can **ever** fully oust the elite, Beijing-backed hacking group—Salt Typhoon—from its telecommunications backbone without unleashing U.S. hackers inside China — or at least, credibly threatening to.*
>
> *Mark Warner said: "Your diplomatic pushback on the Chinese would be a hell of a lot stronger if the U.S. could tell China, 'We're going to go into your networks the exact same way you go into ours.'"*
>
> *Warner is the first Democrat to come out so clearly in support of punching back harder in cyberspace against China in the aftermath of the Salt Typhoon breaches, with congressional Republicans and members of Trump's new administration having already signaled their support for that shift.*
>
> *Warner said that replacing aging and vulnerable networking equipment could cost the telecom companies tens of billions, while evicting the Chinese from every nook and cranny inside the nation's sprawling phone system could take <quote> "50,000 people and a complete shutdown of the network for 12 hours."*
>
> *Warner said that he has been in talks with the heads of the congressional intelligence committees and that "consensus was already there" for a new, more hawkish hacking strategy.*
>
> *The next step, he said, was "putting meat on the bones" of that idea — something that might require the formation of a bipartisan expert commission, he said. He also emphasized that he believed working through the Hill and building support among Democrats was critical to a more robust cyber deterrence strategy. Warner argued that <quote> "If it comes from Trump, you know, any Democrats will just say, 'He's just going over the top.'"*
>
> *Warner did say he felt part of the long-term solution was the promulgation of new cybersecurity regulations for the telecom sector. That's something the Biden administration and several congressional Democrats have supported, but the Trump administration has at least for now pooh-poohed.*
>
> *Overall, Warner said he was **apoplectic** that so few people seem to be paying attention to Salt Typhoon. He said: "The fact that people's heads are not exploding still makes me crazy."*

As we've often noted, we must assume that the NSA has just as much penetration into Chinese networks as they have into American networks.

It strikes me as a sad state of affairs that our political leaders are now suggesting that we're incapable of securing our own networks, and that the only way to "get them out of ours" is to credibly threaten to do more damage to them through theirs.

Speaking of Salt Typhoon
And speaking of Salt Typhoon, this group has been on the radar of several cybersecurity threat tracking groups for some time. The commonly known "Salt Typhoon" name is the one it received from Microsoft's Threat Intelligence. But the same group is also known as RedMike by Insikt which is the Recorded Future Network Intelligence's Group. Meanwhile, Kaspersky calls them "GhostEmperor" and ESET tracks them as FamousSparrow.

Although Microsoft has not chosen to share their findings within the broader security community, several others have. The news from Recorded Future's network intelligence group is somewhat dispiriting, because it turns out that RedMike, as Recorded Future calls them, is exploiting two very well known, long since patched, two year old vulnerabilities in Cisco's IOS XE Web UI. Yes, you heard that right. In infamous Salt Typhoon has been gaining entry into the world's Telecom carriers using an exposed Web management user interface. <<sigh>> And not only that, they are a pair of privilege escalation vulnerabilities: CVE-2023-20198 and CVE-2023-20273. That's right, 2023.

The '20198 privilege escalation vulnerability was found in version 16 and earlier of Cisco's IOS XE web UI and the patch for it was published by Cisco in October 2023. Attackers exploit this vulnerability to gain initial access to the device and issue a Cisco IOS "privilege 15" command to create a local user and password. Following this, the attacker uses the new local account to access the device. They then exploit the associated '20273 privilege escalation vulnerability to gain root user privileges. And once that's done, the group uses this new privileged user account to change the device's configuration and add a GRE tunnel – which is similar to an encrypted VPN link – to give them persistent access and data exfiltration.

And all of this pain because those Telecom carriers have never bothered to update their Cisco gear to close an 18 month old vulnerability, not to mention leaving a web management UI exposed to the Internet.

#2 cryptocurrency exchange loses $1.5 BILLION to North Korea
For a while, I'm sure we were all somewhat intrigued by the news of this or that never-heard-of-em-before Cryptocurrency exchange being hacked and losing millions of dollars worth of never-heard-of-it-before cryptocurrency, or contracts, or monkey cartoons, or whatever. But as also eventually happened with the constant torrent of ransomware attacks, over time they were tuned out as just so much background noise for the sake of our sanity.

But not this one. Not this time. Under the headline, *"Boy, that's gotta hurt!"* is the news that the world's second largest major cryptocurrency exchange was, as they say, taken to the cleaners by a group of quite determined North Korean hackers to the tune of – are you sitting down? – $1.5 BILLION dollars worth of completely liquid Ethereum tokens. This makes it the largest crypto-heist ever in history (and the largest heist of any kind for that matter) and is nearly 2.5 times larger than the previous record, which was the theft of $625 million from the Ronin Network back in April of 2022.

I have a link in the show notes showing the fraudulent transaction event on the Ethereum blockchain where 401,346.769 ETH are being transferred. Ethereum peaked at around $4,000 each in early December last year, and it's currently trading at around $2,800 USD.

https://etherscan.io/tx/0xb61413c495fdad6114a7aa863a00b2e3c28945979a10885b12b30316ea9f072c

So the hack took place last Friday, February 21st, and in addition to being the largest single crypto-heist ever, it's also considered to be one of the most complex crypto-heists ever pulled. The blockchain analytics firms Arkham Intelligence and Elliptic have independently claimed that they were able to trace the hack to the Lazarus Group, a well-known North Korean advanced persistent threat (APT) group.

What we know is that Lazarus first infiltrated Bybit's network some time ago. They then quietly studied the company's internal procedures, identified, and then infected with malware all of the multiple employees who are required to mutually sign off on any major movement of the company's funds. This multi-sign-off requirement is obviously designed to solve the problem of any single employee being hacked or phished or scammed or whatever. But that didn't thwart the attack this time.

The hackers specifically targeted the process of replenishing the company's active wallets — known as hot wallets — where the company's daily operational funds are stored. When hot wallets run dry, crypto exchanges move funds from their reserves — the so-called cold wallets — to make sure there's enough liquidity to cover user withdrawals and token inter-exchanges.

The same goes for when hot wallets hold too much money. In those instances, crypto exchanges will move funds back to the offline cold reserves to safeguard themselves from malicious actors and exploits and limit possible losses. That all makes sense.

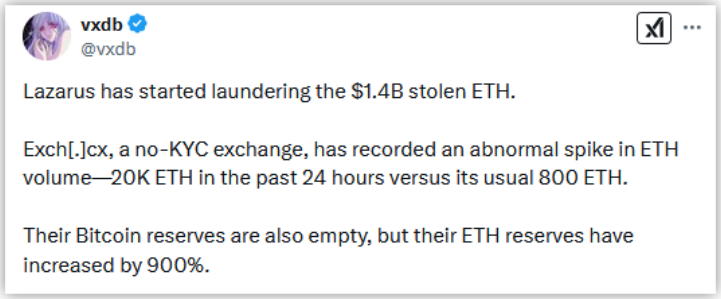
Bybit's CEO Ben Zhou *(cho)* says that when his staff wanted to replenish the hot wallets with new funds on Friday, the hackers altered the user interface of the crypto-wallet software the company was using to move funds. The modification appeared on the systems of every one of the multiple engineers who needed to simultaneously sign off, in what is known as a multi-sig transaction. A tweet describing what happened reads:

Not surprisingly, Bybit's loss of that $1.5 billion in Ethereal Tokens did not go unnoticed and since this makes many investors nervous about other potential weaknesses in Bybit's security, the company said that news of the hack had led to a surge in withdrawal requests. CEO Zhou *(cho)* wrote that the company had received more than 350,000 requests from customers to withdraw their funds and that this surge of departing money could lead to delays in processing.

In response, Bybit set up a bounty program for the recovery of the stolen funds offering to pay anyone who is able to recover the funds, 10% of anything they're able to recover. This has, in turn, set off the biggest bounty hunt on the internet, with the winners being eligible to earn up to a whopping $150 million.

At the same time, not surprisingly, the perpetrators, who were ready to deal with this massive windfall quickly began laundering their funds in the hopes of hiding their tracks and diffusing the proceeds of their theft among the world's cryptocurrency. They're moving quickly because if they leave the funds in their normal wallets, they risk having them hacked back by multiple parties including law enforcement, bounty hunters, or other threat actors.

Another Tweet observed:



As we know, since blockchain activity can be monitored and tracked, what we have now is a bit of a shell game.

So what's our takeaway from all of this? If we're wise, every event teaches a lesson that prevents its recurrence. And hopefully, others are also able to learn and gain from seeing what has befallen others and take away the same lessons without needing to first fall off the same cliff. In this case, I think the lesson here is that the systems which manage these massive cryptocurrency reserves need to be far more isolated from everyday systems than they currently are.

In other words, they need to be fully **air-gapped** ... with nothing less being sufficient.

These are lessons that the professional intelligence community and those practicing the tightest security in the world learned decades ago. And nothing we've done since with our computer and networking technology has served to make full air-gapping any less necessary. We could easily argue that, in fact, the reverse is true and that air-gapping systems that absolutely and positively must ***never*** be compromised has grown **more** necessary today than ever before.

I would bet that Bybit has just learned this lesson. They obviously felt that requiring a multi-person multi-keyed funds transfer authorization process would be sufficient. It's certainly better than requiring just one person. They just learned a $1.5 billion dollar lesson, that it isn't enough.

The U.S. is falling behind its enemies in cyberspace

We have North Korean-backed hackers stealing around $1.5 billion dollars of cryptocurrency while a former head of the NSA and ex-CyberCommand chief says, in a wide-ranging speech and interview this past Saturday, that the U.S. is falling behind its enemies in cyberspace. Wonderful.

Speaking at the DistrictCon cybersecurity conference in Washington, D.C., retired General Paul Nakasone (naka-sony) said that *"our adversaries are continuing to be able to broaden the spectrum of what they're able to do to us."* and that the United States is falling *"increasingly behind"* its adversaries in cyberspace. Unfortunately, he would be in the position to know. Here's what CyberScoop wrote in their coverage of the event:

Nakasone said incidents like Chinese government-backed breaches of U.S. telecommunications companies and other critical infrastructure — as well as a steady drumbeat of ransomware attacks against U.S. targets — illustrate "the fact that we're unable to secure our networks, the fact that we're unable to leverage the software that's being provided today, the fact that we have adversaries that continue to maintain this capability."

Nakasone, who led NSA and CYBERCOM from 2018 until early last year and is now founding director of Vanderbilt University's Institute of National Security, said he fears the threats of the future are only going to get more dangerous. One example is "we are starting to see the beginnings of the bleed from the non-kinetic to the kinetic for cyber operations," he said, referring to actual physical damage.

Nakasone said, "What's next is that we are going to see cyberattacks against a series of platforms being able to actually down platforms with ones and zeros." A board member for OpenAI, Nakasone also talked about how artificial intelligence could make cyber offense more potent. Specifically, he mentioned the notion of generative targeting, such as the idea of physical drones choosing their targets powered by AI.

Oh, lord. He should read some Daniel Suarez to see how he thinks about the wisdom of autonomous AI-powered drones. CyberScoop continues ...

"We're starting to challenge this idea of humans in the loop, and I also offer to you as we think about artificial intelligence models, think about cyber weaponry," he said. "How far are we talking to this idea of being able to create an agent that's going to move through your network, that's going to change based upon topology in the network, being able to evade the defenses that are there, choosing targets of the future?"

Members of the Trump administration, and some members from both parties in Congress, have called for the United States to get more aggressive with offensive operations in cyberspace. In a separate conversation with reporters, Nakasone said he agreed with those sentiments. Nakasone's Cyber Command conducted operations dating back to at least 2018 to disrupt Iranian and Russian hackers in conjunction with more defensive "hunt forward" missions in other nations designed to fortify allies' defenses and detect future threats against the United States. He also advocated for a philosophy of "persistent engagement" — to be in constant contact with cyber enemies, proactively rather than reactively.

Nakasone said of offensive operations: "We need to do more of that, certainly. It's not just the only thing we need." He said that one of the points of persistent engagement was to ensure anyone who attacked U.S. election infrastructure knew they would suffer consequences from the United States. "Can we be more forthcoming in terms of some of the things we did? Yeah, I think there is opportunity."

Okay, now that's interesting. That suggests that we did something in response to foreign interference with our national elections but that whatever it was was kept on the down-low.

In his speech, Nakasone said the top priority for the United States should be hiring top talent. Under President Donald Trump, the government has been removing some of those who were in the cyber talent pipeline. Eventually, Nakasone said, "we're going to have to be able to engage folks again and say, 'Hey, please come and work in government.'" It's an open question how long any damage to the trust of potential hires will last, he said.

Another change under Trump is that Defense Secretary Pete Hegseth has reportedly sped up the implementation of a Cyber Command overhaul, from 180 days to 45 days.

In response to a question from CyberScoop, Nakasone said: "How doable is it? It's really doable when you get that direction from the secretary." Asked if he was worried about whether the tightened timeline would lead to that implementation suffering, Nakasone answered only that the concepts of Cyber Command 2.0 have been in the works for a while already.

That's true, and I'll just add that the Cyber Command 2.0 initiative was started toward the end of President Biden's administration. And finally ...

During a question-and-answer session with the DistrictCon audience, Nakasone did not voice any criticisms of Trump's purge of top military officials, such as Gen. Charles "CQ" Q. Brown, chairman of the Joint Chiefs of Staff. While praising Brown's work, Nakasone said: "At the end of the day, the president gets to choose his own principal military adviser"

Soooooooo... yikes. We're apparently not giving as well as we're getting. The NSA is as annoyed as we all are over our inability to secure our own networks, and the future planners are seriously considering AI powered attack drones without any of those pesky slow humans in the loop, having second thoughts and gumming up the works. It's just too easy to pose our favorite rhetorical question: ***"WHAT could POSSIBLY go wrong?!?"***

DNS Benchmark

I wanted to announce the achievement of another milestone for the DNS Benchmark. Friday evening I dropped the 5th pre-release of the DNS Benchmark. To be clear, these are not betas or even alphas. They are incremental works-in-progress. For example, the first of the pre-releases was the day after Christmas, where the Benchmark was first able to query and benchmark remote DNS nameservers over IPv6. Last Friday evening's 5th pre-release published its new ability to also query nameservers using DNS over HTTPS and DNS over TLS. All of that is now working. As always, and the reason this wide-spectrum testing is so valuable, even though everything appeared to be working perfectly for me, the result of that 5th release has been the discovery of a handful of bugs. So I could not be happier. The Benchmark is coming along nicely, and I have a terrific proving ground of pre-release testers who will help me assure that the Benchmark's final release will be as completely bug-free as version 1 of the Benchmark was 16 years ago.

Listener Feedback

The great "backdoor" replacement

Last week's call for a replacement for the term "backdoor" produced the expected massive wave of replies. So first, ***thank you everyone***. We now have 16,350 subscribers to the weekly podcast emails, so I'm receiving all the feedback I could ever ask for. Among the suggestions for "backdoor" replacement were many fun ideas. But the one that I saw multiple times, and the one that feels best, is simply "**Master Key**" — the idea that Apple, or any similar provider, would arrange their technology to have a "Master Key" that, implicitly, only they would know. I think that term offers precisely the concept I was looking for, since while the key itself is a secret, the designed-in existence of such a key, and capability, is not.

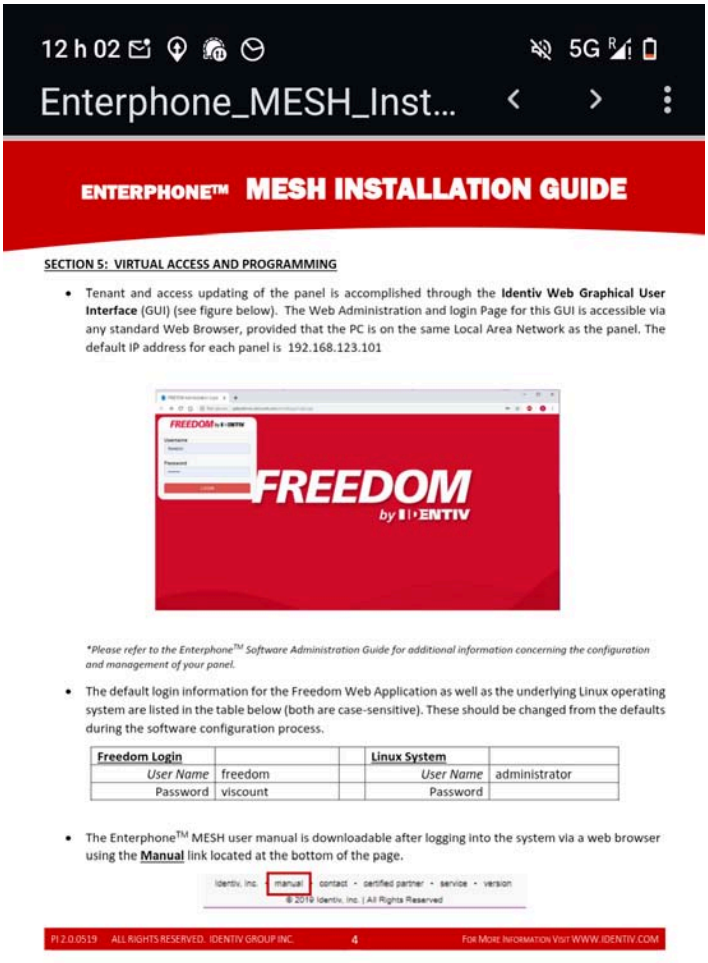
FREEDOM Administration Login

Today's main story just makes you shake your head, but the underlying lesson is too important to ignore. Even so, if it weren't already so public I would not be shining any brighter light on it. You'll see why. But I guess I'm glad others have, even if I would have probably passed. The first sign of something having gone very wrong was the following short news blurb, which read:

> ***Default password in Hirsch building entry systems:*** *Hirsch Enterphone building entry systems contain a hardcoded username and password for their web admin panel that can allow threat actors to unlock doors via the internet. The default creds are for an admin account named* ***freedom*** *that uses the password* ***viscount****. According to security researcher Eric Daigle, there are more than* ***700 Hirsch Enterphone*** *systems available over the internet, with most used by apartment blocks across the US and Canada. Hirsch says customers did not follow their instructions to change the default passwords. However, the misconfiguration's discoverer, Eric Daigle says customers are never prompted to change the password during the setup process. Tracked as CVE-2025-26793, the vulnerability has a 10 out of 10 severity score and is very likely to be exploited.*

Which is likely the understatement of the year so far.

Eric gave his blog posting the title *"Breaking into dozens of apartment buildings in five minutes on my phone"* and the sub-head: *"What a place to use default credentials"* In his posting Eric shared his entire process of discovery which is so fun that it bears sharing here. He explained:



> *A few months ago I was on my way to catch the SeaBus when I walked by an apartment building with an interesting looking access control panel. I wrote down the "MESH by Viscount" brand name and made a note to look into it when I had a chance. I ended up just missing my ferry (the 30 minute Sunday headways are brutal), so I decided to see if I could find anything promising on my phone while waiting at Waterfront for the next boat.*
>
> *Googling the name of the system brings up a sales page advertising "TCP/IP capability to remotely program and maintain the system." That sounds promising, so let's try to find a manual. "mesh by viscount" filetype:pdf gets us an installation guide. Page 4 explains how to log in to the system's web UI.*

Eric attached the snapshot he took of his Android mobile phone, from which we learn, among other things, that his location has good 5G coverage, but that he's also in rather desperate need of rechanging his phone's dying battery.

On that page we see the statement: *"The default login information for the Freedom Web Application, as well as the underlying Linux operating system are listed in the table below, both are case-sensitive."* (Be sure to point that out to the attackers). *"These should be changed from the default during the software configuration process. And below that is a table showing that the Freedom Login has the Username "freedom" and the Password of "viscount"*. And that the underlying Linux system has the Username "administrator" and a blank password.

Eric's blog posting notes:

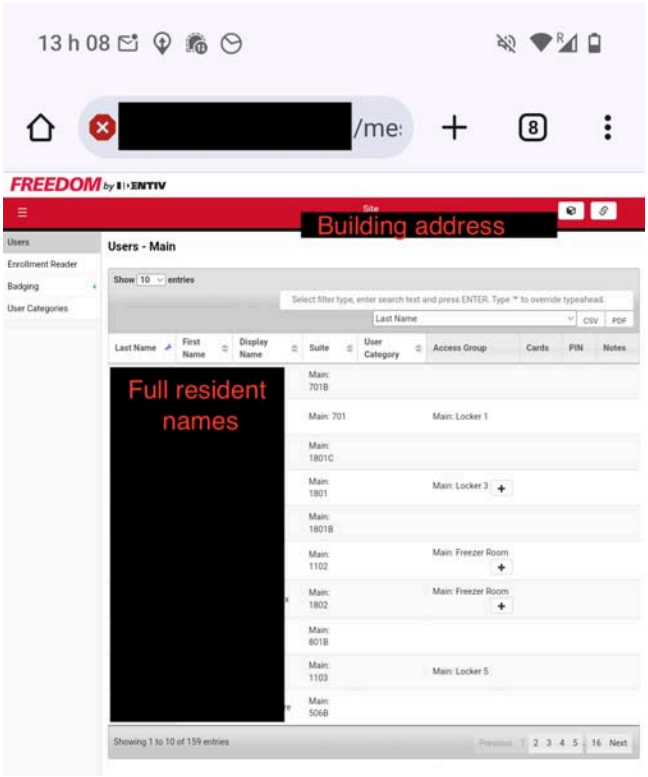
> *Default credentials that "should" be changed, with no requirement or explanation of how to do so. Surely no building managers ever leave the defaults, right? And even if they did, they'd surely have no reason to expose this thing to the Internet, right? The screenshot from the manual tells us the web UI login page's title is "**FREEDOM Administration Login**", which gives us something to search for.*

Okay. In other words, this web portal's login page has the title "FREEDOM Administration Login", which means that Google will have discovered and happily indexed all of them, sitting there wide open on the Internet. I was hoping that it might have used some non-standard port. Stilly me.

And everyone can do this, right now, from home or from your own mobile phone just like Eric did while he was waiting for the ferry and desperately hoping that his phone's battery would last. Just search the internet for the phrase: "FREEDOM Administration Login" and you'll be rewarded with countless hits. I clicked on one. The web server is using port 80, not 443, so it's HTTP and not HTTPS (which makes sense for a cheesy application like this.) So when I told Firefox that, yes, I wanted to go to this old school HTTP site: http://98.174.254.140/mesh/jsp/login.jsp ... and sure enough, I was greeted with a big beautiful login page for Viscount Systems FREEDOM:

And there in the upper-left corner was the prompt for the system's administrative login Username and Password. Naturally, that's as far as I took it. But Eric went in. Here's what he shared. Under "Part 1 – Personally Identifiable Information galore" he wrote:

Exposing the panel to the Internet is dumb, but fortunately none of these systems were accessible using the default — just kidding — of course they were. The very first result happily lets me in with the freedom:viscount login. The first interesting thing here is the Users section:



Eric shares another screen shot, from which we learn that he's now on WiFi and his phone's battery is much happier. The screen shot he shares has blanked out the site's URL, the building's physical address and the full building resident's names. But they're all there in their full glory – alongside each resident's unit numbers so anyone can see exactly who lives where. Eric notes:

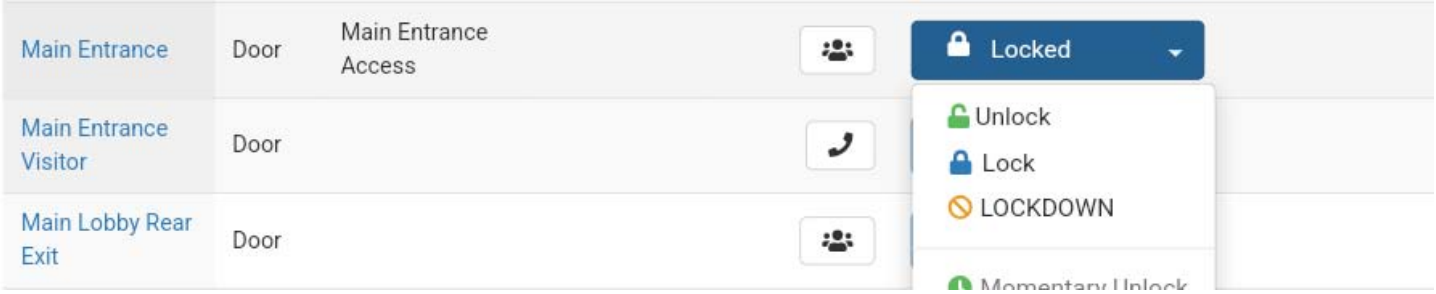
This maps residents' full names to their unit numbers. The building address is also used as the Site title. That's already not great, but it's worse in conjunction with the ***Events*** *section.*

This is a multi-year log of every time a fob associated with a certain suite number accessed an entrance or an elevator. So we can now easily determine that, say, Jon Snow of Unit 999, 123 Bear St Vancouver BC comes home every day at 6pm.

For good measure, there's also a Users section which exposes every resident's phone number.

Then we get to "Part 2: Breaking in", where Eric writes:

The Personally Identifiable Information (PII) leaks are pretty wild, but the most interesting thing we have access to is the ***Controlled Areas*** *section. In here I can apparently register new access fobs, disable existing ones, and change the floors they're authorized for. The system for this is somewhat convoluted. Fortunately I don't need to understand it at all, because I can just unlock any entrance I want through an override function:*



So, an attacker has the ability to unlock any of the doors controlled by this otherwise rather high-end building access control system. And Eric notes:

> *So I can break into this building in about 5 minutes without attracting any attention whatsoever. Neat.*

And then we get to Eric's Part 3: How widespread is this? Eric writes:

> *Maybe I just got lucky that the default credentials worked on the first result and this is actually really rare. Let's get back to a desktop and scan more properly...*

Which he then does. He uses some semi-automated scripting to attempt logging into the 742 exposed instances that his quick search turned up. It might be that using a more robust scanner would find many more. But of those 742, Eric's script was able to successfully login to the building's access control system of 43% of them, leaving them completely vulnerable and unprotected while also disclosing information about the building's residents that many would find quite objectionable.

So why is Eric sharing all this, despite the fact that this is significant and far from being merely a theoretical vulnerability? Presumably because he first tried to do the right thing but the vendor who indirectly created this mess in the first place could not be bothered to address it.

Here's Eric's responsible disclosure timeline:

- 2024-12-20: Vulnerability discovered.
- 2024-12-27: Current vendor of MESH identified as Hirsch (subsidiary of Vitaprotech Group) and contacted.
- 2025-01-09: CEO of Identiv, former vendor of MESH, contacted.
- 2025-01-11: Hirsch product security responds requesting details and are asked if they intend to alert clients.
- 2025-01-29: Hirsch replies stating that these vulnerable systems are not following manufacturers' recommendations to change the default password.
- 2025-01-30: Hirsch asked for an update as to whether clients running vulnerable systems have been alerted (no response as of publication).
- 2025-02-14: CVE-2025-26793 assigned.
- 2025-02-15: Publication.

Anyone who's been listening to this podcast for long will be well aware that there are several fundamental design flaws present here. First and foremost, as Eric briefly noted, there's almost certainly no need for an apartment building's access control system to be exposed to the public Internet. So while the Linux-based web server on the network would need to have its web server bound to the internal LAN interface to allow for administrative access by management on the LAN, it should never be bound to the WAN interface.

The second thing that's wrong with this picture is the entire concept of built-in factory-supplied usernames and passwords. Those days **MUST** come to an end, and that should have happened long ago.

The lesson the industry has learned the hard way, over a span of decades of trying very hard not to learn it, is that usernames and passwords is a place where security **MUST** trump convenience and the associated annoyance of *"I cannot login to my management portal"* tech support calls. Deal with it. There must be **no** default username and password, and also **no** form of manufacturer hidden backdoor username and password. As we know, any of those will be discovered the first time anyone goes looking. The system simply needs to generate a long unique username and password the first time it is started. When it discovers they are blank, it needs to use whatever entropy it's been able to gather from the universe up to that point – which is trivial for any connected device given unpredictable network packet timings – to initialize the username and password with pseudo-random gibberish. This cannot be left to chance or to someone reading *"please change the username and password from their initial default"* and then presumably thinking "yeah, I'll need to get back to that once everything has settled down. The system must enforce their being changed just once.

Given that the username and password will initially be gibberish, an administrator should be free to change them immediately if they wish, or the gibberish can be written down. Or the user's password manager can be used to record it. Or the browser's automatic built-in offer to remember for its user can be accepted. Today's ubiquitous tools mean that gibberish is no longer the daunting problem that it once was.

We've learned that doing what these clowns have done, of shipping their system with a publicly documented and thus publicly known username and password, while also allowing that system to be accessed from the Internet, is asking for exactly the sort of trouble that will now be visited upon all of this system's owners.

And finally, adding insult to injury, the damn things all have the same webportal page title, meaning that a simple Google search brings up hundreds and hundreds of potential victims, with, as Eric's login testing script discovered, a 43% chance of those publicly-known usernames and passwords allowing any casual passer-by to see who lives there, where exactly they live, to view detailed historical logs of their comings and goings, and unlock any of the doors that are controlled by the system's so-called security.

Lord only knows how many other similarly insecure systems exist in the world today. There's no way the owners of these systems, who are obviously not IT trained and focused administrators, will ever be made aware of this trouble, until they begin suffering from mysteriously unlocked doors and mysterious thefts that cannot be explained because there's no sign of break in. At that point, who's ultimately responsible for the damage that results?

The saddest thing is that all this is so avoidable with better system design. It would be tempting to conclude that the coders who are designing and implementing such security systems have no security training. But who knows? Perhaps the coders did have security training, but when they presented a secure system with a strong password policy built-in and no public access, they were overridden by management demanding an easier-to-use system that would not burden them with tech support calls and would allow them to have remote access for easier support?

That worrisome Log4J vulnerability that was discovered back in December of 2021, which kicked off our 2022 podcast year, turned out to be more worry than reality – for exactly one reason: It was difficult to do. Its fruit wasn't low-hanging, it was up at the top of a very tall tree, well out of reach for all but the most determined and capable hackers. We've learned that not all would-be hackers are rocket scientists. There is, indeed, an upper crust of elite hackers who can hack anything, but their numbers are blessedly few. The great mass of hackers are those who need to follow a hacking script.

My point here is that this "FREEDOM Administration Login" catastrophe doesn't even require a script. This is not low-hanging fruit. The fruit has fallen from the tree and is lying on the ground waiting to be picked up or kicked around. A governing rule of computer abuse is *"The easier it is to abuse, the more often and likely it is to happen."* I came to full attention when I encountered this story this week, because it's been a long time since we've encountered anything that's been begging this loudly to be abused. And there's no doubt that it will be ... especially when you add in the fact that the physical street address of the building being managed by these systems is loudly presented at the top of every logged-in page. There's no need to guess which buildings may as well have left all of their doors permanently unlocked and the schedules of their tenants posted publicly.

Given that it's trivial to login to these portals to determine their physical address, and that the majority of these facilities appear to be located in Canada – so said Eric – a good Samaritan among us might take it upon themselves to login, determine the building's address, and notify the building's management of this glaring security trouble. If anyone listening to this podcast wishes to do so, despite having the best of intentions, I would advise taking some anonymizing precautions, since we've seen instances where white-hat hackers are still being accused of wrongdoing.

It would make for a nice security project for anyone interested in doing some good, and it's somewhat astonishing that the publishers of this atrociously insecure access control system replied to Eric that *"vulnerable systems are not following manufacturers' recommendations to change the default password"* rather than taking any proactive measures to cure these and any future "recommendation failures." For anyone who might be interested in pursuing this, I've included the link to Eric's blog posting on the last page of this week's show notes:

https://www.ericdaigle.ca/posts/breaking-into-dozens-of-apartments-in-five-minutes/

I haven't mentioned that ***even if*** these systems' default username and password are changed, we're still looking at the always questionable security presented by exposed Internet-facing web UI portals. We know how challenging their security can be. So who's to say that there isn't some other, albeit less trivial means, of bypassing these systems' login security? Having them exposed to the Internet, and readily indexed by anyone who looks, is such a bad idea.

In any event, no matter what happens from here, this made a terrific case study for our one thousand and fourteenth Security Now! Podcast.

We'll see everyone back here next week for number one thousand and fifteen!