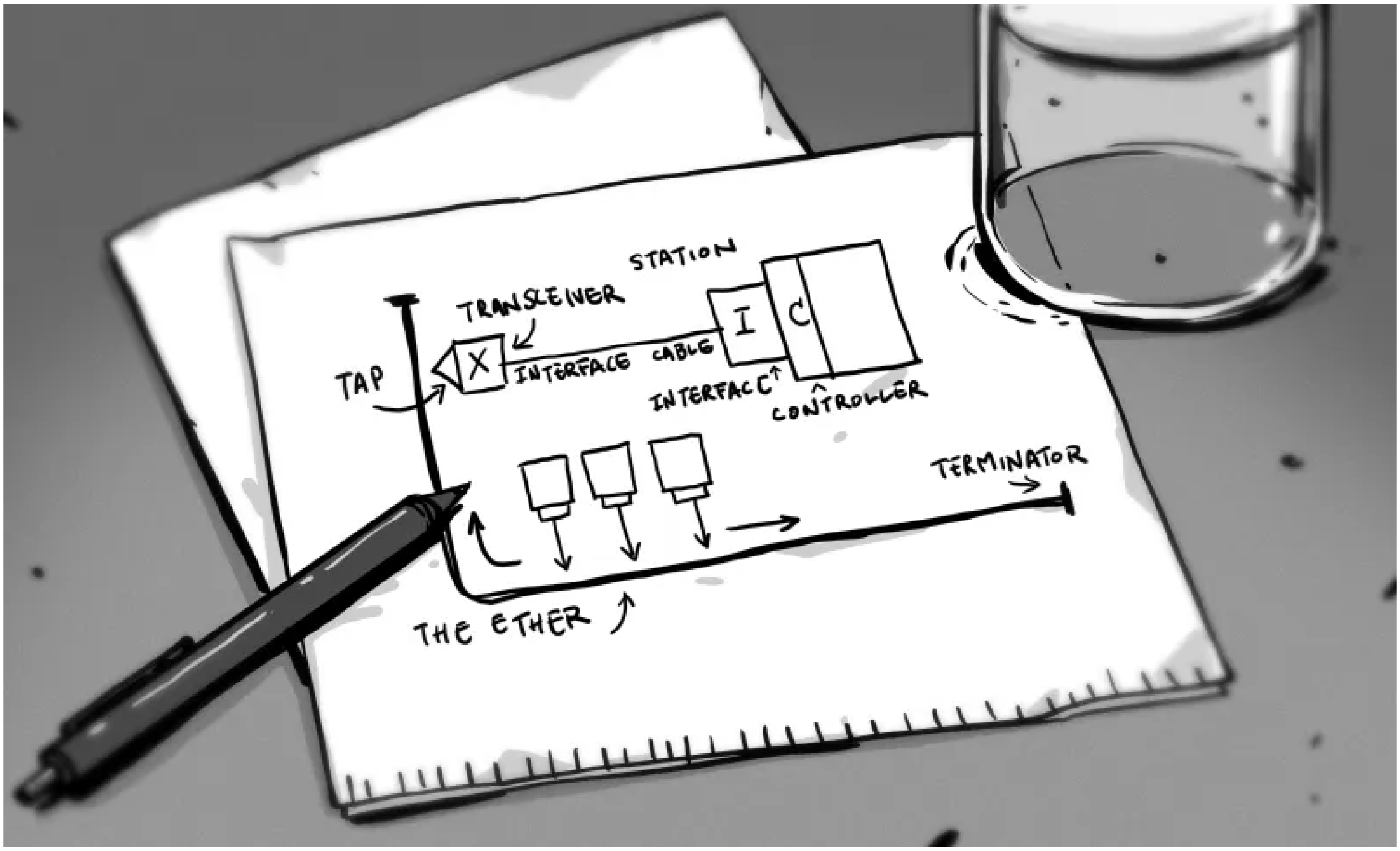
Security Now! #949 - 11-21-23

Ethernet Turned 50

This week on Security Now!

Is there any such thing as truly free privacy? What has Elon done now? What's the latest new tactic in post-breach cyber-extortion? Has Europe finally come to their senses over old and creaky proprietary radio encryption? What new forthcoming iPhone communications feature took everyone by surprise? What discovery did I make for super-secure code signing? Just how sticky are those barnacles? What's a good way to measure USB drive speed? Is the EU's proposed eIDAS 2.0 QWACs system as bad as it seems? And if it passes into law as-is, CAN companies realistically say no? What's my favorite little PC platform for building security gateways? Why couldn't we just use the good part of a fake drive? What should ex-LassPass users watchout for in their credit card statements? And, finally, we recognize the 50th birthday of Ethernet and look back at the history of its creation.

Bob Metcalf's first 1973 "napkin sketch" visualization
of the Ethernet's physical layer conception…



We'll have **MUCH** more to say about this at the end of today's podcast.

Security News

“Privacy is Priceless, but Signal is Expensive”

Last Thursday, Meredith Whittaker, Signal’s CEO whom we saw being the first to stand up to the UK with an absolute refusal to compromise Signal’s encryption, and a lead developer, Joshua Lund, authored a lengthy fund raising wake-up call in the form of a breakdown of their expenses. While they are a registered 501c3 non-profit organization, they maintain a staff of 50 and many significant infrastructure costs. I’ll share the beginning of their posting to give everyone a sense of it. It starts out, under the headline: *“Privacy is Priceless, but Signal is Expensive”*, saying:

> *Signal is the world’s most widely used truly private messaging app, and our cryptographic technologies provide extra layers of privacy beyond the Signal app itself. Since launching in 2013, the Signal Protocol—our end-to-end encryption technology—has become the de facto standard for private communication, protecting the contents of billions of conversations in WhatsApp, Google Messages, and many others. Signal also continues to invest in research and development in the pursuit of extending communications privacy. This commitment underlies our recent work to add a layer of quantum resistance to the Signal Protocol, and our previous work on metadata protection technologies that help keep personal details like your contact list, group membership, profile name, and other intimate information secure. This singular focus on preserving the ability to communicate privately is one reason that we work in the open, documenting our thinking and making our code open source and open to scrutiny—so you don’t have to take our word for it.*
>
> *Signal is also a nonprofit,* ***unlike*** *almost every other consumer tech company.*
>
> *This provides an essential structural safeguard ensuring that we stay true to our privacy-focused mission. To put it bluntly, as a nonprofit we don’t have investors or profit-minded board members knocking during hard times, urging us to “sacrifice a little privacy” in the name of hitting growth and monetary targets. This is important in an industry where “free” consumer tech is almost always underwritten by monetizing surveillance and invading privacy. Such practices are often accompanied by “growth hacking” and engagement maximization techniques that leverage dark patterns to keep people glued to feeds and notifications. While Signal is also free to use, we reject this kind of manipulation, focusing instead on creating a straightforward interpersonal communications app. We also reject business models that incentivize such practices.*
>
> *Instead of monetizing surveillance, we’re supported by donations, including a generous initial loan from Brian Acton. Our goal is to move as close as possible to becoming fully supported by small donors, relying on a large number of modest contributions from people who care about Signal. We believe this is the safest form of funding in terms of sustainability: ensuring that we remain accountable to the people who use Signal, avoiding any single point of funding failure, and rejecting the widespread practice of monetizing surveillance.*
>
> *But our nonprofit structure doesn’t mean it costs less for Signal to produce a globally distributed communications app. Signal is a nonprofit, but we’re playing in a lane dominated by multi-billion-dollar corporations that have defined the norms and established the tech ecosystem, and whose business models directly contravene our privacy mission. So in order to provide a genuinely useful alternative, Signal spends tens of millions of dollars every year.* ***We estimate that by 2025, Signal will require approximately $50 million dollars a year to operate—and this is very lean compared to other popular messaging apps that don’t respect your privacy.***

Their blog post proceeds from there to substantiate that claim and to further detail the nature of their current cash outlay for all facets of what it takes to make Signal go: https://signal.org/blog/signal-is-expensive/

I'm not a big Signal user, though I do have it installed on my phone and desktop because back when I was bringing up GRC's XenForo web forums, one of our listeners, Rasmus Vind, who knew XenForo and PHP came to my rescue and implemented the forum's interface to SQRL, which remains in heavy use and is the way many people logon. Rasmus suggested we use Signal to converse in real time and it worked perfectly. But I have to admit that I never even stopped to consider the fact that Signal was both free **and** devoid of any annoying advertisements or other nonsense.

We've become very accustomed to receiving "free" things in our lives. I have "free" in air quotes because something pays for the things we receive. We grew up, well, those of us with thinning or gray hair, listening to free AM and FM radio and watching free television sprinkled with ads. And today it's still possible to get lots of high quality free stuff if you don't mind ads – like this podcast. GRC's various services like ShieldsUP!, and our growing library of ad-free freeware on a 100% ad-free website is entirely financed by the sales of SpinRite. So the 8,661,248 people who have downloaded and used our DNS Benchmark, and the 68,000 people who have downloaded and used ValiDrive, received something of value for free... but only because a sufficient number of other people have been interested in having access to SpinRite and were willing to pay for it.

So Google exists because of advertisements and extensive tracking. The TWiT network and this podcast are here thanks to advertisements and the direct support of Club TWiT members, and all of the stuff I'm able to do, create and give away is thanks to people purchasing SpinRite.

But what of Signal? What we're living in now is an "Attention Economy" where commercial interests are vying for, and are willing to pay dearly for, people's attention. But not Signal. It occurs to me, and I really hope I'm wrong, that this is going to be a heavy lift and that they're probably in a very tough spot. For all the best and right reasons, they've put themselves in the spot of needing to ask for voluntary donations from a global community that's grown accustomed to getting everything for free... or at least apparently for free. In other words, not needing to directly part with any of their hard earned cash. So how will Signal support itself? **Can** it support itself? It will be up to those who use it and who depend upon its integrity – or perhaps other wealthy donors who want to see it survive – to keep it going. Do most people actually care about the integrity of their messaging service? I've come to doubt it. It's fine if it's there for free. But will they pay for it? Will its users even understand the value they're receiving in return? Or is it just a convenient messaging app they're using without really understanding what's behind it and what it takes to offer such a service with absolutely no strings attached? And that's what differentiates it from everything else – Signal is 100% absolutely no strings attached. Elsewhere in their blob post they write:

> *Data is profitable, and we're a nonprofit, focused on collecting as **little** data as possible. Most tech companies collect and create as **much** data as they can. They build large data warehouses, and then later invent new terms like "data lake" when their unquenchable thirst for more of your private information can no longer fit within the confines of a single warehouse. Their default move is **to store everything for as long as they can** in an easily*

> *accessible and unencrypted format, suffering data breach, after data breach, after data breach, hoping to monetize this data by indirectly (or directly) selling it to advertisers or using it to train AI models. Again, data is profitable.*

They noted that their data storage costs are **far** less than other messaging companies specifically because unlike everyone else, they **only** retain the bare minimum needed for the system to function.

One of the surprising line items they highlighted was the cost of registration. Get a load of this:

> *"Signal incurs expenses when people download Signal and sign up for an account, or when they re-register on a new device. We use third-party services to send a registration code via SMS or voice call in order to verify that the person in possession of a given phone number actually intended to sign up for a Signal account. This is a critical step in helping to prevent spam accounts from signing up for the service and rendering it completely unusable—a non-trivial problem for any popular messaging app.*
>
> *Signal's registration service routes registration codes over multiple telephony providers to optimize delivery across the globe, and the fees we pay to third-party vendors for every verification code we send can be very high. This is in part, we believe, because legacy telecom operators have realized that SMS messages are now used primarily for app registration and two-factor authentication in many places, as people switch to calling and texting services that rely on non-telecom Internet data. In response to increased verification traffic from apps like Signal, and decreased SMS revenue from their own customers, these service providers have significantly raised their SMS rates in many locations, assuming (correctly) that tech companies will have to pay anyway.*
>
> *The cost of these registration services for verifying phone numbers when people first install Signal, or when they re-register on a new device, currently averages around **$6 million dollars per year.**"*

And just think of all the people who might download then set up the app, then wind up not using it that much. My phone is chock full of such apps. Why would I pay anything for something I never use? Yet they're footing the cost of my sign-up verification whether I ever use it again or not. Another thing I appreciated is how lean they're running. They have 50 employees total. How does this compare to other similar services? They wrote:

> *Signal isn't just a collection of privacy-preserving services that route end-to-end encrypted messages and calls around the world. It's also a set of cross-platform apps and modular development components (commonly called libraries) that make this type of private communication possible in the first place. Because the norm is surveillance, we're often required to create or modify our own libraries from scratch, swapping in privacy instead of using more common frameworks that assume surveillant defaults. Swimming against the tide of an ecosystem whose incentives and infrastructure promote surveillance and privacy invasions is, of course, more time-intensive and more expensive, and requires dedicated and experienced people.*

> *First, we have three distinct client teams, one for each platform (Android, Desktop, and iOS). These teams are constantly working: adjusting to operating system updates, building new features, and making sure the app works on a wide variety of devices and hardware configurations. We also have dedicated engineering teams that handle the development and maintenance of the Signal Server and all of its infrastructure, our calling libraries like RingRTC, and core libraries like libsignal. These also need constant development and monitoring.*
>
> *Product and design teams help shape the future of the app and determine how it will look and function, while our localization team coordinates translation efforts across more than sixty languages. We even have a full-time, in-house support group that interfaces with people who use Signal and provides detailed technical feedback and real-time troubleshooting information to every other team. This is an essential function, particularly at Signal, because we don't collect analytics or telemetry data about how people are using Signal.*
>
> *This is a lot of work, and we do it with a small and mighty team. In total, around 50 full-time employees currently work on Signal, a number that is shockingly small by industry standards. For example, LINE Corporation, the developers of the LINE messaging app popular in Japan, has around 3,100 employees, while the division of Kakao Corp that develops KakaoTalk, a messaging app popular in Korea, has around 4,000 employees. Employee counts at bigger corporations like Apple, Meta, and Google's parent company (Alphabet) are much, much higher.*

And the last bit that I wanted to share is this:

> *Growth in Signal translates into increased infrastructure costs, and having more infrastructure requires more labor. As of November 2023, Signal's server network is regularly responding to around 100,000 requests per second, and we routinely break our previous records. A funny thing happens when a globally accessible service starts handling billions of requests every day. Suddenly one-in-a-million possibilities are no longer unique or rare, and unlikely situations become more and more common as Signal grows. It's not unusual for our engineers to do things like write custom code to reproduce an esoteric and complicated IPv6 connectivity issue that's affecting people running an arcane operating system configuration in specific regions, but only when connected via a certain set of internet service providers. Troubleshooting such infrastructure issues can be very expensive, because isolating a problem and developing a fix can take a lot of time and expertise.*

When I opened the app just now, I found a request for a donation. Clicking the "Donate" button took me to a screen which read: *"Privacy over profit. Private messaging, funded by you. No ads, no tracking, no compromise. Donate now to support Signal. (Read More)"* Having read everything I just had, I decided I would give them some money. So I selected an amount and was taken to a screen that said *"Donate to Signal. Get the Signal Boost badge"* and the payment options were Apple Pay, Debit or Credit Card, or PayPal.

It'll be interesting to see whether a user-supported secure message system is an oxymoron. Can such a system support itself? I have no idea whether a sufficient number of users will step up and pay – and on the ongoing basis that Signal requires – to use a miraculously secure and clean service that's truly free in every sense of the word. I'm not inclined to pay continuously because I don't use it on a regular basis. I am a continuing supporter of Wikipedia because I do often use it.

My fear, based upon everything I've seen, is that people do not appreciate and probably cannot appreciate what Signal is, and that they use it because among all of the other free messaging services, they can see that it's the cleanest and totally free of debris. But they have no idea why. The problem is that being totally debris free is an expensive service for Signal to deliver. I'm glad they took the time to explain their financial reality. Those of here, get it. But most Signal users will never see this posting and without that posting that "Donate" button at the bottom of Signal's screen doesn't pack nearly the same punch.

Twitter / X loses additional advertisers

Last week I received a number of Twitter DMs from our listeners who fell on both sides of the most recent Twitter brouhaha. Because of that, while we're on the topic of the support for free services, and because I've said that I plan to create a secure eMail-based means for our listeners to send me Tweet equivalents, for those who haven't heard, last week, after Elon Musk Tweeted something that many found extremely offensive, more than 12 of Twitter's **major** advertisers suspended their advertising on Twitter. This included Apple, Sony, Disney, Lionsgate, Paramount, Comcast, Warner Bros, and IBM. Elon's response, was to Tweet: *"Many of the largest advertisers are the greatest oppressors of your right to free speech."* Now, I think Elon often voices the first thing that comes to mind. I'm sure he knows that the 1st amendment of the US Constitution, which protects its citizens from our **government's** suppression of speech – often referred to as "free speech" – has nothing whatsoever to do with the way private corporations choose to manage their own communications. That's entirely up to them. Elon has every right to do whatever he wants to with Twitter, which he now owns. And major American corporations have no obligation to spend their advertising dollars where they don't want to. So the idea that large advertisers are the great oppressors of free speech is utter nonsense. I love the fact that in these United States Elon gets to express his feelings any way he wants to and that, in turn, his service's users and its advertisers get to express their feelings by deciding what they want to do.

Ransomware Group Files SEC Complaint Over Victim's Failure to Disclose Data Breach

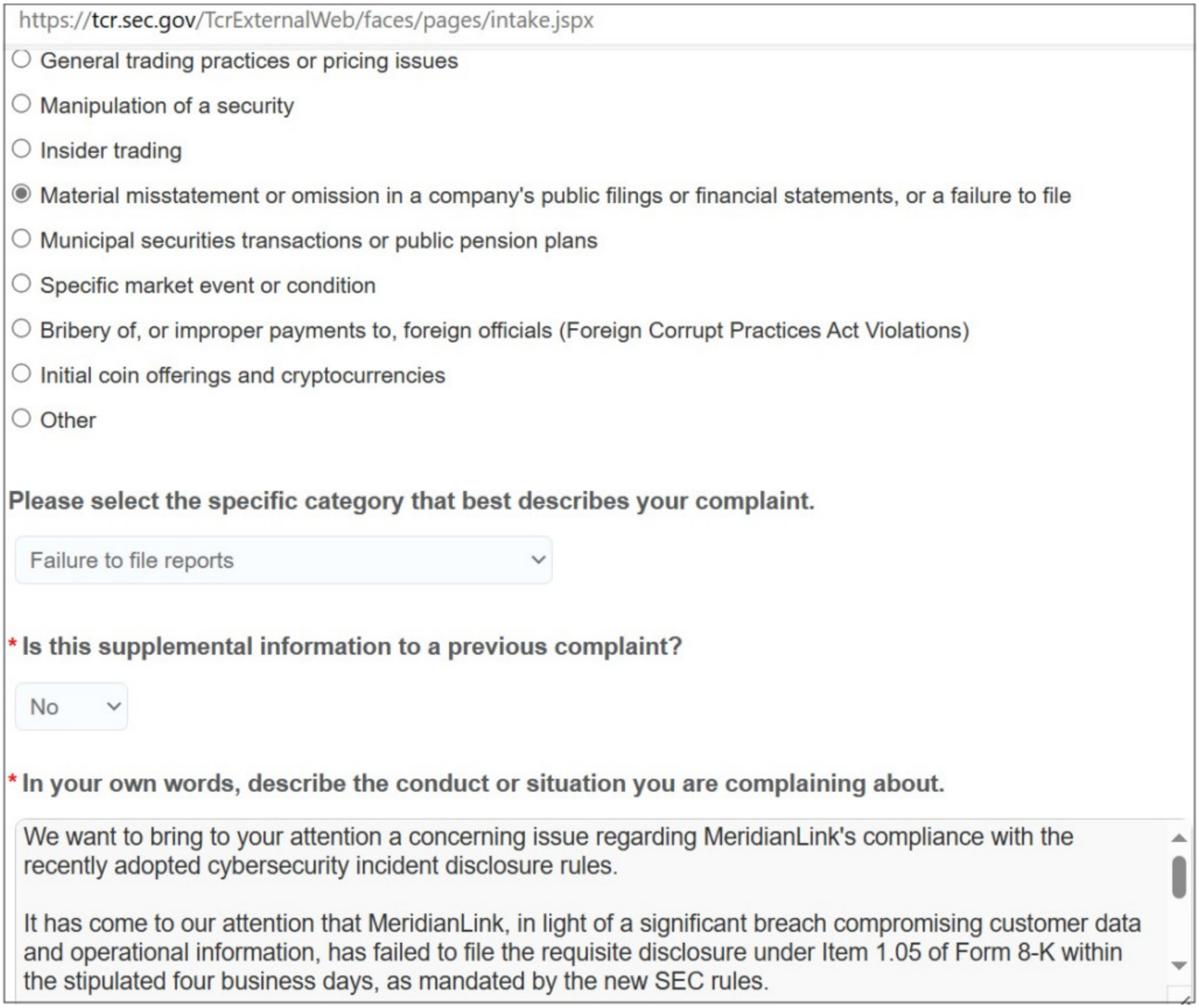
Here's one that just makes your head shake. It was tied for most listener news mentions with feedback about last week's discussion of The Barnacle, which we'll be getting to a bit later.

We've talked before about how ransomware has evolved. In the good old days, ransomware attackers would just encrypt a businesses various servers, workstations and backups and leave it at that. But when that wasn't always delivering the results they wanted – meaning getting paid in lots of cryptocurrency in return for providing the decryption keys – some of the gangs would launch a powerful DDoS attack against the company to increase their pressure. And when even that didn't work, the gangs began exfiltrating the enterprise's data before encrypting it so that they could also hold it ransom, threatening to release it to the public or to sell it on the dark web unless the enterprise met their extortion demands. And, in true escalation, when even **that** wasn't producing the results they sought, they further threatened to use the exfiltrated data to contact the victim's clients and customers, informing them directly that the company had lost control of their personal and presumably private data. This brings us current, where today, believe it or not, we have yet another step upward in this seemingly endless escalation:

The ransomware group known as Alphv and BlackCat claims to have breached the systems of MeridianLink, a company based in California that provides digital lending solutions for financial institutions and data verification solutions for consumers. So, seemingly quite sensitive data.

This cybercrime gang claims to have stolen a significant amount of both customer data and operational information belonging to MeridianLink, and they've been threatening to leak it unless a ransom is paid. But apparently negotiations were not going as well as they hoped so they decided to escalate. So what could they do to make matters worse for MeridianLink? In an effort to increase their chances of getting paid, the malicious hackers claim, and have presented documentary evidence, to have filed a complaint with the U.S. Securities and Exchange Commission, our SEC, against MeridianLink, accusing the company of failing to disclose the breach – which they, themselves, perpetrated – within four business days, as required by the new rules announced by the SEC in July.

The BlackCat group published screenshots on its leak website last Wednesday, November 15th showing that the complaint has been filed and received by the SEC. I have their screen shot in the show notes.



https://tcr.sec.gov/TcrExternalWeb/faces/pages/intake.jspx

○ General trading practices or pricing issues

○ Manipulation of a security

○ Insider trading

● Material misstatement or omission in a company's public filings or financial statements, or a failure to file

○ Municipal securities transactions or public pension plans

○ Specific market event or condition

○ Bribery of, or improper payments to, foreign officials (Foreign Corrupt Practices Act Violations)

○ Initial coin offerings and cryptocurrencies

○ Other

Please select the specific category that best describes your complaint.

Failure to file reports

* **Is this supplemental information to a previous complaint?**

No

* **In your own words, describe the conduct or situation you are complaining about.**

We want to bring to your attention a concerning issue regarding MeridianLink's compliance with the recently adopted cybersecurity incident disclosure rules.

It has come to our attention that MeridianLink, in light of a significant breach compromising customer data and operational information, has failed to file the requisite disclosure under Item 1.05 of Form 8-K within the stipulated four business days, as mandated by the new SEC rules.

From the multiple-choice selection, they chose “Material misstatement or omission in a company’s public filings or financial statements, or a failure to file.”

Under the category that best describes the complaint they chose: “Failure to file reports.”

And in the fill-in for *“In your own words, describe the conduct or situation you are complaining about”* these criminals wrote: *“We want to bring to your attention a concerning issue regarding MeridianLink’s compliance with the recently adopted cybersecurity incident disclosure rules. It has come to our attention that MeridianLink, in light of a significant breach compromising customer data and operational information, has failed to file the requisite disclosure under Item 1.05 of Form 8-K within the stipulated four business days, as mandated by the new SEC rules.”*

I want to pause here for a moment to take note that the grammar used in this posting is uncharacteristically excellent. Since this is so rarely seen from non-native English speakers, and the AlphV gang operates out of Russia, my first thought was that ChatGPT, or one of its ilk, might have had a hand – or a register – in producing this prose. However, nice as that bit was, the group screwed up a few other substantive and material details that directly bear on the success of this.

First, there’s some confusion over the date of the breach. The hackers told the site “DataBreaches.net” that the attack against MeridianLink — which only involved data theft, **not** file encryption — was conducted two Tuesdays ago, on November 7th and that it was discovered by MeridianLink the same day.

However, MeridianLink has told the tech press that the intrusion occurred three days later, on Friday, November 10th. They said: *“Upon discovery on the same day, we acted immediately to contain the threat and engaged a team of third-party experts to investigate the incident. Based on our investigation to date, we have identified no evidence of unauthorized access to our production platforms, and the incident has caused minimal business interruption.”* Of course, if it was data exfiltration and not encryption, no interruption would have occurred. If MeridianLink is able to assert formally, as they apparently have in reporting, that they quickly detected the breach, engaged a 3rd-party forensics team, and have so far identified no evidence of unauthorized access to the system containing the sensitive customer data, then they would have had no cause to inform the SEC under the new 4-day rule.

But even so, though such disclosure would be prudent for any publicly traded company, that new 4-day rule doesn’t actually go into effect until the middle of next month on December 15th. The way that new and still-pending rule is written, companies will be required to notify the SEC within four business days of determining that a cybersecurity incident is material to investors, which, based on MeridianLink’s statement, does not appear to be the case.

And I think it’s probably significant that the one thing that appears to be conspicuously absent is even a shred of actual proof of this breach from the attackers. Uncharacteristically, following any true data breach, nothing has been posted to the dark web to confirm and prove that the attackers actually did obtain any sensitive data. So it appears that MeridianLink is correct in their statement that nothing material was obtained by the hackers and that the entire extortion incident with the SEC may have been an empty threat.

But even so, this made headlines in the tech press because although threats have been made in the past by many ransomware and extortion gangs, that they would follow up their theft of data with reports to the SEC, this appears to be the first time a ransomware group has actually followed through and filed an SEC complaint against one of its victims.

Europe to open "TETRA" radio encryption

There's some welcome news in the world of open versus closed encryption standards. Last summer we covered the story of serious flaws being found in yet another closed and proprietary radio encryption system. The fastest way to bring everyone back up to speed is for me to share part of what WIRED wrote in their coverage of the discovery at the time. They said:

> *For more than 25 years, a technology used for critical data and voice radio communications around the world has been shrouded in secrecy to prevent anyone from closely scrutinizing its security properties for vulnerabilities. But now it's finally getting a public airing thanks to a small group of researchers in the Netherlands who got their hands on its viscera and found serious flaws, including a deliberate backdoor.*
>
> *The backdoor, known for years by vendors that sold the technology but not necessarily by customers, exists in an encryption algorithm baked into radios sold for commercial use in critical infrastructure. It's used to transmit encrypted data and commands in pipelines, railways, the electric grid, mass transit, and freight trains. It would allow someone to snoop on communications to learn how a system works, then potentially send commands to the radios that could trigger blackouts, halt gas pipeline flows, or reroute trains.*
>
> *Researchers found a second vulnerability in a different part of the same radio technology that is used in more specialized systems sold exclusively to police forces, prison personnel, military, intelligence agencies, and emergency services, such as the C2000 communication system used by Dutch police, fire brigades, ambulance services, and Ministry of Defense for mission-critical voice and data communications. The flaw would let someone decrypt encrypted voice and data communications and send fraudulent messages to spread misinformation or redirect personnel and forces during critical times.*
>
> *Three Dutch security analysts discovered the vulnerabilities—five in total—in a European radio standard called TETRA (Terrestrial Trunked Radio), which is used in radios made by Motorola, Damm, Hytera, and others. The standard has been used in radios since the '90s, but the flaws remained unknown because encryption algorithms used in TETRA were kept secret until now.*
>
> *The technology is not widely used in the US, where other radio standards are more commonly deployed. But Caleb Mathis, a consultant with Ampere Industrial Security, conducted open source research for WIRED and uncovered contracts, press releases, and other documentation showing TETRA-based radios are used in at least two dozen critical infrastructures in the US. Because TETRA is embedded in radios supplied through resellers and system integrators like PowerTrunk, it's difficult to identify who might be using them and for what. But Mathis helped WIRED identify several electric utilities, a state border control agency, an oil refinery, chemical plants, a major mass transit system on the East Coast, three international airports that use them for communications among security and ground crew personnel, and a US Army training base.*

We dug into this much more deeply at the time, but that explains the breadth and importance of this system. It is far more widely used throughout Europe than in the US, but that doesn't make its security any less important. The fact that the system is so old, that it's been in place since the 1990's, likely explains part of the problem. Once again we have inertia. We think it's encrypted. The colorful glossy brochure says it uses super-fancy "Air Interface Encryption" – whatever that is – and we already have a huge investment in these radios in the field, so we really don't want to be told that it's all crap.

So here's the good news: Although the gears are turning as slowly as ever, after being bombarded with well-deserved criticism for keeping its crappy encryption algorithms secret for the past 25 years, the European standards body ETSI, behind the TETRA algorithms, has decided to finally open them to the public for scrutiny. (Although one could argue that those three Dutch security analysts already did that.)

At the time, Matthew Green, the Johns Hopkins University cryptographer and professor whom we often quote called the technology in use old-fashioned and behind the times for continuing a practice of secrecy that had long been abandoned by the security world. When asked about the recent decision to open the encryption to the world, he said: "This whole idea of secret encryption algorithms is very 1960s and 1970s and quaint. It's nice to see them joining us here in the 21st century." And having now made the decision to go public, now they're owning it. ETSI's statement said *"Keeping cryptographic algorithms secret was common practice in the early 1990s when the original TETRA algorithms were designed. Public domain algorithms are now widely used to protect government and critical infrastructure networks, for example AES (the Advanced Encryption Standard, standardized by the US government). Effective scrutiny of public-domain algorithms allows for any flaws to be uncovered and mitigated before widespread deployment occurs."* Right. As Matthew said, "welcome to the 21st century."

RCS is coming to iPhone

Meanwhile, late next year, those green boxes which appear in iMessage whenever the message's recipient is "out of system" – which typically means an Android user – will be getting many more features. In a move that few saw coming, last Thursday Apple announced that it will be adopting the RCS – which stands for Rich Communication Services – messaging standard. This will finally bring, for the first time, a wide range of iMessage-style features to messaging between iPhone and Android users. This has been made possible as RCS has continued to develop and become a more mature platform than it was originally.

RCS on iPhone will bring many iMessage-style features to cross-platform messaging with things like read receipts, typing indicators, high-quality images and videos, and more. Apple's implementation will also give users the ability to share their location with other people inside text threads. And unlike regular SMS, RCS can work over mobile data or Wi-Fi as well.

At the same time, iMessage isn't going anywhere. It will continue to be the messaging platform used for all "in-system" communication between iPhone users. RCS will simply replace SMS and MMS and exist separately from iMessage when it's available. And SMS and MMS will also continue to be available as a fallback when needed. So as an iPhone user myself, it will be nice to retain some of those goodies when messaging with others' green balloons. :)

SpinRite

On my end, I'm still working on the dynamic server-side code-signing technology I'll be using for all future SpinRite and other commercial software downloads. My favorite discovery last week was finding that Yubico now makes their own HSM which is, as we know, used for securely storing keys and for using them to perform crypto operations inside the HSM so that they are never exposed to any possible hacking. Since their key is called the YubiKey it won't surprise anyone that their HSM is the YubiHSM. There's a YubiHSM 2 and a YubiHSM 2 FIPS which provides additional certification assurances. Since EV code signing certificates can only be signed by FIPS-certified HSM's Yubico has that covered for me. Aside from the fact that it's by Yubico, which is reason enough for me, it is vastly more capable than the Gemalto/Thales SafeNet 5110 dongle that I've been using for manual code signing. It's able to hold many more keys, it can work with much longer keys and it supports many more much more recent crypto algorithms.

The Gemalto/Thales device I had been using has virtually zero developer support. I wrote to them last week requesting access to their developer SDK and I received the reply: "You didn't purchase it from us, so go away." By comparison, Yubico's developer support is astonishing. The product has been around for a while, so it's only that I hadn't been paying attention. But as a consequence, a sizable body of terrific developer support has grown up around it.

Anyway, I'm super happy that my Internet searches stumbled upon this last week. And needless to say, for anyone who may have been thinking – with all of the attention we've recently been giving to the need for an HSM – that switching to one might make sense, now you know that a favorite company of ours, Yubico, offers a terrific looking solution!

Okay, let's close some loops. This past week (still using Twitter) our terrific listeners asked and shared some great tidbits and observations...

Closing the Loop

PhobicCarrot / @PhobicCarrot

@SGgrc: Is this a joke? Someone could easily slide something between the suction cup and the windshield to remove it. Haven't you ever removed a suction cup before? I am guessing a playing card or credit card would do the trick.

Fredrik / @fbrannhage

@SGgrc: How do you beat windshield Barnacle? As it turns out, to take off the Barnacle, all you need to do is run your vehicle's windshield defroster for 15 minutes, and then use a credit card or similar thin piece of plastic to release the suction cup around the edge.

My guess is that the defroster heats the windshield which causes the air trapped underneath The Barnacle's two massive suction cups to expand. That, in turn, lifts it away from the windshield which allows a shim of any sort to be slid underneath to break the suction cup's seal.

art nilson / @art_nilson

Hi Steve - I have a need to determine if a USB drive is fast or slow at writing. Read Speed and ValidDrive are very close to giving me this, but not quite there.. Any suggestions?

Hmmm. ValiDrive is not a useful test for real world speed because it continuously alternates between tiny reads and tiny writes. Not only is that not the way such drives are typically used, but my theory (soon to be confirmed or repudiated) is that many thumb drives may have an especially difficult time getting ready to write after reading. Since ValiDrive is not the way drives are typically used, that's not something that many have been optimized to do.

ReadSpeed fails to meet your needs for two reasons. First, it won't run on USB. It was designed during the early SpinRite work as a test of SpinRite's new native drivers. Secondly, you want a **writing** speed benchmark, not just reading and "ReadSpeed", as its name suggests, only benchmarks read tests.

SpinRite v6.1 has a very nice new drive benchmarking system which will benchmark any drive, including USB drives, in three places: front, middle and end. But like ReadSpeed, SpinRite is only benchmarking read performance. However, If you are a SpinRite owner you could grab the latest pre-release code for it. Level 1 is a read-only test and Level 3 writes back what Level 1 reads. So Level 3 is both reading and write. Until we get to SpinRite 7, SpinRite is still forced to access drives through the machine's BIOS. And that limits us to 127, 512-byte sectors, but that's more than 65,000 bytes at a time. SpinRite 6.1 also allows you to set precise starting and stopping points, down to the single physical sector number. And when it stops it shows and logs the exact time required to do whatever you told it to. So you could first run SpinRite at Level 1 over a specific region and sized region of the drive and note the time required for that pure reading operation. Then, do exactly the same thing but at Level 3. Since Level 3 only adds writing of what was read, the **difference** in the timing of the two levels will entirely be due to the drive's true writing speed for that amount of writing. Since SpinRite v6.1 also now logs not only the percentage of the drive, but also the exact physical sectors, you'll get the exact could of bytes written by multiplying the sector span by 512 bytes per sector, and can then calculate the drive's write bandwidth.

Now, having just written all of that, I realized that with a tiny change to ValiDrive, it **could** become a very nice freeware USB drive read and write performance benchmark. I never really knew why I was posting all of that read and write performance statistics with min, max, median, standard deviation and variance, but now I know. All that would need to be changed for ValiDrive to become a very useful and precise benchmark, would be to have it transfer much larger blocks of data at once. Then, its measured performance, which ValiDrive already does beautifully, **would** echo a drive's speed in the real world.

I've been planning to revisit ValiDrive once SpinRite 6.1 is packaged and finalized. So now I have another reason to create a ValiDrive v2.0. That'll make it quite useful for more than just checking drives for their validity.

I replied to Art via Twitter before I hit on the idea of using SpinRite in a read and read/write mode to isolate writing speed. His reply Tweet was: *I have been running it regularly during development, but my systems are just boring....Spinrite always just worked.*

T A Hofer / @tahyonline
I'm quite certain that Thomas would not mind my sharing his Twitter DM with everyone here. And I definitely want to since he has done a terrific job of painting the picture of the problem that the EU's eIDAS v2.0 QWAC's system is intended to solve. Here's what Thomas shared with me:

> *Dear Steve,*
>
> *Thank you for your relentless coverage of the sometimes too exciting cybersecurity world — and for providing an insightful and entertaining way to earn CPEs!*
>
> *Listening to your coverage of Article 45 and QWACs (perhaps pronounced as kwaks?) or qualified website authentication certificates, it piqued my interest and after some research, I thought I might be able to add perspectives to understand the motivations that I have observed having worked in financial services (the previous globally connected network before the internet) in strategic, operational and audit roles.*
>
> *Well, I am not for or against QWACs, I am not even in the EU anymore, nevertheless these are a few thoughts about this from a compliance perspective.*
>
> *The EU would definitely propose that technology is too big for any single country and that is why they legislate for the territory of the EU. At the moment, practically all major providers are US-based operating under US law. For example, the AWS CDN CloudFront operates in the Virginia region of AWS, where data passes through the territory of the US. Although you, residing within the US, enjoy the protections of the Constitution and other laws enforcing, for instance, your right to free speech and restricting unreasonable search and seizure, these protections don't apply to me and my data passing over there, as I reside in the UK.*

> *The kerfuffle about GDPR, privacy and safe harbor agreements with the US were somewhat about companies, but more painfully about protections against government intrusion.*
>
> *Although it’s true that companies terminate TLS sessions on the edge and do filtering for internal networks, so do CDNs covering a vast part of internet traffic and if routed through US territory, the providers have obligations under US law. That is why the EU would want to assert legal primacy over their own citizens and territories.*
>
> *The financial services industry has already gone through this process about a decade ago and US international banks established local subsidiaries operating under the EU directives. Value added tax or VAT is a similar example: it used to be possible to buy digital content from US companies without VAT, now it’s not, they all registered for VAT. Indeed, if you are a European client of Google, you would be contracting with Google Ireland showing that large US tech providers have already adapted to increasing local laws and regulations on technology.*
>
> *Based on the materials available about QWACs, they appear to serve the exact opposite of eavesdropping. They appear to be THE banner: the idea is that if a QWAC has signed the site certificate, then this would show in the address bar as OV and EV used to. Documentation available on the European Parliament website show that QWACs are considered super-EVs, and would be used to provide assurance that users, and particularly payments providers, are connecting to legitimate counterparties.*
>
> *This way, QWACs would actually defeat eavesdropping and transparent TLS-terminating proxies, because CloudFlare or AWS might be able to issue a valid certificate for the Swedish Government website on the fly, but cannot issue one signed with a QWAC.*
>
> *By the way, that would also be the simplest way to expose eavesdropping, if any: just show a banner that the site used a QWAC-signed certificate. This also answers the challenge of technical feasibility. There is no need to insert a banner into web traffic, as the CA certificate being a QWAC is the banner.*
>
> *For the countries in question, the governments are the elected representatives providing the checks and balances over the technology companies, not the other way around. From Germany’s or France’s perspective, the Mozilla Foundation might not look like an organization that has to police them, rather, they might demand that Mozilla put the countries’ CAs in the trusted store if Mozilla wants to do business there. That’s really the crux of the issue, the QWACs are already long there, just not added to the trust stores.*
>
> *Mozilla might choose not to add them, but it is less unlikely that Apple, Google, Microsoft and others would leave a market as big as the EU, just as large US banks chose to operate under local laws there, too. And yes, that’s a more fragmented world, for better or worse. :-(*
>
> *Apologies, long message, hopefully somewhat useful. Wishing all the best and looking forward for 999, perhaps 0xAAA and beyond… Kind regards, Thomas*

I think Thomas’ counterpoint is a terrific one. It’s useful to see both sides of this.

There are a couple of corrections that I need to make. For one thing, CDNs like CloudFlare actually **do** terminate the HTTPS TLS connections coming into their proxies with their customer’s actual certificate. I looked into this at one point and learned that they had several ways to do this. A customer could provide their certificate or make it available for CloudFlare's use without losing control of it. It's very slick... but it also means that even fully proxied and decrypted communications would still bear the QWACS seal.

So this means that if the presence of a QWACS certificate was somehow surfaced on the browser's UI chrome (where "chrome" used in this instance is the generic term for all of any browser's non-webpage content window dressing), it would be providing a false assurance that eavesdropping had not occurred and was not possible.

I haven't spent too much time digging into this myself because that time would be wasted if QWACS never materializes. But if it appears as though it's going to then I'll definitely be coming up to speed with the details.

The question is, is QWACS a counter-signing of a certificate that was also signed by an existing Certificate Authority for browser trust, or can it also be used stand alone? It would seem that browsers could be designed to require that any QWACS-signed web certificate also be signed by a traditional CA. But then, even so, Thomas describes the effect of this as a sort of super-EV cert – which is likely accurate and exactly what the EU wants. The trouble with that, is that the web industry already had "EV" which was shown proudly on the browser's chrome... and it collectively decided that it was a bad idea to show "extra trust and encryption goodness" to browser users because it could be abused by any site that got an EV cert then used that cert to do bad things to their visitors... under the misunderstood banner of "extra trust and encryption goodness."

If this eIDAS 2.0 QWACs business looks like something that will actually come to pass, you can count on receiving a 100% fully detailed description of exactly what it is right here... because I'm going to want to find out and share it.

I received another note, which is a fitting follow-up to this, from a listener who asked me not to share his name. He wrote:

> *Hi Steve, Thank you for your podcast. It has been a great source of information, laughs, and concerns :)*
>
> *Your explanation of how root certificates work and how Article 45 could be misused has been a factor of stress. I listened to the episodes SN-983 and SN-984 and then went on to read the show notes, just to be sure that it was as bad as I had understood.*
>
> *I was curious about the number of CAs trusted by my Firefox browser and there it was: I counted 165 root certificates. After some manual cleaning, I was able to reduce this number to 84 entities. Some of these are from European countries, many from the United States and China, then we have also from Slovakia, South Africa, Tunisia, Ecuador and many more.*
>
> *From what I understand, any of these 165 Root certificates counterparts could be used to intercept my communications. I have to trust that none of these 84 CAs will lose their signing private keys or be compromised by one of the powerful states that have the capability to intercept communications worldwide.*

*So there's no way to ensure real privacy, even if I remove all but the root certificates that I know are needed for my communication, the CA of the cert used in the TLS will be able to intercept it**?***

He ended that sentence with a question mark. So I'll just say that, yes, that's 100% correct. He finishes:

Is it just me, or is this system still largely based on faith? It seems to rely on the expectation that all participants will behave ethically, and be highly competent in protecting their "precious" keys.

So, yes, just to be clear, our current system of global trust is fragile. This is largely why so many well-placed parties have spoken out against the idea of having the EU muck around with it in any way. All that can do is destabilize an already somewhat precarious system of trust.

The reason the system we have works at all, is that the incentives strongly favor rigorously correct behavior from every single one of those trusted CA's. We've talked about this in the past but it's worth refreshing: Being able to charge money for encrypting the hash of a certificate after verifying its statements is a profitable privilege, not a right. And it's a privilege that those running the world's few root stores can, will, and have rescinded after sufficient evidence of misconduct has been found. No CA wants to lose their privilege of charging money for encrypting a hash. So, as I said, the incentives which are built into this system strongly favor rigorous compliance. We've talked about mistakes and deliberate misconduct here in the past. But overall, the whole trust-based system has been functioning amazingly well.

And everyone wants it to stay that way, which is why allowing EU countries to unilaterally mandate that their individual countries' own certificates **must** be present in OS and web browser root stores, and that there can be absolutely no oversight or recourse by any browser, is politicians with a bad idea running amok. The entire idea runs absolutely contrary to the historical communal spirit which has carefully evolved through the years and which, perhaps against all odds, has been working. This must not be allowed to happen.

M / @mgoldsberry

Hey there, Steve. Long time listener. I just wanted to pass along an observation about your musings on EU Article 45. It is in no way similar to the UK messaging demand. If Apple chooses to remove iMessage in the UK, there is absolutely zero impact to their bottom line. People in the UK still buy iPhones and Macs. But if the entire EU—an enormous market for any tech vendor—decides browsers and operating systems will conform, Apple, Microsoft, and every other publicly traded stock company will absolutely comply. Remember, these companies are owned by stockholders. If Apple executives decided to drop such a major market on principle, their board would fire them before you could say "fiduciary duty." If their board refused to do that, the board would be replaced by the shareholders (many of them financial activists) sooner than you could say "shareholder lawsuit."

Opportunities to exchange potential income for principled stands disappeared when they no longer owned a majority of their own stock. Thanks for the show.

I don’t know how to reply to that, but I hope it’s not true. At the same time, “M”s logic seems sound. We did once have our browser’s crypto deliberately compromised by having strong crypto—any symmetric crypto with a key longer than 40 bits—classified as a munition and therefore against the law to export. Even crypto ideas, conversations and the publication of papers was banned. It was a sad state of affairs at the time. The cryptographer Dan Bernstein sued the State Department using a 1st amendment free speech argument. Anyway, as I’ve been saying more often recently... we’re all living through some very interesting times.

Bob Van Valzah / @bobvan

I love having a personalized copy of SpinRite 6.0. But if you add code signing to personalization for 6.1, how will it ever develop a trusted “reputation” with A/V tools? No two binaries will ever be the same.

Yes. That’s absolutely a problem that’s been haunting me. But here are two points: I’ve confirmed that code signing with an EV certificate, as opposed to a non-EV cert, **does** convey special meaning to Microsoft’s SmartScreen filter. It cares if the signer qualified to receive an EV certificate. (And given the hoops that DigiCert jumps its certificate users through in order to qualify, I’m not surprised.) Also, there’s apparently some level of heuristics at play with the most modern A/V. All of the test releases of SpinRite’s Windows boot prep component have been signed. And they’re all different. But for whatever reason, they have not been setting off alarms for SpinRite’s testers. I’ve looked carefully at what VirusTotal has to say about them, and there does appear to be significant behavior and proximity matching going on for the specific purpose of reducing false positives for “near relatives” that have long been shown to be benign. So I think we’re going to be okay.

Nathan Rzepecki / @Lionslair50

You mentioned you use a pfsense router. I'm interested in switching my router from a ubiquity edge router to pfsense. Mainly because I want to use multiple vlans and wireguard / tail scale networks. Have you shared any details of what you use hardware wise for pfsense or could this be a topic for an episode. I know it's not directly security related for the show. But I would be interested in knowing some of what you're willing to share for your personal home / work / office setup. Thank you for reading this far #securitynow

I’ve been completely happy with the NetGate SG-1100 that I have here. It’s a perfect starter router with three fully independent NIC interfaces. One for the WAN, and two for LANs that can be configured and filtered separately. As we know, that little router’s “wall wart” power supply began causing it to randomly reboot. But after switching to another beefier 12vdc supply it has returned to absolute stability.

But when I was setting things up in the new home I was establishing with my wife, who at the time was my girlfriend, I chose differently. I went with Protectli. https://protectli.com/ Their website’s homepage banner says: “#1 Appliance for Open-Source Software.” I was recently discussing them with Alex Neihaus (recall from Astaro, one of this podcast’s original commercial supporters). He had independently settled upon Protectli and he’s also 100% happy with his choice. So that’s the direction I would go without question.

I purchased the 4-port device, but they have 2, 4, and 6 ports in a very wide of configurations and speeds: https://protectli.com/product-comparison/ And they even offer 4G LTE failover in the case of a WAN outage to keep the network live. The routers are user configurable for storage, RAM, and processor. You can get it bare bones or with software preinstalled, and it runs everything since it's essentially a generic fanless PC with either a CoreBoot or AMI BIOS. You can purchase directly from them to get exactly the configuration you want, and Amazon also sells them off the shelf if you're in a hurry. Until and unless something better comes along, that's what I'll be doing and recommending. Protect-Li — PROTECTLI

Anon John wrote:

> *Hi Steve, something worth sharing: We've rolled out uBlock Origin, specifically to combat malvertising. Thus far it's only deployed in IT, we aim to deploy enterprise-wide (25k users).*
>
> *We recently saw 'Redline stealer' malware, where uBlock wasn't deployed, delivered via malvertising. It slid past EDR but luckily, C2 comms were stopped by a cloud proxy.*
>
> *Blocking advertising categories at the proxy would be a choice, but that results in user browsing issues and so far uBlock has generated barely a peep of user feedback. Perhaps this tale might encourage others to implement security controls for malvertising.*

John's note causes me to realize that we've only been talking about minimizing the annoyance of ads and the tracking aspects. But malvertising, as John reminds us, is also a real thing. The other place my mind jumped to was those Adamnet.works guys whose DNS-based trust no one white-listing approach is also designed to perform this sort of blocking. It would block the browser from ever loading the malvertising content in the first place and then like John's proxy, it would also block access, either by DNS lookup or by direct IP, to the malware's command and control base if, for example, the malware were to ride in on someone's personal machine.

Mike Liljedahl / @lij1954

> *So, can I change the declared size of my mostly fake 2TB stick that is actually 32 GB and can I then use that 32GB for storage? Thank you*

From Mike's terse message it appears that he ValiDrive over a 2TB drive and discovered that it only contained 32GB of actual memory. There's been some discussion of the prudence of reformatting a fake drive to its actual size. GRC's InitDisk utility could be updated to incorporate a true drive sizing feature. It would exactly locate the physical end of the drive, then intelligently give it a file system that matches the drive's true size. But the question was raised about the wisdom of **ever** trusting the memory of a drive from people who are clearly crooks and who are clearly in the "crook business" of selling deliberately bogus drives. For all we know, the chips they're using were swept up off the floor at the end of the shift because they failed other critical reliability tests. They got'em cheap because no one else wanted them. They don't seem like a good place to place anything that anyone ever wants to retain. Since a true and authentic 32GB drive is very inexpensive — a SanDisk brand 32GB Ultra Flair USB 3.0 Flash Drive is $7.69 from Amazon. If one cares at all about the data they're storing on the drive, that would make much more sense.

Shoeless Scoop 🍨 / @ShoelessScoop

> *I am glad I used a Privacy card for LastPass. Because I canceled my account back when you aired the LastPass breach, and they have* ***not*** *stopped trying to charge my family membership. Clearly the days of them being a good company are gone.*

I wanted to share this since not everyone scrutinizes their credit card statements closely and the idea of continuing to be changed for a previously canceled password management service many months later is more than disappointing.

Ethernet Turned 50

What do you get when you subtract 1973 from 2023? You get "50" – and since the design for the Ethernet was first famously sketched out on the back of a coffee stained napkin in 1973, earlier this year the Ethernet turned 50. Many podcast moons ago we thoroughly and deeply covered both the electrical and logical operation of the Ethernet. And its official birthday was widely celebrated in May. But last Thursday the 16th, the IEEE Spectrum magazine posted a birthday retrospective that I thought everyone here would enjoy. With a bit of editing and my editorializing added, here's what they had to say under their title of "Ethernet is Still Going Strong After 50 Years. The technology has become the standard LAN worldwide". They wrote:

> *The Xerox Palo Alto Research Center in California has spawned many pioneering computer technologies including the Alto—the first personal computer to use a graphical user interface—and the first laser printer.*

I've mentioned this before, but that printer was known as the XPG-1. And by coincidence I was there at the time. I clearly recall the silver serial number plaque on the back of the printer which had a bunch of 0's and a single 1' – it was XGP-1, serial number '1' – and I had the privilege of designing and building the first interface for that printer to the DEC PDP-10 at the nearby Stanford University Artificial Intelligence Lab which employed me in the summer of 1973 while I was between high school and college.

> *The PARC facility also is known for the invention of Ethernet, a networking technology that allows high-speed data transmission over coaxial cables. Ethernet has become the standard wired local area network around the world, and it is widely used in businesses and homes. It was honored this year as an IEEE Milestone, a half century after it was born.*
> *Connecting PARC's Alto computers*
>
> *Ethernet's development began in 1973, when Charles P. Thacker—who was working on the design of the Alto computer—envisioned a network that would allow Altos to communicate with each other, as well as with laser printers and with PARC's gateway to the ARPANET. PARC researcher Robert M. Metcalfe, an IEEE Fellow, took on the challenge of creating the technology. Metcalfe soon was joined by computer scientist David Boggs.*
>
> *Metcalfe and Boggs had two criteria: The network had to be fast enough to support their laser printer, and it had to connect hundreds of computers within the same building.*
>
> *The Ethernet design was inspired by the Additive Links On-line Hawaii Area network (ALOHAnet), a radio-based system at the University of Hawaii. Computers transmitted packets, prefaced by the addresses of the recipients, over a shared channel as soon as they had information to send. If two messages collided, the computers that had sent them would wait a random interval and try again.*

As we know, this is exactly the way today's Ethernet operates. The brilliance of Bob's original conception was in its simplicity: Essentially, an Ethernet network is a big party line to which everyone is attached. Anyone who wishes to talk on the line first listens to be sure the line is clear and that no one is currently talking. If so, the party who wishes to talk just does so. But since two waiting parties might start talking at exactly the same time, anyone who is talking also listens to that communal party line to detect any collision of their message with someone else’s.

The abbreviation that’s been given to this bit of brilliance is CSMA/CD which stands for carrier sense/multiple access with collision detection. As the IEEE article noted, when two or more talkers detect that their message had collided with someone else’s, they would each pick a back-off interval at random and wait before trying again.

This is somewhat similar to the way the Internet itself operates, where the guarantees for delivery were almost counter-intuitively softened by design, like the Internet’s deliberate lack of any guarantee that a packet sent would ever reach its destination. But the somewhat surprising result of these approaches was the creation of quite robust networking systems, because the assumption of failure was deliberately designed into the system as part of the solution.

One of the obvious problems with this freewheeling system is congestion. The collision and random retry solution is very clever. And it works terrifically so long as the overhead from collisions and retries does not become too great – since none of that represents a successful use of the bandwidth. As a consequence, the Ethernet does suffer from one fatal flaw known as congestion collapse. Ethernet does not degrade gracefully under too great a load, it collapses as everyone is trying and failing to get their message through without collision. There is, however, one simple solution to this: simply provide more bandwidth... which is what we’ve been doing ever since.

Continuing with what the IEEE wrote, they said:

> *Metcalfe outlined his proposal, then called the Alto Aloha Network, in a now-famous memo to his colleagues. Using coaxial cables rather than radio waves would allow faster transmission of data and limit interference. The cables also meant that users could join or exit the network without having to shut off the entire system. In a 2004 oral history conducted by the IEEE History Center, Bob Metcalfe said:*
>
> *“There was something called a cable television tap, which allows one to tap into a coax without cutting it,” Metcalfe said. “Therefore, [Boggs and I] chose coax as our means of communication. In the memo, I described the principles of operation—very distributed, no central control, and a single piece of ‘ether.’”*
>
> *Metcalfe and Boggs designed the first version of what is now known as Ethernet in 1973. It sent data at up to 2.94 megabits per second and was “fast enough to feed the laser printer and easy to send through the coax,” Metcalfe told the IEEE History Center.*
>
> *A 9.5-millimeter thick and stiff coaxial cable was laid in the middle of a hall in the PARC building. The 500-meter cable had 100 transceiver nodes attached to it with N connectors, known as vampire taps. Each of the taps—small boxes with a hard shell—had two probes that “bit” through the cable’s outer insulation to contact its copper core. Thus new nodes could be added while existing connections were live.*
>
> *Each vampire tap had a D-type connector socket in it, consisting of a plug with nine pins that matched to a socket with nine jacks. The sockets allowed Alto computers, printers, and file servers to attach to the network. To enable the devices to communicate, Metcalfe and Boggs created the first high-speed network interface card (NIC)—a circuit board that is connected to a computer’s motherboard. It included what is now known as an Ethernet port.*

> *The researchers changed the name from the original Alto Aloha Network to Ethernet to make it clearer that the system could support any computer. PARC researcher Alan Kay recalled a comment Thacker had made early on, that "coaxial cable is nothing but captive ether." Metcalfe, Boggs, Thacker, and Butler W. Lampson were granted a U.S. patent in 1978 for their invention. They continued to develop the technology, and seven years later, in 1980, PARC released Ethernet that ran at 10 Mb/s. The update was done in collaboration with researchers at Intel and the Digital Equipment Corp. (DEC) to create a version of Ethernet for broad industry use.*
>
> *Ethernet first became commercially available that year, in 1980, and quickly grew into the industry's Local Area Network (LAN) standard. To provide computer companies with a framework for the technology, in June of 1983 Ethernet was adopted as a standard by the IEEE 802 Local Area Network Standards Committee.*
>
> *Currently, the IEEE 802 family consists of 67 published standards, with 49 projects under development. The committee works with standards agencies worldwide to publish certain IEEE 802 standards as international guidelines.*

Today's Ethernet protocol is carried over twisted-pair, optical, and of course radio media – the WiFi that has mostly replaced wires in any ad hoc setting. The interconnection technology that began 50 years ago with a single long run down the center of the hallway is the technology that is now literally everywhere.