Security Now! #993 - 09-24-24

Kaspersky exits the U.S.

This week on Security Now!

The case of the exploding pagers and walkie-talkies. Are Ford Motor Company autos planning to listen-in to their occupants? Highly personal data of 106,316,633 U.S individuals was found unprotected online. Passkeys takes a huge step forward with native support in Chrome. Is there a serious 9.9-level unauthenticated remote code exploit in Linux? More credit bureau freezing insanity, Drobo vs Synology, GRC's email adventure, WiFi security with and without a VPN, obtaining CPE credits from listening to Security Now, and in defense of Microsoft Defender XDR. Then, what mess did Kaspersky make leaving the U.S. market last week and what are the wider implications for the Internet's future?

What event could have prompted the addition of this sign?

Security News

The case of the exploding pagers and walkie-talkies

The Gold Apollo Rugged Pager AR-924

Gold Apollo Wireless Rechargeable alphanumeric Rugged Pager with Up to 85 Days of Battery Life and Rechargeable battery with USB-C connector.

Last Tuesday, shortly after the news of the exploding pagers broke, I started receiving notes from our listeners saying that they were looking forward to my talking about this today. As always, what mostly interests me and what is also the proper focus of this podcast, is the technology and the facts, to the degree that either are known, behind what happened. This is not a podcast that will examine or comment upon the politics or the morality of what occurred. That's not what we're here for. As I often say in GRC's newsgroups and forums when such hot topics arise, there are ample other places on the Internet for such discussion if that's what one is seeking. But not here.

I first spent some time coming up to speed about what was known. I had the advantage of being able to wait nearly a week for the dust to settle (almost literally) and for the various news reporting and investigative bodies to dig into the backstories and report their findings. I finally found exactly the sort of background and technical coverage that's appropriate for this podcast over on the CryptoMuseum.com site. Here's what they wrote:

> *On 17 September 2024, thousands of pagers of the Lebanese terrorist organization Hezbollah exploded more or less simultaneously. Around 5000 pagers had been obtained by Hezbollah shortly before the incident, 4000 of which exploded that day, after receiving a specially crafted message. In the incident, at least 12 people were killed and around 2750 were injured. A day later, more than 400 handheld radios (walkie-talkies) used by Hezbollah also exploded. Although there was no direct proof, it was widely speculated that Israeli services were behind the attack.*
>
> *The AR-924 pager from the Taiwanese manufacturer Gold Apollo is intended for use on local infrastructure in the 450-470 MHz UHF radio band, and does not depend on the public telephone network.*

Hezbollah used these pagers for security reasons, as they were afraid that their communications via public networks could be intercepted or cut-off.

It seemed that the pagers had been manipulated somewhere in the supply chain between Taiwan and Lebanon, or that a special (fake) company had been set up by an intelligence service to supply manipulated devices to Hezbollah.

Experts believe that Israeli intelligence services managed to manipulate the firmware and added a small (plastic) explosive device. The Taiwanese manufacturer – Gold Apollo – denied that the devices were supplied by them, and suggested that they might have been supplied by Hungarian company BAC Consulting. BAC had purchased the production rights and the use of the brand name for certain regions, and later produced their own pagers under the Apollo brand.

A specially crafted message was sent to the newly purchased devices, which triggered a small plastic explosive device that was hidden inside its enclosure. According to the German newspaper Welt, the explosive RDX had been integrated into the batteries. In addition, the markers that are normally present in plastic explosives to reveal them in an x-ray scan, were said to have been omitted. Other sources report that the explosive known as PETN was used. RDX and PETN are the main ingredients of the plastic explosive Semtex.

According to the Taiwanese manufacturer of the pagers, their Hungarian license holder BAC Consulting could be involved in the rigging of the devices. The company was founded on May 5th, 2022 and reported 2023 annual income of 549,420 EUR. It is possible that it was a 'shell' company, created especially for the purpose of selling rigged equipment to certain parties.

A day after the incident, a representative of the Hungarian president Viktor Orbán, told the press that the pagers had never actually been in Hungary, and that BAC merely acted as an intermediary. When reporters visited the company at its registered address, no BAC representative was available for comment. At the address – a modest office building in the outskirts of Budapest – several other (unrelated) companies were housed, and no one had seen the BAC director since the pager attacks of September 17th. She had reportedly been placed under the protection of the Hungarian security services.

In addition, the Bulgarian authorities started an investigation into a company that they thought might have facilitated the sale of the pagers to Hezbollah. Although the name of that company wasn't disclosed, Bulgarian media revealed it was Northa Global Ltd. in Sofia (Bulgaria).

A day after the incident with the Apollo pagers, on September 18th, a similar thing happened to the two-way handheld radios that were also used by Hezbollah. In this case it involved the IC-V82 handheld radio, a 20 year old model from the Japanese manufacturer ICOM. The IC-V82 works in the VHF amateur radio band, which ranges from 144 to 146 MHz (optionally 136-174 MHz).

The ICOM IC-V82 is a straightforward two-way radio of the kind that are also used by Amateur Radio Operators (HAMs). It was discontinued around 2014, and should no longer be available on the market. ICOM stressed that the devices had not been supplied by them. It is known however, that counterfeit IC-V82 radios (i.e. not manufactured by ICOM) are widely available.

Counterfeit radios are commonly produced in China and are difficult to distinguish from real ones. They are available from electronics stores in Asia and come in 'original' packaging.

In the case of the exploding IC-V82's it was not the battery that exploded, but they front top. Apparently an explosive device had been placed inside the radio, close to the microphone/ speaker, which is the part that is closest to the face when the radio is operated. This suggests that it was the intention to cause maximum – potentially fatal – harm to the user.

In Bulgaria, an investigation has been launched into a company in Sofia, that might have been involved in the supply of counterfeit IC-V82 radios from Asia to Hezbollah. This is the same company – Northa Global Ltd. – that might have been involved in supplying the AR-924 pagers.

The number of radios (~450) is smaller than the number of exploded pagers (~4000), but since the radios are physically larger, they carried more explosives and were therefore more damaging. It is currently unclear how and when the handheld radios were manipulated and how they were triggered remotely, but we can make a few educated guesses. The radio features CTCSS and DTCS — two techniques to selectively open the radio's noise canceling "squelch" system using analog or digital tones. It is also possible to fit an optional DTMF ("Touchtone") coder/decoder which can be used to activate the pager function of the device, by sending it a 3-digit DTMF digit sequence user ID. It is likely that a unique combination of the above techniques was used to trigger their synchronized detonation.

https://www.cryptomuseum.com/covert/cases/pager/

So, we have an example of a seriously well planned, well coordinated, and breathtaking real world physical supply chain attack. The article said authoritatively, and I've seen it in several places, that the 5,000 pagers had been recently ordered and received. There's been no exact reporting of the elapsed time between the 5,000-pager order and their delivery, but if Israel was somehow able to do this without extensive pre-order preparation then it's even more impressive. Given the evidence of this attack's sophistication, and what we know of the time that would be required to implement and test a fully functional pager incorporating specialized firmware with secret code recognition to trigger a custom detonator, probably along with an additional power transistor to supply the current for the detonator, which would require a custom circuit board, there's no way this could have been done overnight. If it were, it would be quite astonishing.

The Gold Apollo SR-924 is a ruggedized device with a rechargeable 85-day battery life. As such, it's particularly well-suited for rough use in the field. I suspect it's more likely that Hezbollah's choice of pager was known ahead of time since this pager model has been available for years. That would have given someone, presumably someone with ties to Israel, time to replace the original guts of thousands of these devices with their own. At which point they would have been standing by and patiently waiting for Hezbollah to place their order. And the same must have been true for the next day's handheld radio attack.

This is another of those situations where we're unlikely to ever have all of the facts, since those who have all the facts only stand to lose if more becomes known.

In some other reporting by Vox, Charles Lister, senior fellow at the Middle East Institute was quoted, saying:

> *"What we have seen over the past two months shows that Israel and its intelligence apparatus have completely infiltrated the most sensitive echelons of the entire Axis of Resistance."*

Charles' reference to the Axis of Resistance is the informal name for Iran's network of proxy militias throughout the Middle East. He continued:

> *"It was only a year ago that the reputation of Israel's intelligence services took a major hit with the failure to anticipate the October 7th attacks, despite abundant signs that Hamas was preparing for a major operation. It's worth noting that while the operations in Lebanon and Iran were likely carried out by Mossad, Israel's foreign intelligence service, Israeli-occupied Gaza is the responsibility of the Shin Bet, the domestic security service.*
>
> *The Shin Bet official responsible for Southern Israel and Gaza resigned over that failure, as have two senior military intelligence officials. While October 7th damaged the reputation of Israel's vaunted spy services, they have now restored that notion of deterrence based on fear and the notion that Israel has eyes everywhere."*

I've left a link in the show notes to this page at www.cryptomuseum.com for anyone who's interested in learning more, though that's pretty much everything that they had to report.

"Ford seeks patent for tech that listens to driver conversations to serve ads"

The Record published a piece two weeks ago that I didn't have the chance to get into until now. But it's too important for us to miss in this podcast. The Record's headline makes it very clear where we're headed, reading "Ford seeks patent for tech that listens to driver conversations to serve ads". You heard me right. Ford Motor Company wants to listen in on the conversations being held inside the car in order to present advertisements on the system's entertainment system. The Record writes:

> *Ford Motor Company is seeking a patent for technology that would allow it to tailor in-car advertising by listening to conversations among vehicle occupants, as well as by analyzing a car's historical location and other data, according to a patent application published late last month. The patent application says: "In one example, the controller may monitor user dialogue to detect when individuals are in a conversation. The conversations can be parsed for keywords or phrases that may indicate where the occupants are traveling to."*
>
> *The tech — labeled as "in-vehicle advertisement presentation" — will determine where a car is located, how fast it is traveling, what type of road it is driving on and whether it is in traffic. It also will predict routes, speeds and destinations to customize ads to drivers, the application said.*
>
> *The system could pull data from "audio signals within the vehicle and/or historical user data, selecting a number of the advertisements to present to the user during the trip."*

By monitoring dialogue between vehicle occupants the ad controller system can determine when to deliver audio versus visual ads, providing ads to drivers as they travel "through a human-machine interface (HMI) of the vehicle," the patent application said.

So, okay... hold on a second. The ads can be audio? So, what, your car interrupts during a pause in the conversation to helpfully comment with something like: *"Excuse me, but I heard you mention that you were hungry. And we know from your past travels that you like burgers. There happens to be a highly-rated burger joint just around the corner. If you're interested, take a left at the signal after the next one."* If that's the case, I doubt that I'm ready for this brave new world. The article continues:

"Such systems and methods provide maximum opportunity for ad-based monetization," the patent application said. "These systems and methods may use knowledge of vehicle destination prediction to provide more relevant advertisements, for example, if a user is going grocery shopping, merchandise purchasing, etc."

The patent application does not describe how the collected data would be protected. The technology would be primarily software-based and would require no new hardware, according to the application. Ford filed the application in February and it was published on August 29th. Contents of the application were first reported by Motor1.com.

Ford has since defended the patent application with a Ford spokesperson saying: "Submitting patent applications is a normal part of any strong business as the process protects new ideas and helps us build a robust portfolio of intellectual property."

That's certainly true. Many patents are defensive and are primarily meant to beef up a portfolio for mutual agreements among competing manufacturers within an industry. Ford's statement continued, stating:

"The ideas described within a patent application should not be viewed as an indication of our business or product plans." And in a followup statement, Ford said it "will always put the customer first in the decision-making behind the development and marketing of new products and services."

Uh huh, let's hope.

The system also could cull data from third-party applications or set up screen input preferences to predict the number of ads a driver should be served. [How about zero.]

The types of trips being made by drivers also will play a role, the application said, noting that whether a vehicle owner is making a "long drive versus trip to medical care facility" would be considered by the system.

That's right... because what I really want is my car reporting to my insurance company that I've been spending a lot of time at medical facilities. And speaking of "tattle tales" ...

A Ford patent filed in July proposed technology that would enable vehicles to monitor the speed of nearby cars, photograph them and send the information to police. Not surprisingly, the idea sparked a backlash from privacy advocates but that's of no concern to the U.S. Patent and Trademark Office. That application pointed to how difficult it is for police to pinpoint speeding cars and said *"it is desirable to provide systems and methods that assist traffic police and/or other law enforcement officers perform such tasks."* And let's not forget that Ford quietly backed away from another controversial patent application last October after a firestorm of criticism over its plans for a system that would commandeer vehicles whose owners were late to pay and allow the cars to repossess themselves.

That patent application said that the technology would allow self-driving cars to automatically head to repossession lots while standard vehicle lenders would be able to permanently lock cars and cripple steering wheels, brakes and air conditioning in order to pressure delinquent drivers to pay. You have to really wonder what they're thinking. If nothing else, the communications available thanks to the Internet means that if this happened just once to someone, it would make headlines and Ford's sales would crash overnight.

I want to reiterate and reinforce, though, what that Ford spokesperson said about patents not necessarily implying future product plans. That's really true. While patents certainly can indicate a company's future direction, they do not necessarily do so. For a massive company like Ford, that has an entire division of in-house patent attorneys, their job is to emit patents more or less continuously. So they'll have members of their patent squad regularly attending product planning and brainstorming meetings, taking notes and turning random comments into patents.

Some random employee may have quipped at some point during a brainstorming meeting that once they've got the self-driving technology figured out, it **would** be possible to eliminate the need for tow-truck repossession by having their cars start themselves up in the middle of the night and drive themselves to the local repo lot. While everyone was laughing at that idea, the weenie from the patent department was taking notes to get that idea captured and filed.

Another large chunk of personal data exposed

Just when you thought it might be safe to unfreeze your credit reporting... Okay, I'm joking. I know you know that it will never again be safe for you to unfreeze your credit reporting. That ship has sailed. And following the National Public Data breach, it's difficult to imagine that anything could be worse. And I don't know that yesterday's news is worse because there's no evidence that bad guys got their hands on this latest treasure trove of data. But it was publicly exposed, unencrypted and unprotected for some length of time.

Yesterday, Cybernews headline was: "One-third of the US population's background info is now public" Cybernews wrote:

> *MC2 Data and similar companies run public records and background check services. These services gather, compile, and analyze data from a wide range of public sources, including criminal records, employment history, family data, and contact details. They use this information to create comprehensive profiles that employers, landlords, and others rely on for decision-making and risk management.*
>
> *Websites that MC2 Data operates include: PrivateRecords.net, PrivateReports, PeopleSearcher, ThePeopleSearchers and PeopleSearchUSA.*

Despite dealing with staggering amounts of sensitive data, it is not always kept secure. Cybernews research reveals that the company left a database with 2.2TB of people's data passwordless and easily accessible to anyone on the internet. What was likely to be a human error exposed 106,316,633 individual records containing private information about US citizens, raising serious concerns about privacy and safety. Estimates suggest that at least 100 million individuals were affected by this massive data leak.

The people and organizations using MC2's background check service have also been exposed, as the data of 2,319,873 users who subscribed to MC2 Data services was leaked.

The leaked data included: Names, Email, IP addresses, User agents, Encrypted passwords, Partial payment information, Home addresses, Dates of birth, Phone numbers, Property records, Legal records, Family, relatives, neighbors data and Employment history.

I looked over the data and I didn't see any reference to social security numbers. But there's plenty of personal data that goes far beyond what the NPD breach offered. And this is the problem we keep seeing with so-called "Big Data" — this latest MC2 leak data could be merged with the NPD breach data to create a single even more powerful database.

Passkeys takes a big step forward: Now supported by Chrome.
Yep. This is significant. Last Thursday Google Chrome's product manager blogged under a headline that under-hyped this announcement: *"Sync passkeys securely across your devices"* That really doesn't say what I would think Google should be saying, because we're talking about having the world's leading web browser – by a large margin – and presumably other Chromium-based browsers too, now natively supporting Passkeys. Here's what Google's posted:

In addition to Android devices, you can now save passkeys to Google Password Manager on desktop.

Signing into your favorite sites and apps on any device should be as quick and easy as unlocking your phone. That's where passkeys come in. They're safer than passwords and easier to use, letting you use your fingerprint, face, or screen lock to securely sign in to apps and websites — moving us one step closer to a passwordless future.

Up until now, you could only save passkeys to Google Password Manager on Android. You could use them on other devices, but you'd need to scan a QR code using your Android device. Today, we're rolling out updates that make it even easier to use passkeys across your devices. You can now save passkeys to Google Password Manager from Windows, macOS, Linux and Android, and under ChromeOS which currently available for testing in Beta. Once saved, they'll automatically sync across your devices, making signing in as easy as scanning your fingerprint.

To let you create passkeys and access saved ones across your devices, we're introducing a new Google Password Manager PIN. This PIN adds an additional layer of security to ensure your passkeys are end-to-end encrypted and can't be accessed by anyone, not even Google. When you start using passkeys on a new device, you'll need to know either your Google Password Manager PIN, or the screen lock for your Android device. These recovery factors will allow you to securely access your saved passkeys and sync new ones across your computers and Android devices. You can set up a six-digit PIN by default, or select "PIN options" to create

a longer alpha-numeric PIN.

You can already create passkeys for popular sites and apps, such as Google, Amazon, PayPal and WhatsApp. And since Google Password Manager is conveniently built into Chrome and Android devices, you can get started today, without having to download any additional apps.

The "started today" is a link to: https://passwords.google/ So open Chrome and head to "passwords.google" to enable, configure and start using Chrome's built-in passkeys solution.

A nascent 9.9 Linux Unauthenticated RCE?

News of what appears to be a potentially serious (as in 9.9) Linux unauthenticated remote code execution vulnerability just broke. It was sent to me this morning by a listener of ours, Alessandro Riccardi. Thank you, Alessandro. The researcher is not someone we've encountered before, so I spent some time doing a bit of background checking and he's clearly the real deal. His name is Simone Margaritelli. He's based in Rome, Italy and uses the handle "evilsocket". He has a presence on Linked-In with more than 500 connections with many projects under his evilsocket handle on GitHub. His Twitter handle is, of course, @evilsocket and since 2009 he's posted more than 15 thousand times and has accumulated more than 42 thousand followers. His site is https://www.evilsocket.net/ and he uses the glider from Conway's Game Of Life as his icon. Looking over his five pages of projects indexed on his site, although he's been somewhat less prolific the past few years, as I said, this guy is very clearly the real deal.

I went to the trouble of doing this bit of vetting because of the potential significance of the claims he's making in his still-not-public responsible disclosure. He's what he just posted, and why it might matter, yesterday. He leads with six bullet points:

- *Unauthenticated RCE vs all GNU/Linux systems (plus others) disclosed 3 weeks ago.*
- *Full disclosure happening in less than 2 weeks (as agreed with devs).*
- *Still no CVE assigned (there should be at least 3, possibly 4, ideally 6).*
- *Still no working fix.*
- *Canonical, RedHat and others have confirmed the severity, a 9.9, check screenshot.*
- *Devs are still arguing about whether or not some of the issues have a security impact.*

I've spent the last 3 weeks of my sabbatical working full time on this research, reporting, coordination and so on with the sole purpose of helping and pretty much only got patronized because the devs just can't accept that their code is crap - responsible disclosure: no more.

The writeup is gonna be fun, not just for the technical details of it, not just because this RCE was there for more than a decade, but as a freaking example on how NOT to handle disclosures.

Like, I write software, I get it, I get how someone can be defensive about the stuff they write, I really do. But holy sh, if your software has been running on everything for the last 20 years, you have a freaking responsibility to own and fix your bugs instead of using your energies to explain to the poor bastard that reported them how wrong he is, even tho he's literally giving you PoC after PoC and systematically proving your assumptions about your own software wrong at every comment. This is just insane.

*Just wanted to add for the sake of clarity, that i have *so much respect* for the people at Canonical that have been trying to help & mediate from the beginning, I really don't know how they manage to keep their cool like this.*

This is going to be the writeup opening statement. It's an actual comment from the github conversation. I mean, it's not wrong ...

And YES: I LOVE hyping the sh1t out of this stuff because apparently sensationalism is the only language that forces these people to fix.

At this point we don't know more. We do know that any unauthenticated RCE requires something to be listening on the Linux end and accepting packets. It's impossible to say more than that without more information. So we don't know, for instance, what percentage of Linux systems might be vulnerable, nor if not all, why not. The fact that there's some controversy about this with some distro devs apparently disagreeing should give us pause and should tamp down any panic. Perhaps the exploitation of this requires the moon to be in a certain phase. We just don't know.

Annoyingly, his Twitter feed is locked so I've been unable to view the various clues he's dropped. However, I've been able to view the comments and reactions to his postings made by people whose feed is not locked, and there are things such as:

- *Probably and luckily the first to point it out publicly, but not the first that exploited it. It's sad.*
- *Please don't disclose on a Friday. Preferably on Tuesday I like my weekend :-)*
- *Please don't rush this! "All Linux systems" is a gigantic and diverse attack surface and the vulnerability sounds trivial in hindsight, making it almost impossible to fix without telling the world about it.*
- *Any observed active exploitation ? A vuln impacting all linux distros with a low attack complexity going unnoticed for a decade is highly unlikely*
- *Seen both sides of this...working on some unrelated disclosures at the moment, but it's taking a LONG time to keep all sides happy...thankfully other times, fixes and CVE's have been confirmed in the blink of an eye, don't let one bad one put you off :)*

- *Also, all Linux systems and others? Does that mean android and bsd?*
  - *Reply: Says elsewhere in the thread BSD is included*
- *Not to piss anyone off, but I have seen far too many high CVE that just turn out to be fringe or "the devs don't agree with me so they are dumb"*

I've put in my request to follow him. If he accepts that request I'll be able to see more of what he's shown to his followers. And in two weeks we'll apparently know more. Either way, this will be interesting. Stay tuned! https://threadreaderapp.com/thread/1838169889330135132.html

Closing the Loop

Stephane

*Hi Steve, I just wanted to post some feedback in regards to credit freeze. I'm not sure why, but credit bureaus need to be forced by law by local government (provincial here in Canada) to allow us to freeze our credit. I tried in Ontario and there is no way for me at the moment. Under the previous party they had started trying to implement it. But since we changed from liberal to conservative this law is now in limbo. Could you share this feedback to have your listeners contact their local provincial MP to try and force the change. Or if anyone knows where I could go to force the credit bureaus to change this without being forced by law that would be great! It is **my** credit. I should not be held hostage by the credit bureaus. Thanks Stephane*

I'm glad I'm in the United States, where this long fought battle has finally given its citizens not only the ability to request their credit to be frozen, but also for that to finally be free of charge. I hadn't stopped to consider the situation for our Canadian listeners, so I was glad for Stephane's feedback. We know that the credit bureaus went kicking and screaming in the U.S., fighting these changes all the way. And massive breaches, such as the National Public Data breach which have openly exposed everyone's personal data to make identity theft so much more practical must have helped to further demonstrate the need for the system to change even further. As I've noted before, credit queries should be locked by default and selectively opened by the individual who is requesting to have their creditworthiness verified. We're not there yet in the U.S. and from Stephane's feedback it appears that Canada has even further to go.

And while we're on the topic of credit bureaus...

Steve & Leo,

I'm a software engineer in the fintech industry and have been an avid listener of Security Now since I started my programming career in 2005. Thanks to the podcast, I've had a frozen credit report ever since the topic was first introduced. After the National Public Data breach, I persuaded my girlfriend to freeze her credit as well, but we encountered a horrifying issue.

When we created a new account for her on Experian and logged in, we discovered that her newly created account was linked to someone else's profile! That's right—we had full access to another customer's credit history.

The sign-up process requires your first and last name, some address details, and part of your social security number. However, Experian seemed to match only the first three letters of my girlfriend's first name and the last four digits of her social security number. This caused her account to be matched with another woman who had a similar first name (though spelled differently by four characters), the same last four SSN digits, and lived in the same state (Michigan). But aside from these details, everything else was different—different last name, different previous addresses, and so on.

After hours of frustrating calls with Experian support, where several agents insisted this wasn't possible, we could still view the other woman's entire credit profile. Eventually, Experian reset my girlfriend's account, and on the second attempt, the sign-up process completed correctly

with the right information.

Thank you & Leo for all the incredibly valuable knowledge you have provided me over the years. I was an early Astaro adopter if that helps date how long I've been listening. Thank you!

Wow. What a mess. I suppose the use of only a few characters of the person's name might make sense if matching against spelling variations were a problem. But what could be the possible reason for not matching against the individual's entire social security number? The user needs to know it and the credit bureau obviously knows it. So why not require a complete match? Are they afraid that the user cannot enter the entire thing correctly? I'm at a loss to understand what twisted numbskull logic could suggest that only providing "the last four" of the social security number could make any sense? Makes ya wonder.

Nile Davis

Hello Steve, I've been a loyal listener since #1 and I love that you are going beyond 999! I have a Drobo 5N that I got many years ago after hearing that you had one too. It seems to still work great. I took my drives out and reran Spinrite 6.1 on each of them without a hitch. I got a Synology DS1522+ a year ago and love it. I know that with Drobo being out of business, the question that I have is this: Should I still trust my Drobo (that is upgraded to the latest firmware) or should I just ditch it and get another Synology? Thanks for all you and Leo do! Take care, Nile.

I'm in a very similar situation as Nile. My first experience with consumer grade NAS was the Drobo 5N. Since it was working well, when my wife and I set up a second nest for ourselves seven years ago, I purchased another identical Drobo 5N for that location. Then, my original Drobo 5N died. It had given me many years of service, but something went South. I tried another power supply, swapping drives and doing everything I could think of, but it refused to behave. I'd been hearing about Synology and we knew that Drobo would on the chopping block. So even though I could still have obtained a replacement Drobo 5N from the supply chain, I decided to switch to Synology. And all I can say about that is that I have never been happier.

The Drobo was fine for a non-power user who's happy with fewer options. But that's not me. After I set up my four-drive Synology to replace the original Drobo 5N, I purchased another identical Synology for my second location. So now that location has the original second Drobo 5N and a Synology.

My wife, who has a lot of letters after her name, some of which are PhD, has her doctorate in applied psychophysiology. Seven years ago she asked me whether there was any way we could set up her clients with a laptop and a two-channel EEG amplifier to facilitate "at home" neuro-feedback training. As with all forms of real-time biofeedback, neurofeedback is the process of showing a client some aspect of their brain's function that would be better if it were changed and, amazingly, it's possible to effect such change just by showing them what's wrong. So I found a fantastic two-channel EEG amplifier from Bulgaria, and we purchased a fleet of inexpensive recycled Dell laptops from Amazon.

I'm sharing this backstory because all of those widely distributed laptops are running instances of SyncThing which are sync'd to that second Drobo 5N which is still going strong and is being used to keep all of the therapy that those laptops are doing synchronized with homebase. The system works perfectly.

Nile asked: "*Should I still trust my Drobo or should I just ditch it and get another Synology?*" I'm still trusting that original Drobo 5N and I'm hoping it continues purring away until my wife decides she's no longer going to offer this form of remote therapy. If that second Drobo also throws in the towel while its laptop synchronization services are still required, I'll move its synchronization functions over to the Synology. But if I never need to do that, that would be my first choice. If my wife retires from offering remote neurofeedback therapy before the Drobo retires itself, that would be great.

So my feeling is, keep the Drobo as long as it's running and as long as it does what you want. But given my experience with Synology, that's what I would recommend without hesitation to anyone.

Dan in sunny Scotland

FYI, last week's Security Now email was routed to my Junk folder. I'm using Apple Mail (I have my own domain set up on iCloud). It was fine until last week, so I guess something must have spooked their filters. In any case, I marked it as 'not spam'. Hopefully their filters will get the message, so to speak! All the best from sunny Scotland, Dan

Last week I asked any of our listeners who discovered their weekly Security Now! email going to spam to please mark it "not spam". Many listeners like Dan noted that they had done so. So I wanted to thank everyone for that.

What I've learned so far through this mailing adventure is that just as with code signing, the "earned reputation" of the signer is everything. GRC has been using email for our business decades and has enjoyed a spotless reputation – since we never have and obviously never would actually send spam. But GRC's reputation is being challenged at the moment because for the past several weeks I've been slowly sending out email to GRC's past SpinRite 6.0 purchasers to notify them that v6.1 can be theirs at no cost. And I suppose from that standpoint that it would technically be classified as UCE – Unsolicited Commercial Email. Except that I'm trying to give away an upgrade that I and many others spent three and a half years working to create.

But it's not email from a Nigerian prince and every email address I'm using is what SpinRite's purchaser used at the time to receive a purchase receipt from us.

However, I haven't bothered any of those people until now, and those addresses date back as far as 2004. There are addresses with CompuServe account numbers in the list. I've been mailing in reverse order, from most recent toward least recent, and having now progressed as far back as 2008, more than 10% of the addresses are bouncing. Overall, it's going better than I had hoped.

But when a major ISP like Apple or Google or Microsoft sees grc.com sending to many non-existent addresses, they will quite reasonably decide not to bother their current users, and to route any valid messages originating from the same domain into their users' spam or junk folders.

There's nothing I can do about it, but fortunately it's a one-time transient problem which we should be on the other side of in a few weeks. Once that's happened I'll have a much smaller, updated and clean list that I'll be able to use going forward without trouble. Until then, I need to ask for your patience. It would help greatly if anyone who discovers their weekly Security Now! email in their spam or junk folder would mark it as "not spam" – that's a very effective way of training the spam filters that GRC is not and never has sent out spam... even if it is attempting to contact some of its very old purchasers.

Steve P.

Hi Steve, I'd appreciate your latest thinking on the safety, or otherwise, of connecting to public WiFi. I'm currently 'enjoying' an extended stay in hospital, and as with most public places here in the UK, they're offering 'free WiFi'. However, unlike most, the network here does NOT require a password to connect - you get briefly taken to a portal, and then granted internet access.

I seem to remember long ago you touching on this subject on Security Now, but I'm uncertain if this type of public WiFi network with no password is a 'risk too far'. I'm using an iPhone and iPad here, typically via the Personal Hotspot on the iPhone, but this can by restrictive. So I'd like to use the faster free WiFi offered here - but only if it's safe. I've briefly connected to the free network, but I'm still uneasy about this.

I'm also using a VPN (ExpressVPN) to connect. If it's generally a bad idea to connect to public WiFi with no password, does a VPN mitigate the risks somewhat? The ceiling-mounted WiFi APs appear to be branded Cisco, but of course I have no way of knowing how this is set up in the background, e.g. client isolation?

Anyway, thanks for all you do (6.1 continues to work very well, of course!).

Regards, Steve P. (currently an in-patient in St. Thomas' Hospital, London - although hopefully not for much longer!).

The short version is that the use of any high-quality VPN system, such as Express VPN, completely encrypts all traffic inside of the VPN's tunnel. It is only decrypted as it emerges onto the Internet at the VPN provider's servers. There is no better or more complete protection available for shielding one's traffic as it passes through a WiFi hotspot, whether open or password protected.

The big upside to the use of a VPN provider is the convenience of being able to use their always present server. The only downside to the use of any big provider is that once the tunneled traffic emerges onto the public Internet, it's visible to everyone. And there's always been speculation that such places are where national intelligence services might be sniffing around since overall it could be expected that traffic emerging or going into a VPN service might be more interesting than just random packets on the Internet.

So the one possible improvement would be to run one's own VPN server at home or office. In that case, not being any big and well known VPN service, there would be less chance of generic traffic capture. On the other hand, if someone was interested in your traffic specifically, that's where they would look.

And for the sake of completeness, what about the case of no VPN whatsoever in an open public WiFi hotspot? Things are definitely 100% better these days than they were back in the earlier days of this podcast #272, recorded October 27th, 2010, titled "Firesheep". 14 years ago, the simple unencrypted HTTP protocol was still dominant and connections typically only switched to HTTPS when credentials were being exchanged. But these days, 14 years later, all connections are always encrypted. This makes it far safer to use an open public WiFi hotspot without a VPN than it once was. It's true that DNS queries are probably not being encrypted, so it would be possible for someone to eavesdrop on your DNS lookups. But the IP addresses you're visiting could also not be hidden, even if what you do there would be.

So I suppose I'd say that today, in a pinch, using open WiFi is not high risk though it's not ultra private and if you have access to a VPN or overlay network there's no better time to use it.

Richard Anthony, CISSP

Steve, Those of us who use Security Now for CPE credits for certs like CISSP and CEH need to post proof when we submit credits. Many of us grab a screenshot at the end of a video podcast for proof (we use the end of the video to show that we've watched the whole thing.) I've been doing this for many years now. I do this on my ipad and show the date/time I watched along with the episode number. Would there be any way for Leo or his team to show the episode number on the screen during the last few minutes of the podcast? It would be a terrific help to all those of us who reply upon Security Now to maintain our certifications. Many thanks, Richard Anthony, CISSP

I have no idea whether that could be done, but Leo and his team have just heard the idea.

And from another listener, Richard Cornell, this one an IT Security Manager in the UK

Hi Steve. A few times in recent SN episodes you have referred to Windows Defender when discussing CrowdStrike. You are correct in saying the free Windows Defender product is nowhere near as feature rich as the alternative enterprise products, however, if you purchase a Microsoft 365 enterprise license such as M365 E5 you get Microsoft Defender XDR which is every bit as capable as CrowdStrike and the alternatives. Like all these products, it's not perfect but we have used it for a number of years and it is just as good with the advantage that it's part of the integrated Microsoft stack. Keep up the good work and onwards to 999 and beyond!

Thank you, Richard. I appreciate hearing from someone who has experience with Microsoft's high-end enterprise solutions. And as a user of the simple free Windows Defender, I'll certainly admit to a bias toward native solutions.

Kaspersky exits the U.S.

I started off treating today's main topic as just another news item to which I had given the title: **How to mishandle an A/V handoff.** And I'm going to still start with that, because what transpired last Thursday is still news. But this is also the perfect segue for addressing the much bigger and broader issue of what it means that Kaspersky has been kicked out of the U.S. and what this and similar moves mean for our future global technology landscape.

So let's start with BleepingComputer's headline, which was: *"Kaspersky deletes itself, installs UltraAV antivirus without warning"*. Ask yourself what you would think if something completely new and totally unknown suddenly appeared in your computer. And when you went to check on it using the A/V system you had purchased and installed... that A/V solution was nowhere to be found! Talk about mishandling a transition. Here's what BleepingComputer reported:

Starting Thursday, Russian cybersecurity company Kaspersky deleted its anti-malware software from customers' computers across the United States, automatically replacing it with UltraAV's antivirus solution. This comes after Kaspersky decided to shut down its U.S. operations and lay off U.S.-based employees in response to the U.S. government, in June, adding Kaspersky to the Entity List, a catalog of <quote> "foreign individuals, companies, and organizations deemed a national security concern."

On June 20, citing potential national security risks, the Biden administration announced a ban on sales and software updates for Kaspersky A/V software in the United States beginning September 29, 2024.

In July, Kaspersky told BleepingComputer that it would begin closing its business and lay off the staff on July 20 because of the sales and distribution ban. In early September, Kaspersky also emailed customers, assuring them they would continue receiving "reliable cybersecurity protection" from UltraAV (owned by Pango Group) after Kaspersky stopped selling software and updates for U.S. customers. However, those emails failed to inform users that Kaspersky's products would be abruptly deleted from their computers and replaced with UltraAV without warning. According to many online customer reports, including BleepingComputer's forums, UltraAV's software was installed on their computers without any prior notification, with many concerned that their devices had been infected with malware.

One user write: "I woke up and saw this new antivirus system on my desktop and I tried opening Kaspersky but it was gone. So I had to look up what happened because I was literally having a mini heart attack that my desktop somehow had a virus which had somehow uninstalled Kaspersky."

To make things worse, while some users could uninstall UltraAV using the software's uninstaller, those who tried removing it using uninstall apps saw it reinstalled after a reboot, causing further concerns about a potential malware infection. Some also found UltraVPN installed, likely because they had a Kaspersky VPN subscription.

Not much is known about UltraAV besides being part of Pango Group, which controls multiple VPN brands (e.g., Hotspot Shield, UltraVPN, and Betternet) and Comparitech (a VPN software review website).

And... ya gotta love that one. This Pango Group controls multiple VPN brands and also runs their own VPN software review site because why wouldn't anyone go to a site that also publishes multiple VPNs to obtain an objective overview of all available solutions? Apparently even they cannot decide which VPN is better so they publish three themselves.

> *For its part, UltraAV says on its official website, on a page dedicated to this forced transition from Kaspersky's software: "If you are a paying Kaspersky customer, when the transition is complete UltraAV protection will be active on your device and you will be able to leverage all of the additional premium features. On September 30th, 2024 Kaspersky will no longer be able to support or provide product updates to your service. This puts you at substantial risk for cybercrime."*
>
> *A Kaspersky employee also shared an official statement on the company's official forums regarding the forced switch to UltraAV, saying that it "partnered with antivirus provider UltraAV to ensure continued protection for US-based customers that will no longer have access to Kaspersky's protections. Kaspersky has additionally partnered with UltraAV to make the transition to their product as seamless as possible, which is why on 9/19, U.S. Kaspersky antivirus customers received a software update facilitating the transition to UltraAV. This update ensured that users would not experience a gap in protection upon Kaspersky's exit from the market."*

Okay. Now anyone would take issue with the use of the term "facilitate." This wasn't a facilitation, this was an abrupt and unsupervised "switcheroo". I suppose they felt they were covered by sending that email notification in advance. And I didn't see that email. It may have said, in the fine print, that if you did not want to have your A/V and VPN services switched from Kaspersky to the Pango Group you could terminate your subscriptions first.

What's clear is that for something as important as a system's A/V, users should have been in the loop. A user interface should have popped-up explaining that today was the day that Kaspersky was going to be uninstalled and then giving the user the **option** of replacing it with UltraAV **=or=** uninstalling Kaspersky without replacement. I would bet that didn't happen because Kaspersky almost certainly made a bunch of money selling their entire paying A/V and VPN subscriber base to this Pango Group. So no one wanted to give anyone a button they could push to say "No thanks" and opt-out of a continuing paying subscriber relationship with UltraAV and UltraVPN.

Note that a continuing subscription relationship with these entities implies that Kaspersky also transferred their entire U.S. subscriber database – with all billing information – to these Pango Group owned UltraAV and UltraVPN companies.

No one thinks this is ideal. But Kaspersky's behavior was at least understandable under the circumstances. I can't recall a time that there wasn't a Kaspersky. Consider the beginning of Wikipedia's article about them:

> *Kaspersky Lab is a Russian multinational cybersecurity and anti-virus provider headquartered in Moscow, Russia, and operated by a holding company in the United Kingdom. It was founded in 1997 by Eugene Kaspersky, Natalya Kaspersky and Alexey De-Monderik. Kaspersky Lab develops and sells antivirus, internet security, password management, endpoint security, and other cybersecurity products and services.*

Kaspersky expanded abroad from 2005 to 2010 and grew to $704 million in annual revenues by 2020, an 8% increase 2016, though annual revenues were down 8% in North America due to US government security concerns. As of 2016, the software has about 400 million users and has the largest market-share of cybersecurity software vendors in Europe. Kaspersky Lab ranks fourth in the global ranking of antivirus vendors by revenue. It was the first Russian company to be included into the rating of the world's leading software companies, called the Software Top 100. Kaspersky Lab is ranked 4th in the Endpoint Security segment according to IDC data. According to Gartner, Kaspersky Lab is currently the 3rd largest vendor of consumer IT security software worldwide and the 5th largest vendor of Enterprise Endpoint Protection. In 2012 Kaspersky Lab was named a "Leader" in the Gartner Magic Quadrant for Endpoint Protection Platforms.

And so, not only with no evidence of any wrongdoing, but despite the fact that Kaspersky's presence in the cybersecurity world has been nothing but a benefit, their business has been summarily ejected from the U.S. only because they share a country of origin with Putin. Consider this:

- In 2010, Kaspersky Lab worked with Microsoft to counteract the Stuxnet worm, which had infected 14 industrial locations in Iran using four zero-day vulnerabilities in Microsoft Windows.

- In May 2012, Kaspersky Lab identified the malware Flame, which a researcher described as potentially "the most sophisticated cyber weapon yet unleashed".[107] According to the researchers in Kaspersky Lab, the malware had infected an estimated 1,000 to 5,000 machines worldwide

- In January 2013, Kaspersky discovered the Red October malware, which had been used for widespread cyber-espionage for five years. It targeted political targets like embassies, nuclear sites, mostly in Europe, Switzerland and North America. The malware was likely written by Russian-speaking hackers and the exploits by Chinese hackers.

- In February 2014, Kaspersky identified the malware Mask, which infected 380 organizations in 31 countries. Many organizations that were affected were in Morocco. Some of the files were in Spanish and the group is believed to be a state conducting espionage, but Kaspersky did not speculate on which country may have developed it.

- In November 2014, Symantec and Kaspersky authored papers that contained the first disclosure of malicious software named Regin. According to Kaspersky, Regin is similar to QWERTY, a malware program discovered the next year. Regin was used to take remote control of a computer and is believed to have originated from the Five Eyes alliance.

- In 2015, Kaspersky identified a highly sophisticated threat actor that it called "The Equation Group". The group incorporated sophisticated spying software into the firmware of hard drives at banks, government agencies, nuclear researchers and military facilities, in countries that are frequent targets of US intelligence efforts. It is suspected to have been developed by the National Security Agency (NSA) and included many unique technical achievements to better avoid detection.

- In June 2015, Kaspersky reported that its own network had been infiltrated by government-sponsored malware. Evidence suggested the malware was created by the same developers as Duqu and Stuxnet, in order to get intelligence that would help them better avoid detection by Kaspersky in the future. Kaspersky called it Duqu 2.0.

- Also in June 2015, Kaspersky Lab and Citizen Lab both independently discovered software developed by Hacking Team and used by 60 governments around the world to covertly record data from the mobile phones of their citizens. The software gave police enforcement a "menu of features" to access emails, text messages, keystrokes, call history and other data.

- In 2016, Kaspersky discovered a zero day vulnerability in Microsoft Silverlight. Kaspersky identified a string of code often used by exploits created by the suspected author. It then used YARA rules on its network of Kaspersky software users to find that string of code and uncover the rest of the exploit. Afterwards, Microsoft issued a "critical" software patch to protect its software from the vulnerability.

- In 2016, Kaspersky uncovered the Poseidon Group, which would infiltrate corporations with malware using phishing emails, then get hired by the same company as a security firm to correct the problem. Once hired, Poseidon would install additional malware and backdoors. In June 2016 Kaspersky helped uncover a Russian hacking group, leading to 50 arrests.

... and on and on and on. So not exactly a blight on the cybersecurity landscape.

Thus, it's no surprise that so many people have trusted Kaspersky's anti-malware solutions through the years – actually for decades – and this was driven by high-quality independent reviews that found Kaspersky's solutions to consistently rank among the best. Kaspersky earned and deserves the trust they've enjoyed. And at no point have they done anything that would call that into question. As I noted earlier, the world is better and more secure for having Kaspersky's beneficial and highly technical participation.

At the same time, what the U.S. Department of Commerce decided last April is also understandable. **COULD** Kaspersky Lab be forced to subvert all of the personal computers in the U.S. which are using its software? Yes, that's possible. Could the KGB plant a rogue and trusted employee into Kaspersky's midst who might subvert their systems without anyone knowing? Sure, that could happen too. Just as Microsoft or a well-placed Microsoft employee could do the same for all of the machines in Russia and China that are still running Windows. And as a result, as we've reported here previously, both of those countries are also moving away from their dependence upon closed software from the West – most notably Windows – as rapidly as they can.

Across the span of the last 50 years, computing has become personal to the point that we now all carry communicating computers in our pockets. And those communicating pocket computers are all communicating through an incredibly well-working global network that grew up right alongside, and kept pace with, this incredible evolution in technology. And across this span of time most of the world enjoyed relative peace and a great deal of relative prosperity while technology continued rushing ahead at breakneck speed.

Everyone was in a hurry to see what could be done, what new value could be created and what personal fortunes might be amassed. National geographic and political boundaries were ignored in the rush to interconnect everything for maximum value and profit and the entire world has truly been transformed.

But the world remains politically divided and now after 50 years of astounding prosperity and technical advancement, we're beginning to witness rising tensions among some of the world's largest political powers. Given how deeply intertwined the world's technologies have become, it's inevitable that these technologies, our software and our networks would begin to fall victim to the rising tides of nationalism.

As we know, Russia has even been testing their big Internet cutoff switch which they can pull to isolate Russia from the rest of the global Internet, just running internally on RussiaNet.

And I've joked for years, using my $5 automated AC outlet as a target, about the absurdity of the West being at odds with the Chinese manufacturers of most of our technology. It's insane. Our homes are filled with Internet connected gizmos and gadgets that phone home to Beijing or other data centers outside of Western control.

And in recent news, the US Commerce Department is expected to ban the use of Chinese and Russian hardware and software in American smart cars. According to Bloomberg and Reuters, the upcoming ban is the result of an investigation of cybersecurity risks associated with smart cars. The US government fears foreign adversaries may use technology embedded in US cars to hack vehicles, intercept communications, or track targets. And so it goes.

The problem is that in today's current climate of increasing mistrust, the demonstration of "risk" is all that's necessary to drive policy and policy drives behavior. Having the Internet as a single connected global network is an inherent risk – but it's also been unbelievably valuable. At the least it has allowed people the world over to have access to markets and opportunities that would never have been available without this incredible global communications network. And yes, communication itself is risky, especially within countries that wish to exert tighter control over what can be communicated. So is the solution to follow Russia and break this global network into separate pieces, with each piece only shared among those whose goals and motivations are aligned and trusted? If that's what ends up happening it would be a horrible shame and would represent incredible lost opportunity... especially for those parts of the world that are being so rapidly advanced and lifted up through access to this amazing Internet resource.

Kaspersky's ejection from the U.S. is worrisome as a tangible indicator of the changing politically-changed technological environment that will affect us all. I sincerely hope our various governments don't allow fear to blind them to the fact that communication is always better than isolation.