Kaspersky Exits the U.S.

Description: 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?

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-993.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-993-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here, the man we trust with the information you need to stay safe these days. We're going to talk about the weird thing that Kaspersky antivirus did on its last day in the United States. Why you should worry if you're one of 106 million U.S. individuals whose information was, yes, once again leaked online. And Google takes a big step forward with Passkeys. All that and more coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 993, recorded Tuesday, September 24th, 2024: Kaspersky Exits the U.S.

It's time for Security Now!, the show where we cover the latest security news with this cat over here to my right, Mr. Steven "Tiberius" Gibson, your host at the Gibson Research Corporation. Hello, Steve.

Steve Gibson: Hello, Leo.

Leo: Good to see you. We're looking at each other like the Brady Bunch.

Steve: That's right. There he is. Welcome back. Mikah held down the fort for you for a couple weeks.

Leo: Thank you, Mikah. Thank you, thank you.

Steve: We had a good time, learned some things. I did not want to forget to tell you that one of our pieces of news is that Peter Hamilton is back.

Leo: Oh, good.

Steve: With the first of a duology. So we're not doing anything until he gets the second one done because...

Leo: Yes, we've learned that lesson.

Steve: Oh, boy.

Leo: You start the first one, and then it goes, well, it's not over, but you're going to have to wait a year.

Steve: Oh, and my god, you get all wound up, and you've got all this back story. And then a year from now it's like, okay, who is that? What did he do? You know, because you just, you know...

Leo: It's a lot of detail.

Steve: We're older. We forget stuff.

Leo: And I did hear you talking to Mikah about the Bobiverse and Book 5, which came out. And I got it just in time for my trip.

Steve: Oh, good. And that's - and he's, in fact, is not generally a sci-fi person, he explained. But I guess the Bobiverse is so fun and sort of, you know, lightweight that it fits with his whatever he's doing.

Leo: It's a starter drug for sci-fi.

Steve: [Crosstalk] and cooking and stuff, yeah, exactly. Anyway, probably at the other end of the spectrum is Peter Hamilton, where we know far more than we ever wanted to know about the Commonwealth, which is the background for what happens in "Pandora's Star," and then later all that Dreaming Void business.

Leo: Are we back in the Commonwealth? I hope Al Capone's not.

Steve: No, this is a whole new deal now. We're way, way in the future, so I'm sure people are going to be very, you know, altered and all kinds of cool stuff that Hamilton comes up with. And this is the result of a mass migration exodus from Earth. And colony ships go out, and one of them finds like the right place and sends a message out to all the other ones that says, hey, we've found the right place. Everybody come on over here. But apparently by the time those other ships get there, things are not good.

Leo: Not right anymore.

Steve: Yeah. And so we don't know what's wrong, but apparently there's like overlords, and

people are not happy.

Leo: Uh-oh.

Steve: Anyway, lord knows what he's cooked up. But I'm excited about it, and I did say, if there are any of our listeners who are willing to, like, get all ramped up and then hit the cliffhanger at the end of Book 1, I'd love to hear what you think without any spoilers. But I'm not going there until I can read both at once. And, you know, I think the first book is 993 pages or something.

Leo: Oh, my gosh.

Steve: I know. Again, it will hold open a door with very strong springs. So that's what you can count on Peter for.

Leo: He's our favorite sci-fi author. We do recommend that if you're going to start with Peter F. Hamilton, you start with the single volume "Falling Dragon"; right?

Steve: Yes.

Leo: That's the easy one. It's not - it's well, beautifully written.

Steve: Yeah.

Leo: And he's really good at hard sci-fi, but excellent characterizations and stuff.

Steve: Oh, and it's got the best surprise ending, too.

Leo: It's really good.

Steve: It's like, ooh.

Leo: And then you can start getting into the much longer. The Dreaming Void, not my crazy, my favorite.

Steve: No, no. Especially the last one. The last one was like, wow, did you promise somebody to do nine massive novels, and you just ran out of stuff after number eight, and so you just said, well, we're going to keep on going.

Leo: This does happen. This does happen.

Steve: Yeah.

Leo: So what are we talking - I can guess, but I'm going to let you tell us what we're talking about this week.

Steve: Oh, that's right, we're here to do a podcast. I almost forgot. This is Security Now! #993. And our long-time listeners are saying, well, thank god we're not ending at 999 because...

Leo: Clock is ticking.

Steve: ...you know, we're not. But in six episodes we're going be there. That's going to be very cool.

Leo: It's amazing; isn't it? You know TWiT 1000 is next week.

Steve: Wow.

Leo: Not this Sunday, but a week from Sunday, yeah.

Steve: Wow. Very cool. And so we're going to find out if your four-digit stuff works. I think it will because you've always had a leading zero.

Leo: You know, I must have been prescient.

Steve: I was very impressed when I saw that. I thought, did he really think 20 years ago that he was going to need four digits?

Leo: I mean, really?

Steve: I was thinking that two would be fine.

Leo: Yeah, yeah. Always over-ambitious.

Steve: Anyway, today's title is "Kaspersky Exits the U.S." But by popular demand, and I didn't talk about this last week, actually I didn't have enough information to talk about it last week. But by popular demand I want to talk about the technology and the supply chain aspects of the very powerful event that happened involving exploding pagers and walkie-talkies.

Leo: Wow, what a story.

Steve: Also we've got the question, is Ford Motor Company planning to listen in on their occupants? Some of their recent patent filings would suggest that. But I want to help put that into perspective. We've got the highly personal data of 106 million-plus individuals having been found unprotected online. So again, another NPD-style breach. Big news for Passkeys, making a huge step forward in the industry. And is there a serious 9.9 level unauthenticated remote code exploit in Linux? Probably is, and we're going to find out in two weeks. But we'll share what's known today.

Also we've got more credit bureau freezing insanity, a little bit of question from our listeners about Drobo vs. Synology, an update on my email adventure, a question about WiFi security with and without a VPN, obtaining CPE credits from listening to Security Now!, as many of our listeners do, and a defense for Microsoft's own Defender XDR endpoint security. We've been talking about CrowdStrike. One of our listeners says, hey, XDR is worth looking at, too. And then, what mess did Kaspersky make...

Leo: Oh, what a mess.

Steve: ...leaving the U.S. market last week, and what are the wider implications for the Internet's future? So I think a lot of interesting stuff for us to look at and talk about this week. And of course we've got, as always, a great Picture of the Week.

Leo: I have it ready. I have it ready for you, Steve. And of course among the most important things that you do, Steve, the Picture of the Week.

Steve: So I gave this one the caption, "What event could have prompted the addition of this sign?"

Leo: "Parking available in empty spaces only." Wow,

Steve: Because what you really want to do is to try to park in an occupied space. I, uh, yeah.

Leo: Ay ai ai is right. I don't know.

Steve: Now, I have had some feedback from our listeners who saw this already. My morning's mailing to just shy of 9,700 Security Now! listeners went out over the course of 30 minutes this morning, and a couple of them said, you know, it looks like this is kind of a park or something. I mean, you can kind of see behind the sign?

Leo: Oh, you could park like on the grass.

Steve: There are some non-marked, like some areas which are not spaces. And so maybe people were kind of parking on the lawn or whatever. And I actually think that was probably likely.

Leo: Never put it past them.

Steve: I thought this was funny, nonetheless. And so, you know, we do try for a little humor for our Picture of the Week when we can get it. And in fact we're going to need some humor.

Leo: Uh-oh.

Steve: Talking about our first topic - which is not at all funny, I'm just saying to balance this topic - many of our listeners wrote last week to say, Steve, I hope you're not going to shy away from the topic of the exploding pagers, which happened in the possession of predominantly, largely,

members of Hezbollah last week. Actually it was last Tuesday. As I said, shortly after the news of these exploding pagers broke, I started receiving notes from our listeners saying that they were looking forward to my talking about this today.

And as always, what most 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. You know, this is not a podcast that will examine or comment upon the politics or the morality, even, of what occurred. You know, that's not what we're here for. And we've had hot topics occur in GRC's newsgroups and forums from time to time. When that happens, I note that there are ample other places on the Internet for such discussion, if that is what one is seeking. But that's not here, you know, this is about technology.

So I spent some time coming up to speed about what was known. And I had the advantage of having been 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 back stories and report their findings. As it happens, I found exactly the sort of background and technical coverage that's appropriate for this podcast over on the CryptoMuseum.com site, of all places. Here's what they wrote, and they dedicated a page to this event.

They said: "On September 17th, 2024, thousands of pagers of the Lebanese terrorist organization Hezbollah exploded more or less simultaneously. Around 5,000 pagers had been obtained by Hezbollah shortly before the incident, 4,000 of which exploded that day, after receiving a specially crafted message. In the incident, at least 12 people were killed and around 2,750 were injured. A day later, more than 400 handheld radios (walkie-talkies) used by Hezbollah also exploded. Although there was no direct proof," they wrote, "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 upon the public switched telephone network. Hezbollah used these pagers for security reasons, as they were apparently afraid that their communications via public networks could be intercepted or cut off. It seemed," they wrote, "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 a 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 549,000 euros. It's 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 Orban, 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 there, 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 was not disclosed, Bulgarian media revealed it was Norta 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 through 174. The ICOM IC-V82 is a straightforward two-way radio of the kind that are also used by Amateur Radio Operators. It was discontinued in 2014 and should no longer be available on the market. ICOM stressed that the devices had not been supplied by them. It's known, however, that counterfeit IC-V82 radios, not manufactured by ICOM, are widely available. Counterfeit radios are commonly produced in China and are difficult to distinguish from real ones. They're available from electronics stores in Asia and come with 'original' packaging.

"In the case of the exploding IC-V82s, it was not the battery that exploded, but their front top. Apparently an explosive device had been placed inside the radio, close to the microphone speaker, which is the part that's closest to the face when the radio is operated. This suggests that it was the intention to cause maximum, potentially lethal, 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 the counterfeit IC-V82 radios from Asia to Hezbollah. This is the same company, Norta Global Ltd., that might have been involved in supplying the AR-924 pagers.

"The number of radios, around 450, is smaller than the number of exploded pagers, which was around 4,000. But since the radios are physically larger, they carried more explosives and were therefore more damaging. It's currently unclear how and when the handheld radios were manipulated, and how they were triggered remotely. But," they wrote, "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's 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 three-digit DTMF digit sequence user ID. It's likely that a unique combination of the above techniques was used to trigger their synchronized detonation."

Okay. So we have an example of a seriously well planned, well coordinated, and breathtakingly real-world physical supply chain attack. The article said authoritatively, and I've seen it in several other places, that it was 5,000 pagers that 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 - well, first of all, if Israel was behind this, and if whoever was behind it 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 detonation, which would require a custom circuit board, there's no way this could have been done overnight, or even close to 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 is particularly well-suited for rough use in the field. I suspect, and this is entirely my conjecture, it's more likely that Hezbollah's choice of pager was known ahead of time, you know, from previous contact with them in the field, 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. You know, this is another of those situations where we're ever unlikely to have all the facts, since those who have all the facts stand nothing to gain by leaking anything more.

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

quoted, saying: "What we've 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 their 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."

Leo: Yeah, no kidding.

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

Leo: I think it's important to kind of emphasize that this must have been years in the making, and that they are, you know, this isn't the kind of thing that's going to happen all the time to us, to other people. This must have been - this is a major effort that may have been as long as a decade in the making. And so you're not going to see this, I hope we're not going to see this happening all the time because that would make everybody very nervous about their devices.

Steve: Yeah. It was interesting that they managed to get a hold of plastic explosive that was specifically lacking the markers that would have made this obvious in any sort of an X-ray. And, you know, this is, from a technology standpoint, custom firmware would have been necessary.

Leo: Right.

Steve: Which would have meant that you had to have the source code for the original device's firmware, or maybe suck it out and reverse engineer it, and then edit it in order to incorporate secret code triggering. You also, you know how software goes, you never want this to go off by mistake.

Leo: Right.

Steve: That would be a disaster. You would, for one thing, you would tip your hand. If one blew up, then nobody would, you know...

Leo: These people were carrying around...

Steve: They'd throw all the rest of them in the river.

Leo: They were carrying explosives in their pocket for months; right?

Steve: Yes.

Leo: And unwittingly. I mean, it's kind of a, I mean, I don't want to admire it too much, but with some grudging admiration for what an amazing operation this was.

Steve: And it is an example of a classic supply chain attack because, you know, these essentially off-the-shelf pagers were purchased by a specific organization.

Leo: Middleman; right.

Steve: Yes. And the pagers specifically sent to that specific organization were intercepted and swapped out. And so, you know, people will say, yes, but there were innocent people who were also hurt. And that is absolutely true. And that's [crosstalk] consequence...

Leo: Including children, at least several children, yeah.

Steve: Yes. As the unavoidable consequence of the bluntness of this.

Leo: Right.

Steve: Because, you know, you're not in a position where you're looking at your enemy through a sniper scope. You're, I mean, and I'm sure at some level Israel and Israeli intelligence services were holding their breath that they would get the outcome they were seeking, which was a highly targeted event.

Leo: Well, remember that the CIA at one point was accused of, and I think it was true, of sending booby-trapped cigars to Fidel Castro, at least they thought about - thought about doing that.

Steve: It made a great story, even if it wasn't true.

Leo: Yeah. You know, this is the kind of spycraft you read about in novels or in movies.

Steve: Yes.

Leo: The fact that this worked, and worked so effectively, is...

Steve: Yeah, nobody wants to call this a spectacular success.

Leo: No, because it's horrible.

Steve: Yes.

Leo: But you have to have some grudging admiration for the ability to pull this off. And the real point of it, as with all terrorist acts, is to terrorize. And to make people say, hey, I wonder if my pager's okay. I wonder am I safe. Do they know where I am?

Steve: And there now is reporting that the upper echelon of Hezbollah is no longer using any technology, that they are having to meet face to face. And so that significantly crippled their communications infrastructure.

Leo: Right, slowed them down. And that's why they were using pagers because they decided that phones were compromised, and they couldn't use those anymore. So you get the feeling this had been planned for many years, over a long period of time.

Steve: Yeah.

Leo: Very interesting story.

Steve: So the headline was "Ford seeks patent for tech that listens to driver conversations to serve ads." And at that point you just turn the car off and get out. But okay. The Record, the publication The Record, published a piece two weeks ago that I did not have the chance to get to until now. But it's too important for us to miss in this podcast. And I've got some backpedaling to do after we lay the foundation for this. The Record's headline makes it very clear where we're maybe headed, reading, as I said, "Ford seeks patent for tech that listens to driver conversations to serve ads." Apparently they want to listen in on the conversations being held inside the car in order to present advertisements on the system's entertainment system.

So The Record says this. They write: "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 will also predict routes, speeds, and destinations to customize ads to drivers, the application said. The system could pull audio from 'audio signals within' - this is from their patent application - '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 whether to deliver audio versus video ads, providing ads to drivers as they travel 'through a human-machine interface of the vehicle,' the patent application said."

Okay. So 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 mentioning 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." You know, wow. 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,' said the patent application. '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, et cetera.'

"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 patent process protects new ideas and helps us build a robust portfolio of intellectual property.'"

Now, that is 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, saying: "The ideas described within a patent application should not be viewed as an indication of our business or product plans." And in a follow-up statement, Ford said: "It will always put the customer first in the decision-making behind the development and marketing of new products and services." Okay, so there's hope.

"The system could cull data," the article says, "from third-party applications or set up screen input preferences to predict the number of ads a driver should be served. 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 a trip to medical care facility' would be considered by the system." That's right, because what we really want is our car reporting to our insurance companies that we've been spending a lot of time at medical facilities.

And speaking of tattletales, 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 kind of thing is no concern to the U.S. Patent and Trademark Office. That's not what they focus on. The 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 performing 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 into paying. So you really have to wonder what they're thinking. If nothing else, the communications available thanks to the Internet means that if this ever happened just once to someone anywhere, it would make headlines, and you'd have to imagine that Ford sales would crash overnight.

But I want to reiterate and reinforce the truth about what that Ford spokesperson said about patents not necessarily implying future product plans. That is 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 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. It's like, whoa, that's a great idea. Let's patent it. So again, it's a far cry from actually suggesting that that's what Ford's cars are ever going to actually do.

Leo: Yeah. I think it's really important to say that. On MacBreak Weekly we are regularly challenged with the idea of talking about the patents that Apple has filed. And often they're not, you know, with any intent to release a product, but just for a variety of reasons. You

could even, in fact Ford should probably say this, make the case that, well, we're doing this defensively so that if anybody tries to do it, we can stop them, saying no, we have the patent on that, and you'd better not.

Steve: And nobody should.

Leo: And nobody should, yeah. I mean, seriously. Although I have to point out, you remember when Apple was in the car business briefly, $10 billion later, that a lot of what the consideration was was for autonomous driverless vehicles, where you're in a living room, and how they could turn that living room basically into a mobile ad platform. And you can see that probably Ford's thinking along those lines, as are so many companies.

Steve: And while I was doing a little bit of research on this, Leo, it turns out that YouTube is planning to show ads when you pause the videos.

Leo: Exactly. Oh, yeah, they do now, yeah.

Steve: And so is Hulu.

Leo: It's a popup. It's just a popup that says, hey, you paused it. Why don't you go get a Dr. Pepper? Ads everywhere. Remember the Philip K. Dick short story where ads were everywhere? We thought at the time, oh, that'll never happen.

Steve: Oh, or any of the sort of dark sci-fi that you see.

Leo: Sure, "Blade Runner." Ads on every surface, yeah.

Steve: Yes. Holograms are jumping out at you, soliciting, you know, everything.

Leo: Exactly.

Steve: We are headed there, Leo.

Leo: Speaking of breaches. There's another one.

Steve: Just when you thought it might be safe to unfreeze your credit reporting.

Leo: Never. Never.

Steve: I'm joking. I know you know that it will never again...

Leo: Never.

Steve: ...be safe for anyone to unfreeze their credit reporting.

Leo: That's true.

Steve: You know, that ship has unfortunately sailed and sunk. 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 the bad guys got their hands on this latest trove of treasure. But it was publicly exposed, unencrypted and unprotected by any password, for some length of time. So we don't know. Yesterday, Cybernews' headline was: "One-third of the U.S. population's background info is now public."

Leo: Oh, geez. Good news is they already knew all this stuff from the last breach; right?

Steve: That's right.

Leo: So I'm not going to get too worried about it.

Steve: So they wrote: "MC2" - that's the name of the company. "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."

Leo: They're data brokers; right?

Steve: Yes, exactly, yes. "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."

They wrote: "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 U.S. citizens" - thus one third, since we have about 330 million people here - "which raises serious concerns about privacy and safety. Estimates suggest that at least 100 million individuals were affected by this massive data leak.

"The people and the organizations using MC2's background check service were also exposed, as the data of 2,319,873 users who subscribed to MC2's data services was also leaked." So we know who was pulling all this data, and all the data that was available to be pulled. "The leaked data included names, email addresses, 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."

Now, the good news is I looked over the data, and I didn't see any reference to social security numbers. But on the other hand, that's already out there from NPD; right? So, okay. There is, however, plenty of personal data that goes far beyond what the NPD breach covered. And this is the problem that we keep seeing with the so-called "Big Data breaches." This latest MC2 leak data could be merged with the NPD breach data to create an ever bigger, more comprehensive database. So basically, you know, lock your data, freeze your credit, and just stay home because it's bad out there. I don't know. Anyway, for what it's worth, there were no social security numbers. But still, this could be merged into an even bigger breach.

Okay. This next piece of news is significant. Last Thursday Google Chrome's project manager blogged under the headline that I thought was under-hyped. The headline just said "Sync

Passkeys securely across your devices." Okay. 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, you know, leading by a large margin, and presumably other Chromium-based browsers, too, now natively supporting Passkeys, built into the browser. Here's what Google posted under that under-hyping headline.

They said: "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 into apps and websites, moving us one step closer to a passwordless future.

"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, you know, using it as the authenticator. Today, we're rolling out" - this was written last Thursday; right? "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 is currently available for testing in Beta. Once saved, they'll automatically sync across all your devices" - meaning all your instances of Chrome, right, where you're signed in - "making signing in to other websites 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" - and I'm glad for it - "to ensure your Passkeys are end-to-end encrypted and cannot 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 alphanumeric 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." So it is built into your browser.

That "started today" was a link to passwords.google. So anybody who's interested can open Chrome and head over to passwords.google to enable, configure, and start using Chrome's built-in Passkeys solution. And I did note that, with the addition of a PIN, which can be a passphrase, that is the missing feature which SQRL always had which enabled you to securely use essentially the same kind of public key authentication, which I built, you know, which SQRL was built around, securely on your desktop.

Leo: Oh, Steve. Poor Steve. There's just constant reminders of how it was done right at one time.

Steve: Yeah, yeah, well.

Leo: The market didn't listen.

Steve: But Leo, to have Passkeys in Chrome, that's huge.

Leo: Yeah. I see.

Steve: So now wherever you're using Chrome, you'll have synchronized Passkeys protecting it. Adding an additional layer of a PIN or a passphrase, you know, stronger than a PIN, makes sense.

It sounds like it's used probably in some time-consuming, I'm sure, in a time- and processor-intensive hashing to create a key which then decrypts your store of Passkeys so it's, you know, you need to provide that PIN to decrypt it in order to authenticate, so that's good.

Leo: Of course it's a complete lock-in to Google Chrome.

Steve: It is. So unfortunately that is the nature of Passkeys at this point. It is not, you know, platform agnostic.

Leo: You're going to be locked into something.

Steve: Yeah. They don't want it to be. So, okay. Now, 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. So thank you, Alessandro.

The researcher behind this 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." But he's not evil. He has a presence on LinkedIn 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 15,000 - yes, look at that web page, Leo, the guy has got five pages of links to his stuff there. It's really impressive. He's posted more than 15,000 times under Twitter and has accumulated more than 42,000 followers. His site is www.evilsocket.net, and he uses the glider from Conway's Game Of Life as his icon.

Leo: Oh, good catch. Wow. That is impressive that you saw that.

Steve: You know that, yeah, this guy knows what's going on. And I wrote in the show notes, "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 clearly the real deal."

Now, 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. Here's what he just posted, and why it might matter. He leads with six bullet points. "Unauthenticated," meaning you don't have to provide a username and password, "unauthenticated RCE," so we know that's remote code execution, "versus all GNU/Linux systems, plus others" - and I should note that that also includes BSDs, so the Unixes - "disclosed three weeks ago," he wrote. "Full disclosure happening in less than two weeks (as agreed with devs). Still no CVE assigned."

He said: "There should be at least three, possibly four, ideally six." He said: "Still no working fix." Oh, and Leo, if you want to scroll down two pages, I've got a link that you could put up on the show of this. "Still no working fix." He said: "Canonical, Red Hat, and others have confirmed the severity, a 9.9," and he said: "Check screenshot." He said: "Devs are still arguing about whether or not some of the issues have a security impact."

Okay. Then he wrote: "I've spent the last three 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." He said: "Responsible disclosure no more."

Leo: Uh-oh.

Steve: And there was another link, but I'll explain why I don't have anything more there in a second. He said: "The write-up is going to 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."

He said: "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*t, 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 though he's literally giving you proof of concept after proof of concept, and systematically proving your assumptions about your own software wrong at every turn. This is just insane."

Leo: This guy is Italian; isn't he.

Steve: He says - yeah. He said: "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 and mediate from the beginning."

Leo: The Ubuntu people.

Steve: "I really don't know how they manage to keep their cool like this. This is going to be the write-up opening statement. It's an actual comment from the GitHub conversation. I mean, it's not wrong... And he said: "And yes, I LOVE hyping the sh*t out of this stuff because apparently sensationalism is the only language that forces these people to fix."

Okay. Now at this point we don't know more. We do know that an 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, or 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, you know, 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, because they follow him. I applied to follow him. I don't know if I've been permitted yet. I've been busy. Anyway, so the comments in that thread are things such as: "Probably and luckily the first to point it out publicly, but not the first that exploited it. It's sad." Or "Please don't disclose on a Friday. Preferably on Tuesday. I like my weekends." Someone else said: "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." Yikes. But again, we don't know.

Another comment: "Any observed active exploitation? A vuln impacting all Linux distros with a low attack complexity going unnoticed for a decade is highly unlikely." Also, "Seen both sides of this," wrote someone. "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 CVEs have been confirmed in the blink of an eye. Don't let one bad one put you off." Someone else said: "Also, all Linux systems and others? Does that mean Android and BSD?" And somebody else replied: "Says elsewhere in the thread BSD is included." And finally: "Not to piss anyone off, but I have seen far too many high CVEs that just turn out to be a fringe," or "the devs don't agree with me so they are dumb."

Anyway, as I said, 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 his followers. And in two weeks we'll apparently know more. Either way, this will be interesting. So stay tuned. Maybe a big deal, maybe not.

Leo: Yeah. It sounds like he's credible. But it is a lot to say.

Steve: It is, yeah.

Leo: And that's a big claim.

Steve: I mean, you know, and some of these comments, like, you know, low attack complexity, trivial to execute, like, you know, your microwave is vulnerable, who knows. Anyway.

Leo: As long as my coffee machine's not vulnerable, I'm okay.

Steve: Don't mess with my coffee machine.

Leo: Don't mess with that baby. Let's close the loop, shall we?

Steve: Let's do it.

Leo: All right.

Steve: So Stephane, he said: "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 was no way for me at the moment."

Leo: Wow.

Steve: I know.

Leo: It's federal law in the U.S., but I guess not in Canada.

Steve: Yeah. He said: "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." He says: "It is my credit."

Leo: Yeah.

Steve: "I should not be held hostage by credit bureaus. Thanks, Stephane."

Leo: Badrod in our Discord says Quebec is the only province in Canada now with credit freezes.

Steve: Wow. So it is province by province.

Leo: Yeah, apparently.

Steve: Wow.

Leo: But that's why it's so good. It was the same in the U.S. until they made that federal law. And that's the way to do it.

Steve: Was it state by state?

Leo: It was state by state.

Steve: Ah.

Leo: And the reason that was problematic is that in some states, I think Maine it cost a lot of money to unfreeze your credit. It was different amounts of money for every state. And the federal law in the U.S. made it they have to offer a freeze and an unfreeze at no cost. And all the credit bureaus do that by federal law. You've got to do that in Canada, too. That's shameful.

Steve: And as we know, it ought to be locked by default, and then you ought to...

Leo: I agree.

Steve: ...selectively unlock it for specific lenders.

Leo: We're not there yet, but that I agree.

Steve: When you want to permit access. Yeah. And something like this NPD breach is like, holy crap, I mean, it's no longer difficult.

Leo: It tells you why you need this. Yes.

Steve: Wow. Okay. And while we're on the topic of credit bureaus, a person wanting some anonymity said: "Steve and 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."

Leo: Oh, no.

Steve: He said: "That's right. We had full access to another customer's credit history."

Leo: Oh, my goodness.

Steve: "The signup" - get this, Leo. "The signup process requires your first and last name, some address details, and part of your social security number."

Leo: That's right.

Steve: "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."

Leo: Oh, wow.

Steve: "This caused her account to be matched with another woman who had a similar first name (though spelled differently by four characters), the last same 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..."

Leo: Of course not. That couldn't possibly happen.

Steve: "...we could still view the other woman's entire credit profile."

Leo: Oh, my god.

Steve: "Eventually, Experian reset my girlfriend's account, and on the second attempt the signup process completed correctly with the proper information."

Leo: Wow.

Steve: "Thank you and 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."

Leo: Yeah, since the early days.

Steve: And Leo, wow, what a mess. You know, thinking about this, I suppose the use of only a few characters of the person's first name - well, or last name, really - might make sense if matching against spelling variations was a problem.

Leo: Right.

Steve: 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? You know, what, 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," as if like it has to be a secret from the credit bureau. You know, that's why you do the last four and mask the others, right, is like you're wanting to prove that you know, but you're not wanting to share it. But when you're creating an account with them to access your credit, you absolutely want to prove to them that you know your entire social security number. It's insane.

Leo: Yeah. Yeah. It doesn't surprise me in the least.

Steve: Wow.

Leo: Unfortunately.

Steve: And these are the people who are happily giving away our credit data to anybody who asks. Right. Nile Davis said: "Hello, Steve. I've been a loyal listener since #1, and I love that you're going beyond 999. I have a Drobo 5N that I got many years ago..."

Leo: Oh, I'm sorry.

Steve: "...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 I 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's 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."

Okay. So I'm in a very similar situation, 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 in it 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 be on the chopping block. So even though I could still have obtained a replacement Drobo 5N from the supply chain, I decided it was time to switch to Synology. And all I can say about that is that I have never been happier.

Leo: I'd agree. I had a little Drobo Mini which I loved.

Steve: Yup.

Leo: But, you know, if you're just using it as a USB drive, that seems like that's probably harmless.

Steve: And if it's entirely behind your NAT, so it's not publicly exposed at all...

Leo: Right, right.

Steve: ...then that would be a factor, too.

Leo: But the "N" is a NAS, and it's intended to be sitting on your network.

Steve: And it's on mine, but not exposed. And I've got all kinds of extra security stuff that your typical consumer doesn't have.

Leo: Yes. As long as it's not visible to the outside world, it's probably okay; right?

Steve: So, yeah. So my feeling was the Drobo was fine for a non-power user who's happy with fewer options. But that's not me. That's not you, Leo. And after I set up my four-drive Synology to replace the original Drobo 5N which had died, I purchased another identical Synology for my second location. So now that location has the original second Drobo 5N, which is still going fine, and a Synology.

Leo: Well, now you're fine.

Steve: The reason I have two is that 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 a way we could set up her clients with a laptop and a two-channel EEG amplifier to facilitate "at home" neurofeedback 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, of all places, 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 synced to that second Drobo 5N...

Leo: That is cool, Steve. That's really cool.

Steve: It's still going strong, yup, and it is being used to keep all of the therapy that those laptops are doing synchronized with home base.

Leo: And presumably backs up to the Synology or some other reliable drive.

Steve: Yes. Yes.

Leo: Right. You wouldn't want it to be your only source.

Steve: So Lorrie is able to look at a local drive, a drive that's local to her, thanks to Syncthing, and look at all of the logs of the remote sessions that her clients are doing wherever they are.

Leo: That's neat.

Steve: So it's very - she's even able to, like, to tweak the therapy that a given person is doing, and those settings get propagated thanks to Syncthing to their laptop the next time they boot it up, and they're automatically using updated therapy settings. So it's really unique and cool. The point is, you know, so 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 no longer wants to offer this form of remote therapy. If that second Drobo also throws in the towel while its laptop synchronization services are still required, then I'll move its sync functions over to Synology, which, again, I love. I'm so happy with my Synologies. But if I ever have to do that, it would be a pain. So I'm just hoping that the Drobo continues to purr away. I don't ask it to do anything new. I just say, you just keep what you're doing and let's hope you last longer than my wife's therapy practice.

Leo: Yeah. People, I mean, if you use hard drives, you don't often say, oh, I hope this hard drive manufacturer doesn't go out of business. I mean, if you think of it as a USB drive, that's fine then; right?

Steve: Yeah, exactly.

Leo: As long as you back it up.

Steve: You back it up, and Syncthing's technology is very secure.

Leo: It's so - it's encrypted in flight; yeah.

Steve: It is end-to-end encrypted. And, boy, you know, it took me a while to, like, kind of really get how much work it was doing for me. I was like, this has to be harder than this. But it's actually not. You just say, here, synchronize these things. And it goes, okay, got it.

Leo: And it's surprisingly fast. I mean, it's, wow, I just changed that file, and it's already on the other drive.

Steve: Yes. I abandoned Synology's dual Synology synchronization because, if I made a bunch of changes, it sent the entire drive across again. You know, because I monitor my bandwidth. And it was like, what the heck just happened? You know, and it was like multi terabytes going from point to point. It's like, this is dumb. So I shut that down. Now I just use Syncthing, which is running natively on both of my Synologies. So, yeah, it's a win.

Leo: Yeah, there's a community distro of Syncthing.

Steve: Yes, exactly what I'm using, yup. So Danny in sunny Scotland, he said: "FYI, last week's Security Now! email was routed to my Junk folder."

Leo: Uh-oh.

Steve: Uh-huh. "I'm using Apple Mail," he says, "(and I have my own domain set up on iCloud). It was fine until last week, so I guess something must have spooked their filters." And I know what. "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, signed Dan."

Leo: It's sunny this year. Wow. Good for you.

Steve: He's making a point of that, yeah. So last week, as our listeners may remember, I asked them, any 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 emailing adventure is that just as with code signing, the earned reputation of the signer is everything. GRC, and I'm signing all my email cryptographically, the source as GRC is unspoofable. And we've been using email for our business for decades, and we have enjoyed a spotless reputation since we never have and obviously never would actually send spam.

But GRC's reputation is now being challenged 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 they can have 6.1 at no cost. And I'm careful not to use the word "free" because that raises...

Leo: Or Viagra. Those words.

Steve: I can't put any exclamation points in the email, either.

Leo: No.

Steve: That's bad. So, and in fact I actually saw one spam filter, I said "You are invited to download," and it's like, oh, you can't invite anybody, either.

Leo: Unh-unh, unh-unh.

Steve: So it's like, wow. That's what the world has come to.

Leo: Isn't it sad? Yeah.

Steve: But anyway, I've been slowly sending this out. And I suppose that from the standpoint, you know, it would technically be classified as UCE, right, 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. So I'm not profiting from this. But anyway, 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, it is also true that I have not bothered any of those people until now, and those addresses date back as far as 2004. And Leo, when I saw this I knew you'd get a kick out of it. There are addresses with CompuServe account numbers in the list. You know, they're like 76294.3276@compuserve.com. So anyway, I've been mailing in reverse order, from the most recent toward the least recent, and I've now progressed as far back as 2008, all the way through 2008, so to the start of 2008. At this point more than 10% of the addresses are bouncing. Overall, I have to say it's going better than I had hoped.

But when a major ISP like Apple or Google or Microsoft sees GRC sending to many nonexistent addresses, they will quite reasonably decide to not bother their current users with email coming in from the same source that is going to a valid address, so they route it into the users' spam or junk folders. There's nothing I can do about that. It's not possible to check people's email addresses ahead of time. I actually ran the list through something called Email Hippo in the U.K., which cut out about 20%, I think. But I'm working through the rest.

Anyway, so the good news is this will be a one-time transient problem which we should be on the other side of in a few weeks. Once that's happened, I will have a much smaller, but updated and

cleaned list that I'll be able to use going forward with much less trouble. Until then, I need to ask for everyone's patience. It would help greatly if anyone who again or continues to discover their weekly Security Now! email in their spam or junk folder, if they'd mark it as "not spam," that would be great because that is the most effective way of training the ISP's spam filters that GRC is not and never has actually sent out spam, even if we are attempting to contact some of our very old purchasers.

Leo: I will look in my spam inbox to see if I had anything. By the way, before the show began I said, hey, I don't see your show notes, because normally they go into my "important" folder. I realized why, and I don't know...

Steve: Oh.

Leo: Because at the bottom of your email it says - there's an unsubscribe link because it's a newsletter.

Steve: Yeah.

Leo: And I have a filter that whenever it sees an unsubscribe link, puts the newsletter into a mailing - it doesn't kill it, but it puts it into a mailing list folder.

Steve: Oh, oh, oh, doesn't - ah.

Leo: Because I go, well, that must be a mailing list, and I don't want to have it fill up my inbox. So I did find your email in my mailing list. I can whitelist you so that that doesn't happen in the future.

Steve: Well, thank you. And I am getting so much good feedback from our listeners who love the fact that they get this email from me every week.

Leo: So good.

Steve: It's turned out to be a big win.

Leo: Yeah.

Steve: And I can, you know, you mentioned the unsubscribe link. It was very clear to me that many ISPs are clicking that link on behalf of themselves.

Leo: Gmail does that, yeah.

Steve: When they see email coming into a nonexistent address.

Leo: That's right.

Steve: They go, oh, and they unsubscribe, and that's wonderful. There's nothing I would want more than for email to be unsubscribed when I send to a nonexistent address.

Leo: That's a good point, yeah.

Steve: That is the perfect solution.

Leo: Yeah.

Steve: And of course everything I send has a big, prominent "Unsubscribe." And in fact I was just reading, too, Leo, get this. The threshold for spam is astonishingly low. Google's formal policy, and a service that I used briefly, Postmark, they want it to be 0.1%, which is to say one in a thousand spam complaints is the most you're able to have.

Leo: Wow.

Steve: And if you go over one in a thousand using Postmark as your mailer - I'm not doing it. I've gone back to using GRC.com. But they will stop you. They will freeze your mailing at that point and say what's the problem here. Google says the same thing, but they don't have a policy exception until .3. The problem is this policy was just implemented earlier this year, announced last October. But most business-to-business mass mailings are around 3%, so 10 times the policy violation that Google has set, and 30 times the spam level that people are supposed to keep things under. As I said, we're normally at zero, and we've always been at zero. But, you know, we're getting people who click. And in fact, I've been annoyed by this Gmail UI. When I'm looking at my Gmail, and I click a bunch of things, I have to be very careful not to mismark things as spam.

Leo: Yeah. You'll never see it again.

Steve: Because Google makes it very simple to do that.

Leo: Yeah, yeah. It's gone forever now.

Steve: Yeah. Exactly. And I don't want to do that because some things I do want to keep receiving and not have them disappear into my spam folder.

Leo: Right, right.

Steve: So anyway...

Leo: But isn't it funny? I would have thought, here we are in the year 2024, that spam would have been conquered by now. And in fact it's worse than ever. You don't ever see it because everybody's so aggressively blocking it. But it's more traffic than ever before; isn't it.

Steve: And remember in the early days, Leo, of the podcast, Mark Thompson and I were working on - there was some, we had some heuristic filtering thing.

Leo: I remember it, yeah.

Steve: Of course, well, and this came up because Dvorak's comment...

Leo: "I get no spam."

Steve: "I get no spam."

Leo: He gets spam now, I'm sure. I don't know how anyone could not get spam. But thanks to all of these efforts, we maybe don't see as much of it as we did in the past. But we also, as a result, don't see a lot of email from Mom, either. So I don't know.

Steve: Actually I had a conversation with John just the other day because someone had said to him, he had been using Mailchimp for his podcast stuff.

Leo: Right, right.

Steve: And he was not happy with, you know, I guess the lack of absolute control over it. And so someone had said, oh, you know, Gibson's using this great system, you know, and so he shot me a note, and we talked on the phone for about an hour. And I just want to say again, this nuevoMailer that I found, I am - with all the stuff, all the rigmarole I've been going through, for example, I realized that .me, .mac, and .icloud were all being blocked because I was sending from SpinRite.news, which was a domain with zero reputation, and Apple just said, who the heck are you? No. And just, you know, so it's not that I misbehaved, it's just that they'd never seen me before.

And I guess of course that's what spammers are going to do; right? They're going to create, if they damage the reputation of a given domain, they'll just create a new one and start spamming from there. So Apple has a "deny first" policy. Anyway, so I had to, like, filter out all of the .me, .icloud, and .mac domains and create a separate list which then I sent through GRC.com, which Apple loved. Not so much now, but they did.

And anyway, all of the stuff I was doing, this thing is a workstation for working with email lists and sending. It's nuevoMailer, and this Greek guy, I think he only got like 132 bucks from me one time. It's in PHP. So he and I have been sending code back and forth to each other because I'm sort of in a unique position of having this massive bouncing of the email that I'm sending out, so I'm able to look at and work with him on, like, improving his recognition of the reason for things bouncing. Anyway, I cannot recommend this highly enough. I said the same thing to Dvorak. I said, if you've got anybody around who's a PHP developer, you need to be able to run PHP on your server, and you can use a third party to actually send your mail through. It will connect beautifully so you don't need your own SMTP server.

Anyway, it's just - it is a fantastic facility. So I just, you know, I like to tell people when I find a good sci-fi author or a piece of software like, you know, like the email archiver that I love also. Anyway, for email, this is it. So, you know, it won't do everything that you see from GRC because I wrote all of my own frontend. But, boy, for backend sending of email - and you can do subscriber and double opt-in and all that stuff. I just didn't want to use his because I like to do things, you know, my way. But wow, it's really great.

Okay. Steve P., and I must have given him some anonymity because I think he told me his whole name, but I thought he wouldn't want me to share it. He said: "Hi, Steve." Oh, yeah. He said: "Hi, Steve. I'd appreciate your latest thinking on the safety, or otherwise, of connecting to public WiFi. I'm currently" - oh, I know why, it was because of medical things. He said: "I'm currently

'enjoying,'" he has in quotes, "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're 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 be 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 access points appear to be branded Cisco, but of course I have no way of knowing how this is set up in the background, i.e., client isolation. Anyway, thanks for all you do. 6.1 continues to work well, of course. Regards, Steve P.," he said, "currently an in-patient at St. Thomas's Hospital, London, although hopefully not for much longer."

Okay. So the short version is that the use of any high-quality VPN system, such as ExpressVPN...

Leo: Our sponsor, which we should mention.

Steve: Oh, are they still a sponsor? Cool.

Leo: Oh, yeah.

Steve: ...completely encrypts all traffic inside of the VPN's tunnel. It's 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 servers. The only possible downside to the use of any big provider is that once the tunneled traffic emerges onto the public Internet, it is visible to everyone.

And, you know, there's always been speculation, but I don't think really any evidence, 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. But who knows? So 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, you know, generic traffic capture. On the other hand, if someone was interested in your traffic specifically, that's where they'd be looking for it. So you kind of can't win.

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, podcast #272, recorded October 27th, 2010, titled "Firesheep." Fourteen years ago, the simple unencrypted HTTP protocol was still dominant, and connections typically only switched to secure HTTPS when credentials were actively being exchanged. But these days, 14 years later, all connections are always encrypted. This makes it far safer to use any open public WiFi hotspot without a VPN than it once was.

Now, 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 at the location of the remote IP would be solidly and well encrypted. So I suppose I'd say today, in a pinch, using open WiFi is not super 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. So ExpressVPN, since our listener Steve P. has it, absolutely use it.

Leo: Keep using it, yeah.

Steve: And you should use it without, you know, without any further concern.

Leo: Point of order, Mr. Gibson.

Steve: Yeah.

Leo: So what he described is a captive portal. In other words, and you've seen, we've all seen this, you go, you join a WiFi network at an airport, and you have to go through a login page.

Steve: Right.

Leo: Technically obviously different than password protect, WPA2 password protected. But is it in fact less or more secure? I don't think so.

Steve: I would say it's less secure because all it's doing is intercepting your initial attempt to get out, and requiring you to click OK to agree to the terms of service.

Leo: Right.

Steve: Which are, you know, you're holding us harmless for anything that happens while you're using our WiFi. So click YES if you want to; otherwise, sorry.

Leo: If you're, though, in a hospital, and they have the password on the wall, and you log into a password-protected network, that's effectively exactly the same; right?

Steve: Correct.

Leo: The issue is can someone, some bad guy get onto the network to see your traffic? They could easily get through a captive portal. A password, if they didn't know it, they couldn't get through.

Steve: Right.

Leo: But on the other hand, if it's in a public place, the password is usually publicly posted.

Steve: And if a bad guy got a hold of the traffic on the other side of the access point, it's all of the traffic.

Leo: It's unencrypted anyway.

Steve: I mean, it's regular Ethernet wired traffic.

Leo: Right.

Steve: Which you can easily sniff.

Leo: So a captive portal isn't necessarily better or worse than a password. It's just a different way of doing it.

Steve: Right. And what you really want is what Steve P. has access to, which is a VPN.

Leo: A VPN; right. And one of the reasons people often don't want to use a VPN at home is they're also trying to protect themselves from their ISP.

Steve: Yes.

Leo: So if you use your home VPN, sure, you're private until you get home, and then everything is...

Steve: Exactly right. That's exactly right. Richard Anthony, CISSP, wrote: "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 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 of us who rely upon Security Now! to maintain our certifications. Many thanks, Richard Anthony, CISSP."

Leo: Huh.

Steve: And so I have no idea whether that could be done. But Leo...

Leo: Oh, it could easily be done. I'm trying to think of how we would institutionalize that.

Steve: Just sort of bring it up toward the end while we're doing the wrap-up.

Leo: Yeah. I usually - yeah, like that.

Steve: If that's there, that's all we need.

Leo: I have, in the past, when I was doing it in a studio, I would do that in the last segment of every show because it would have the title in there, and it would be the title topic. These no longer have the topics on there anywhere.

Steve: No, but I think the number and the date probably...

Leo: All they need is the date and number, yeah.

Steve: Absolutely sufficient.

Leo: And don't forget, over my shoulder there's always the date and time, if you need a date and timestamp. That's actually one of the reasons that clock is always there.

Steve: Nice.

Leo: People have asked for that. Yeah, we'll make sure to - I used to always do that. I didn't know that's why I was doing it, but it turned out that was a benefit.

Steve: Cool.

Leo: So Benito, just remember that, or whoever is in charge.

BENITO: Copy that.

Leo: How do I - how could I do that, Anthony? Is there a way I could stick a - it's in the captions? Let me go to the generic...

BENITO: Yeah, [crosstalk] to the captions, and you can hide or unhide that lower third.

Leo: Oh, okay. Good, all right. So if Benito's not around, which he always is...

Steve: Don't go away, Benito.

Leo: If for some reason Benito's not around, I will endeavor to remember that at the end of the show.

Steve: Nice. Nice.

Leo: Which is not over.

Steve: And from another listener, Richard Cornell, who is an IT Security Manager in the UK. He says: "Hi, Steve. A few times in recent SN episodes you've 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've 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."

So 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 towards native solutions as opposed to installing extra stuff outside of the box.

Leo: Yeah.

Steve: So that's good to hear. We hadn't heard anybody. We were hearing people saying, yeah, I'm sticking with CrowdStrike because it saved our butts a bunch of times. So even though they screwed up, we're not moving. And here's somebody who says, yeah, you know, Microsoft Defender XDR works just great, too.

Leo: I think one of the reasons CrowdStrike had such support was because they had so many sensors, distributed so widely globally. But I would imagine XDR has to be the same number, or at least; right?

Steve: Yeah, yeah.

Leo: Yeah. Interesting.

Steve: Okay. Our last break, and then we're going to talk about Kaspersky's somewhat ignoble exit from the U.S.

Leo: Yes.

Steve: And a little bit about what I think that says about where we're headed in the future.

Leo: Subtitled "How to Mishandle Your Transition Out of a Country." Steve is not an AI. I can vouch personally for that. Unless there are AIs that particularly like Cabernet Sauvignon.

Steve: And there could be.

Leo: There might be. All right. Let's get onto this Kaspersky thing here.

Steve: Yeah. So I started off treating today's main topic as just another news item to which I'd given the title "How to mishandle an antivirus 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 what I think is 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 read "Kaspersky deletes itself, installs UltraAV antivirus without warning." So ask yourself what you would think if something completely new and totally unknown to you suddenly appeared in your computer. And when you went to check on it using the AV system you had purchased and installed, that AV solution was nowhere to be found. Talk about mishandling a transition. So here's what BleepingComputer reported.

They said: "Starting Thursday, Russian cybersecurity company Kaspersky deleted its antimalware 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" - not like it had any choice - "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

'foreign individuals, companies, and organizations deemed a national security concern.'

"On June 20th, citing potential national security risks, the Biden administration announced a ban on sales and software updates for Kaspersky AV software in the United States beginning September 29th, 2024." And of course we covered that event when it happened.

"In July, Kaspersky told BleepingComputer that it would begin closing its businesses and laying off the staff on July 20th 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, but with many concerned that their devices had been infected with malware.

"One user wrote: 'I woke up and saw this new AV 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 matters 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 - Hotspot Shield, UltraVPN, and Betternet - and Comparitech, a VPN software review website."

And just to interrupt here, you've got to 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 of them themselves.

Anyway, Bleeping Computer says: "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 U.S.-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 what the email said. It may have said in the fine print that, if you did not want to have your AV and VPN services switched from Kaspersky to the Pango Group, you could terminate your subscriptions first. Who knows?

What's clear is that for something as important as a system's antivirus/antimalware protection, 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 did not

happen because Kaspersky almost certainly made a bunch of money selling their entire paying AV 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 now with UltraAV and UltraVPN.

Note that a continuing subscription relationship with these entities implies that Kaspersky also transferred their entire U.S. subscriber database, complete 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. And I have to say I can't recall a time that there wasn't a Kaspersky. Consider the beginning of Wikipedia's article about them.

Wikipedia says: "Kaspersky Lab is a Russian multinational cybersecurity and antivirus provider headquartered in Moscow, Russia, and operated by a holding company in the U.K. 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 from 2016, though annual revenues were down 8% in North America due to U.S. government security concerns."

Leo: You think?

Steve: "As of 2016" - yeah - "the software was about 400 million users and has the largest market share of cybersecurity software vendors in Europe." So, you know, they're the real deal. "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 fourth in the Endpoint Security segment, according to IDC data. According to Gartner, Kaspersky Lab is currently the third largest vendor of consumer IT security software worldwide, and the fifth largest vendor of Enterprise Endpoint Protection. In 2012, Kaspersky Lab was named a 'Leader' in the Gartner Magic Quadrant for Endpoint Protection Platforms."

So, you know, this is not a fly-by-night outfit. I would argue that they have far more cred than Pango, the Pango Group, who makes AV stuff no one's ever heard of before. But that's what Kaspersky's users automatically got. And I think this is unfortunate. There's, remember, 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.

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 that were in Microsoft Windows.

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

The next year, in January of 2013, Kaspersky discovered the Red October malware, which had been used for widespread cyberespionage 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.

Next year 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.

Later that year, in November of 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 other words, you know, who we regard as the good guys. The next year, in 2015...

Leo: Well, us, in fact.

Steve: Huh?

Leo: Us.

Steve: Yes, us. In 2015, Kaspersky identified a highly sophisticated threat actor that it called "The Equation Group," speaking of us. 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 U.S. intelligence efforts. It's suspected to have been developed by the National Security Agency and included many unique technical achievements to better avoid detection. Yet Kaspersky found it.

Later that year, in June of 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 - six zero - 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.

The next year, 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.

Also that year, 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. Later that year, in June, 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. These guys have dramatically improved the state of cybersecurity through its entire history, starting from 1997. Thus it's no surprise that so many people have rightfully trusted Kaspersky's antimalware solutions through the years, and actually through the 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? We know the answer. Yes, that's possible. Could the KGB plant a rogue and trusted employee into Kaspersky's midst who might subvert their systems without anyone else 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 been truly 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 basically running internally on RussiaNet.

And I've joked for years about 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 U.S. 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 U.S. government fears foreign adversaries may use technology embedded in U.S. 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 have never 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-challenged 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.

Leo: It's interesting because this is the episode that you talked about the pager attacks, the supply chain attacks. And in a way that's a similar risk with software from an unknown source or a potentially enemy source.

Steve: Yes. You made the point, Leo, about how long ago those pagers may have been set up.

Leo: Right.

Steve: We don't know what's in the chips.

Leo: Right.

Steve: That we've been blithely purchasing.

Leo: And this is only going to get worse. We used to think, oh, you know, you can just trust everybody. Now we're learning otherwise, and we're setting up perimeter defenses, saying, well, if they're outside the U.S., you can't use them. But we know perimeter defenses haven't been a good solution for companies for some time. They've moved to something called Zero Trust. And I'm wondering if ultimately we're not going to have to move to a Zero Trust kind of attitude on everything that we use as consumers.

And this might be up to you, Steve. I'm going to put this on you. But we need people like you to come up with ways that we can use stuff, but minimize the risk from that stuff. You know? Because that's what we're going to have to do. There's nothing that's known safe anymore. And soon we're going to get in the position where we can presume that much of what we use is not safe. So we're going to need a system, a Zero Trust system that allows us to somehow control that. Yes?

Steve: I guess the question is, you know, and this reminds me of "Ghostbusters," who you gonna trust?

Leo: I mean, we've gone from trusting everybody; right? And I've often said this is part of - this is civilization. Civilization doesn't exist without cooperation and trust. When you drive down the street you trust the guy coming in the other direction at 30 miles an hour is not going to turn into your lane.

Steve: Yes.

Leo: That's part of being in a civilization, a cooperative environment. But it seems to me that maybe that's not going to work long term with technology.

Steve: So, I mean, it really means that we pull our skirts in, and we don't accept, I mean, for example, that every chip in every auto is designed and fabricated in the USA.

Leo: Right. But is that enough?

Steve: And this was my point about the economy. I mean, yes, that's great for nationalism. But we're able to use incredibly inexpensive design and fab in China because it's incredibly inexpensive.

Leo: Yeah.

Steve: So we're talking about huge increase in cost. Now, on the other hand, we saw a huge supply chain shortage during COVID when automobile prices jumped up because we couldn't get the chips that we needed from offshore. And presumably, if they were being manufactured in the good old USA, then there wouldn't have been a supply chain problem.

Leo: Or would there? What about Ford?

Steve: Right.

Leo: I mean, we live in a world where trust is required. And yet we are rapidly experiencing the erosion of trust.

Steve: And it's so valuable, Leo.

Leo: It is. Without it...

Steve: It is so valuable.

Leo: We can't do what we do without it. Can't drive down the street safely without it. You can't go to Starbucks and have a coffee without it. So what do we do? This is an interesting conundrum. I don't think saying, okay, you can only use stuff from the U.S., clearly that's not the solution. And that's, I mean, that's what we did with Kaspersky. But is that the solution? I don't think so. All of our devices are made in China.

Steve: Well, and we just forced a high-quality source of cybersecurity out of the U.S. Nobody gets to use that anymore.

Leo: Right.

Steve: And so, yes, there are alternatives. There are, you know, there are non-Russia-based actors. And, you know, and some specious claims were made about Kaspersky employees and - I was pronouncing the name wrong the whole time.

Leo: I don't know. Kaspersky, Kaspersky.

Steve: Kaspersky, Kaspersky. Anyway, I mean, what it really is, is sad.

Leo: We need, you know, a chain of trust. And we have that system with the certificate systems. We know how to do it. And I think maybe that's ultimately what's going to happen here, and say...

Steve: Well, and look at what Apple is doing with the servers.

Leo: Apple's the first thing that comes up.

Steve: That are coming in from offshore.

Leo: Yeah. So do you trust Apple? And then...

Steve: I mean, bend over and spread them.

Leo: And then Apple's going to be - the burden's on Apple to make sure that those Shenzhen factories are not compromised, that those workers are not working for somebody besides Apple and us. It's an interesting world we live in. We are very interdependent.

Steve: Look at the extra cost that Apple's going through.

Leo: Right.

Steve: In order to know that what they're plugging into their data centers has not had some supply chain compromise.

Leo: Yeah, and I hope that it's not theater. I hope that that's real. You know what I'm saying?

Steve: Oh, yeah.

Leo: That this isn't merely a marketing term. Because more and more we're going to need to trust them.

Steve: Yeah.