When Governments React

Description: This week we discuss France, Britain, Japan, Germany, and Russia each veering around in their Crypto Crash Cars; WikiLeaks' Vault 7 reveals widespread CIA WiFi router penetration; why we can no longer travel with laptops; HP printer security insanity; how long are typical passwords?; Microsoft to kill off SMBv1; the all-time mega ransomware payout; Google to get into the whole-system backup business; hacking PCs with vape pens; a bit of miscellany; and a bunch of "closing the loop" feedback with our terrific listeners.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-617.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-617-lq.mp3

SHOW TEASE: It's time for Security Now!. Yes, I am back. Thank you to Father Robert Ballecer for filling in for me. We have a lot to talk about, including initiatives by the U.K., by France, and by Japan to infringe on our privacy even more than before. Steve explains, next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 617, recorded Tuesday, June 20th, 2017: When Governments React.

It's time for Security Now!, the show where we cover your latest security woes. Always something to talk about with Steve Gibson of GRC. Good to see you, Steve.

Steve Gibson: Great to have you back, Leo, all rested and relaxed and raring to go.

Leo: I thank Father Robert for filling in. It's nice. Now he's on vacation. And I understand he's not allowed to talk on his vacation.

Steve: No. In fact I sent him a note to follow up on, like hours after we finished recording last week, just to say thanks for standing in, and I got an auto-reply saying "I'm no longer receiving email." It's like, whoa. So, I mean, and he...

Leo: Yeah. How long is that going to be, Lisa, that Robert's - he's on his...

Steve: He said two months.

Leo: He's in his Tertian - they call it his Tertianship. Two months, wow.

LISA: [Off mic]

Leo: Who's going to sign it?

LISA: A one- or two-star general.

Leo: A two-star general's going to sign this. Maybe - this just in, Steve. We got an email from the National Security Agency. And this is not a joke.

LISA: [Off mic]

Leo: Yeah, but it's been redacted; see? "The NSA would like to import your Security Now! show onto its Intranet for general dissemination to our cybersecurity workforce." You're not surprised, so you've obviously received the same email, Steve?

Steve: No, but I have a standing invitation from them to come and talk.

Leo: They like you over there at the...

Steve: Yeah.

Leo: They say, "While we believe under the Creative Commons license this is permissible," which it is, "there are elements within your website's term of use we cannot agree to and therefore precludes us from importing those shows. Specifically, parts of the Disputes and Indemnities section are inconsistent with federal law." I think we just pasted it from some website, so I'm not surprised. "We would like to execute a Memorandum of Understanding between the NSA and TWiT to modify these sections in a manner consistent with federal law." And apparently - then we said, well, okay, but who's going to sign it? And they said, well, it'll be either a two- or a three-star general.

LISA: One- or two-star.

Leo: One- or two-star. There'll be stars involved. So is that okay with you, Steve? We give Security Now! to the NSA?

Steve: That's absolutely fine. I was hoping that maybe Donald would sign the order, but...

Leo: It would be fun if - could you get the President to sign it?

LISA: [Off mic]

Leo: Okay, just asking, you know. General Clapper will be signing it. I don't know who'll be signing it.

Steve: Tell Lisa thank you and hi.

Leo: Yes. Steve says hi. Okay.

Steve: Cool.

Leo: No, I saw that this morning, I thought, that is great. Steve will love that.

Steve: I do. That's great.

Leo: Yeah, yeah. Well, you know what, it never fails to impress me the number of people who listen to the show and then the variety of places that they listen. I think this has, at this point, become the premier show for security information. And so everybody wants to know what's going on, and no one tells the story better than Steve.

Steve: Well, you know, I learned the lesson back when I was doing the Tech Talk column for InfoWorld that endurance is one of the defining factors. After a couple years, I got a nice note from the then-editor in chief of InfoWorld, Jonathan Sacks, who said - he was responding to one particular column I had written about how optical magneto drives functioned, and the lesson I learned when as a child I dropped a powerful magnet, and it lost its magnetism. Anyway, so I put it all together into a column, and he said, wow, I just, you know, I love what you're doing.

And I said to him at the time, I responded, and I said, "Gee, thanks. You know, I kind of feel like sometimes my voice is going off into the wilderness, and nothing is happening." And he said, "Steve, you have to understand, it takes time for people to get to know you." And he was referring, of course, to the print version of InfoWorld, which is pretty much all we had at the time. He said, you know, "They're taking you into the bathroom with them," which is why I wanted to clarify that, "and into bed at the end of the day. And they have to form a personal relationship with a columnist." And I think that it's very much the same with a podcast. And so here we are approaching the end of year 12. And endurance, as I said.

Leo: Yeah. It's true in radio, too, that the longer you last on a show, people just - you become like an old shoe. And I'm the king of old shoes.

Steve: Oh, I've got so many old shoes. They're much better than new shoes.

Leo: Very soft and accommodating. Yes.

Steve: So this is Episode 617. And as I said to you, last week's title was "Things Are Getting Worse." And looking over the news from this week, I thought, okay, I have to title this one "When Governments React." So we're going to discuss this week France's, Britain's, Japan's, Germany's, and Russia's - the way I put it in my little summary, each veering around in their Crypto Crash Cars because they're reacting to the crypto problem on the Internet. We'll also talk about WikiLeaks' Vault 7 reveal of a widespread CIA WiFi router penetration. And, oh, my lord, the number of vulnerable WiFi routers and access points is what's sort of stunning about this. It's not like one or two. Also we got some information, thanks to some fresh reporting, about exactly why it is that we can no longer travel with our laptops.

Some more details about the HP printer security insanity that we originally covered in April. Now we know the nature of the problem, and it's been exploited in the lab and explained to us. So we're going to cover that. A fun chart that was made from, I think it was 32 million passwords, analyzing, for example, in one case, what is the distribution of password length, which is sort of fascinating. Microsoft has finally said, in the wake of the WannaCry, that they're going to kill off v1 of their SMB, the file and printer sharing protocol, which is what enabled WannaCry to propagate.

Leo: Good, good.

Steve: Yes, although of course now we've got patches. We also have the all-time mega ransomware payout, which is somewhat stunning. Google has announced that they're going to get into the, it's not quite "whole system backup" business, but it's closer. So it won't be competing with one of our sponsors, in fact a sponsor of this particular today's podcast, Carbonite. But it's kind of related. We'll talk about that. And believe it or not, it's possible to hack a PC with, of all things, a vape pen. We'll also cover a little bit of miscellany and some "closing the loop" feedback with our terrific listeners. So I think another great podcast.

So our Picture of the Week is brought to us by the ever-clever xkcd. And reading the caption is the way to explain this best over the air. I titled it "Lunch Order." And the caption reads: "Everyone complains about autocorrect. But we forget about the time it prevented a nuclear war." And so we have some guy who's approaching the control console who says, "Sir, Strategic Command has sent us a lunch order." And the supervisor says, "Don't they have anything better to do?"

Leo: Not launch, lunch.

Steve: Exactly. Wonderful.

Leo: Lunch. That's pretty funny.

Steve: Okay. So in our coverage of how governments are reacting, the first is a combined "French-British Action Plan," as it's titled. I've got the PDF to it. It's just two pages. But I'll just pull the highlights from it. The link to the PDF is in the show notes.

So it says: "Terrorists, and the people they influence, are using the Internet, websites, email services, and social networks to gather information, organize, spread propaganda and operating methods, send and receive instructions, and claim responsibility for their acts. At a meeting in Paris on the 13th of June" - that is, just a week and a half ago - "Prime Minister May and President Macron agreed to a joint U.K./France initiative to ensure the Internet cannot be used as a safe place for terrorists and criminals. They stressed that coordination with G7 and EU partners will be sought on these issues. The following four points were agreed as priorities."

I'm not going to go into them in detail, but the first one was improve methods to remove illegal content from the Internet. And so the idea of, by coming up with ways to prevent unwanted...

Leo: Bomb-making stuff or...

Steve: Yeah, exactly. So, for example, they said: "While efforts have been observed from companies regarding removing terrorist content, we need industry to move from their current position of reactively removing content when it is notified to them, to proactively identifying content and preventing it from being made available on their platforms in the first place."

So this is getting kind of dicey because, as we'll see, essentially governments are, as we've been predicting, wanting to exert explicit control over what has historically been a communications commons, a global commons, where people had anonymity and the freedom to put up what they ever wanted to, and the presumption was people would use their best judgment in how to decide about the veracity of the information presented. The second point was...

Leo: By the way, you remember, you're old enough - we are old enough - to remember "The Anarchist Cookbook." Remember?

Steve: Yes.

Leo: In the '60s everybody wanted to take that out of every library - it was pre-Internet, obviously - because it had bomb-making recipes in it, and free speech won out.

Steve: Yes.

Leo: And you've always been able to get "The Anarchist Cookbook." And of course now you can get it on the Internet. So this is nothing new. Governments have been trying to do this forever.

Steve: Right. I guess maybe what's different is, you know, we've talked about...

Leo: We're more scared.

Steve: Well, we've talked about how law enforcement is complaining on one hand that they don't have the access that they want to the communications. But on the other hand, they've never had more access in the history of man to online activities. So I think it's natural for law enforcement to want everything that they can get, and it's probably also useful for there to be a compromise, for there to be some pushback so that it's just not like, I mean, I guess what I'm trying to say is...

Leo: Well, this first part is they want to censor the Internet. They don't want stuff to be on the Internet because you could use it, partly because of maybe bomb-making information, but partly because it would be terrorist propaganda designed to encourage the weak-minded to become terrorists.

Steve: Right. Well, in fact...

Leo: That's government censorship. And in fact, it's, what do they call that, before the fact?

Steve: Oh, wait. Just let me think. It was, well, we're coming to it. Actually it's been called "precrime."

Leo: Yeah, yeah.

Steve: And that's, well, I can't...

Leo: We'll get to it. I don't want to - I'm sorry.

Steve: We'll be getting to it in a second.

Leo: I'll shut up.

Steve: Oh, it's Japan. Anyway, that's next. So the second point you were just alluding to, quote: "Support the efforts of civil society organizations to promote alternative and counter narratives." So they're saying...

Leo: I don't have a problem with that.

Steve: Right. Pull down the bad stuff; put up the good stuff. But then number three is what has been lurking around, and I think it's inevitable: "Work together to ensure our countries can access data for investigative purposes."

Leo: Yeah. This is the snooper stuff.

Steve: Yes. And so we have 3.1 under that: "Seek to preserve the retention and access to traffic and location data. Under current terrorist threat levels, the ability to retain data useful to investigations remains essential." Second point: "Enable subscription holders to be identified in all circumstances."

Leo: Oy.

Steve: So now we're talking about loss of anonymity.

Leo: Yeah.

Steve: They said: "A single Internet Protocol address can be shared between hundreds of users accessing the Internet or social platforms via their smartphones. The capability to identify specific users is important, particularly where suspects have accessed terrorist content." So then they said, under their proposals: "Share expertise and legislative experience regarding these issues, including with Europol, with a view to intensifying dialogue with the industry." So the idea being they're saying now IP address is no longer sufficiently granular because of course everyone behind a NAT or behind a Tor proxy, or any other major proxy or VPN, has their traffic mixed together. So they're beginning to say, you know, we want some way to penetrate identity beyond IP.

And then of course the inevitable 3.3: "Allow access to encrypted content." And they said: "When encryption technologies are used by criminal groups and terrorists, it must be possible to access the content of communications and their metadata. This is not about," they say, "backdoors or banning encryption, but ensuring governments and companies develop shared solutions to this issue." Of course without suggesting how we achieve that miracle. And so they said under their proposals: "Share strategies on the challenge of accessing content from encrypted services, and coordinate our engagement with the major communications service providers."

So here again we're seeing this move towards the ability to move, at least in the U.S., we have a Constitution which protects us against unwarranted search and seizure, so you get a warrant in order to do that. I'll be very surprised if that isn't what happens with the U.S. And then this is a challenge globally because we're all sharing a single big network at this point.

Anyway, the second country, or the third country - that was France and Britain getting together. Last week Japanese Prime Minister Shinzo Abe's government passed a controversial piece of legislation giving prosecutors - get this - the power to monitor and

arrest people in the planning stages of crimes. So this is what some coverage of this has called "precrime."

"After an all-night legislative session in Tokyo, lawmakers, who were deliberately delayed by the bill's opposition, finally voted to pass the so-called 'anti-conspiracy bill,' controversial legislation that gives prosecutors the power to monitor and arrest people in the planning stages of crimes. The government claims this is needed to bolster counterterrorism precautions ahead of the 2020 Tokyo Olympics. Under the bill, terrorist groups or criminal organizations could be punished for the planning of" - and I thought it was amazing that there was a number put on this - "277 different crimes" - apparently they're enumerated - "ranging from arson to copyright violation."

Leo: Uh-oh.

Steve: Uh-huh. "Critics of the legislation argue that the legislation is vague and could lead to the suppression of civil liberties and excessive state surveillance. It's also seen by many as a preamble to Abe's ambition to revise Japan's constitution. Commenting about this, a professor of political science at Sophia University in Tokyo was quoted: 'This fits Abe's agenda in the run-up to a prospective national referendum on constitutional revision and Japan's possible involvement in future wars. Both of these would require new means to control unruly citizens who object to government decisions.'"

So, yeah. And not surprisingly, Russia is moving forward. We discussed, I think it was last year when Russia changed some laws to ban some classes of VPNs. And you'll remember, Leo, that one VPN provider in particular, Private Internet Access, pulled their service from the country after they were raided and had some of their servers seized. So now there's a new surveillance bill in the Russian parliament, promising to deliver "greater security" to the country. But as with so many countries, the bill's effect looks like it's going to do the opposite, mandating new encryption backdoors and imposing new data retention requirements on ISP and VPN providers. So this legislation is expected to take effect in 2018, next year. And the new law - this is a little chilling - would require messenger users, that is, users of messaging apps, to verify their real-world identities using their phone numbers with Russian mobile phone operators.

Leo: Oh, god.

Steve: So you will be [audio dropout] explicitly deanonymized, so you can no longer use anonymous messaging [audio dropout]. Your messaging identity has to be tied to your real-world identity. So something that we've been taking for granted about the Internet and that no doubt a lot of Russian citizens appreciate will become unlawful next year.

And there's also some additional impositions imposed on VPN providers. In Russia, broadband users, as we've been covering, have increasingly turned to VPNs to avoid the growing list of censored websites. To help thwart such usage, the bill would not only impose steep fines on VPN providers who don't agree to block blacklisted websites, but would require ISPs to terminate [audio dropout] of those VPN providers who do not comply.

The legislation reads, quote: "As it stands, the bill requires local telecoms watchdog Roskomnadzor to keep a list of banned domains while identifying sites, services, and software that provide access to them. Once the bypassing services are identified,

Roskomnadzor will send notice to their hosts, giving them a 72-hour deadline to reveal the identities of their operators. After this stage is complete, the host will be given another three days to order the people running the circumvention-capable service to stop providing access to banned domains. If the service operator fails to comply within 30 days, all Internet service providers will be required to deny access to the service and its web presence, if it has one." So within Russian borders, basically they're legislating out of existence some of the fundamental operating flexibility and freedom that the Internet has provided.

And, lastly, Germany. A follower of ours, Ian Beckett, often sends me photos of pages because it's just easier for him to do, and this one is an article from The London Times headlined: "Germany to change law on encryption." And the article reads: "Laws to enable security services to see messages before they're encrypted by providers such as WhatsApp are being drawn up in Germany because of concerns over secret communications between Islamist terrorists. Angela Merkel's government believes that the same balance of eavesdropping and privacy should exist in the digital age as in the analog era of letters and phone calls. Ms. Merkel aims to put digital security on the agenda for the G20 summit that she's hosting in Hamburg next month.

"Theresa May [as we know] has also called for a global approach to regulating digital providers, saying during the election campaign that there should be no 'safe space' for terrorist ideologues. Germany is known as one of the countries most protective of personal privacy because of the legacy of surveillance by the Nazi regime and the Stasi secret police of communist East Germany. However, terrorism in Europe is fueling calls for change.

"British authorities were incensed that they could not access the last WhatsApp message sent by Khalid Masood, the Westminster attacker, minutes before he began his killing spree by driving into pedestrians and fatally stabbing a policeman. The messaging company, owned by Facebook, said that its service" - meaning WhatsApp, of course - "that its service was so secure that no one but the sender and recipient could see a message, not even WhatsApp itself.

"'We want messenger services to have an end-to-end encryption so that the communication of respectable citizens is undisturbed and secure,' said [Thomas de Maizire], the German interior minister. But 'Nevertheless, security authorities need the option of access under certain circumstances.' That would allow the authorities to read a suspect's communications before it was encrypted, he said."

So standing back from all this, we should remember that, as we know, it's in the commercial interests of Facebook, WhatsApp, Apple, and so on to claim that they are unable to read messages because their customers state that they want security. I would argue that evidence suggests that people want it, but they're not that concerned about it. It's like, yeah, if I can have it, that's fine. But if you give me an ice cream cone, I'll tell you my password. So no biggie. But remember that the actual tradeoff for the convenience of users not being burdened with explicit key management and endpoint verification, for example, as Threema requires its users to do, is that any of these providers can in fact tap into their service's communications. So I'm not saying they can do this retrospectively at the moment, though that capability could be added. But we do know that they could do it prospectively, as with a wiretap order, under a warrant.

So anyway, I think that the future is uncertain. But as our listeners know, this is one of the reasons that I stopped work years ago on my own VPN solution, because from our own coverage of what we saw happening it looked like the handwriting was on the wall and that it was going to be impossible to have truly secure communications that were

unbreakable. Which is unfortunate.

Leo: Let me, okay, I'm going to play a little devil's advocate.

Steve: Good, good.

Leo: I mean, is there not a way to balance privacy with security a little bit? So, for instance, there's nothing I'm sending in my emails that really need to be private.

Steve: Yup.

Leo: And if it helped prevent another Westminster Bridge attack to have those rules, wouldn't that be kind of, I mean, there's conflicting needs, obviously.

Steve: Correct. And I agree with you completely, Leo. I use iMessage because I'm sending tweets to my friends about what's going on or, I mean, iMessages to my friends. And, I mean, I understand the position of people who are strongly opposed to any kind of opportunity for surveillance. I mean, I want to respect that. But the fact is, no one using WhatsApp or iMessage or Facebook Messenger, no one using those tools actually has that. So again...

Leo: You're saying that because the companies that make those programs actually could, if they wanted to...

Steve: Yes.

Leo: ...access the communications.

Steve: They are controlling the cryptography and the keys. And iMessage is a multi-way messaging system. So if someone said to Apple, "We must have this communications," then an additional key could be added, and the user would have - it's completely nontransparent.

Leo: However, Signal and Threema and a variety of other apps don't have that flaw and are in fact secure.

Steve: Correct, correct.

Leo: And presumably bad guys know that.

Steve: Well, yes. And notice that in this...

Leo: Although, wait a minute, he used WhatsApp, so maybe he didn't know that.

Steve: Well, precisely. And I would argue that somebody who really cares isn't going to be using one of these easy mass use. Although there was the interesting wording here about "capturing before encryption."

Leo: Eh.

Steve: So that suggests that the legislators have been having hearings and are listening to people saying once it's encrypted, it can't be decrypted. And they're saying, well, how about then before it gets encrypted?

Leo: Before, yeah.

Steve: And we all know, as you're typing it in, and you're seeing it on the screen before you hit Send, it's sitting there in the clear. So, I mean, and this is why we've said on this podcast, the only way to actually have true security is for two naked people to meet in the middle of Central Park under an umbrella, or throw an opaque bag over their head so no one can read their lips, and then whisper to each other. I mean, if you're using technology, it provides lots of benefits. But actual security is an illusion. I mean, absolute security is an illusion.

Leo: And then, on the other hand, you can say, well, the terrorists win because we have decided to abridge our own liberties to protect ourselves. And really, I mean, as bad as this is, the risks of death or injury from terrorist attack are very, very, very small. Vanishingly small.

Steve: Well, and Leo, I would also argue that governments want the ability to eavesdrop.

Leo: For other reasons. Well, you see when they mention copyright; right?

Steve: Right.

Leo: That they're not just protecting us against people who would harm us. They're...

Steve: Well, and how many times have they marched out the child abuse and child pornography? And so the point is some of these things are a means to the end that the government wants.

Leo: That's something you want to watch. They're using fear to further their own agenda which has nothing to do with terrorism.

Steve: Although in the U.S. we have a Constitution that says, if a judge decides that there is probable cause for someone's phone to be tapped, historically law enforcement is able to do that. And I argue I don't think that should change. I mean, to me, that seems like it's a tradeoff that has worked. And the challenge is that doing it without introducing extra vulnerability is tricky. That is, that's why, for example, selectively adding a key to a dialogue under warrant seems like the right tradeoff, where an additional encrypted stream is captured, and only the matching key can decrypt it. That seems controllable. But if a system is in place where it's possible, for example, to put a tap in before the encryption, then you really - that is a backdoor. You really are then opening it up to abuse. And it's difficult for me to see from a technology standpoint how you keep the bad guys from being able to pry that open, too. And so, again...

Leo: That's another issue, absolutely, yeah.

Steve: Let's just move forward slowly on this and hopefully not have some bad legislation occur.

Leo: It's also, you know, possible to get paranoid, over-paranoid about that stuff. For instance, I was really worried about taking a laptop and phones outside the United States, for fear of what would happen as I crossed the border. And of course nothing happened. It was the easiest thing. It took me 15 seconds to get back into the U.S. with my U.S. passport. So, yeah, you know, you can get over-worried about this kind of thing, as well.

Steve: Well, in fact I know that the U.S. saw a dramatic drop in foreign tourorism [sic] during the whole...

Leo: Tourism, not tourorism.

Steve: Tourism.

Leo: I don't want to confuse the two.

Steve: A drop in tourism during the early days of the new Trump administration with the travel ban.

Leo: Right, right, like 17% or something, yeah.

Steve: Yes. Not that people couldn't come in, they just didn't know. And so they didn't want to get on a plane if they were going to be sent home after reaching the other end of

their flight. So exactly as you say, just the uncertainty creates a chilling effect.

Leo: And if I were a brown Muslim, I might have gotten a lot more hassle coming into the country, U.S. citizen or not.

Steve: Sad as that is.

Leo: Yeah, unfortunately.

Steve: So WikiLeaks dropped another blob of Vault 7 leaked documents from the CIA, and we learned last week of a project called CherryBlossom. And it's a little chilling. This is a rather comprehensive WiFi router and access point hacking system, in place and used by the CIA. And I would argue that perhaps the most breathtaking aspect is the breadth of exploitation possible. I have a link to the PDF document of the affected devices in the show notes. And although in the document they're in alphabetical order, I first snapped this that wasn't. But it looks like maybe they're in most popular order: Belkin, D-Link, Linksys, Aironet/Cisco, the Apple AirPort Express, Allied Telesyn, Ambit, AMIT Inc, Accton, 3Com, Asustek Co, Breezecom, Cameo, Epigram, Gemtek, Global Sun, Hsing Tech, Orinoco, PLANET Technology, RPT Int, Senao, US Robotics, and Z-Com, and many models of all of those routers.

As we know, many of these routers share common firmware across their model line, where they just have different numbers of ports and antennas and speeds and things. But the core firmware is the same. And so, I mean, I didn't count the line items. I don't want to say all models of all of these routers, but anyone interested should go look.

With this latest batch of leaked Vault 7 documents are the details of what is basically WiFi device firmware hacking framework, which is being used by the CIA for monitoring Internet activity of targeted systems by exploiting vulnerabilities in these WiFi devices. So this was reportedly designed in a joint effort by the CIA, with the help of SRI International, of all people - I was surprised by that, you know, that's Stanford Research Institute, which is a U.S. nonprofit research institute, I think they're located in Palo Alto - as part of its CherryBomb project.

So CherryBlossom is a remotely controllable, firmware-based implant for both wireless routers and access points, which exploits router vulnerabilities to gain unauthorized access and then replace the firmware with custom CherryBlossom firmware. So the wireless devices are implanted with this custom CherryBlossom firmware. And since many devices support over-the-network updates, physical access is not required. Once implanted with this firmware, these devices then perform, not surprisingly, man-in-the-middle attacks to monitor and manipulate the Internet traffic of their connected users.

So in the documentation, which is extensive here - there's even an installation guide - it states that the CherryTree command-and-control server must be located in a secure, sponsored facility and installed on Dell PowerEdge 1850 powered virtual servers running Red Hat Fedora 9, with at least 4GB of RAM. So the whole toolkit is laid out.

And these compromised routers and access points naturally are able to monitor network traffic to collect email addresses, chat usernames, MAC addresses, and VoIP numbers. They're able to redirect connected users to malicious websites, or non-authentic websites, I guess I would phrase it, to inject custom content into the data stream to

fraudulently deliver - well, now, in the bullet points here it says "malware and compromise the connected systems." I would argue maybe it's "mal" depending upon your perspective. Setting up VPN tunnels to access clients connected to Flytrap's WLAN and LAN for further exploitation, Flytrap being another one of the monikers in this system. And also the ability to copy the full network traffic of a targeted device, essentially exfiltrated to some remote server for later analysis.

So again, what we're seeing here, sort of in all of this post-Snowden era, is that unfortunately our law enforcement agencies have lost control of apparently much of their secret toolset, or at least lost control of the documentation; and that in fact, as I said earlier, the fact that there are WiFi access points and routers, which used to be a rarity, I mean, it was like, well, do you have WiFi? Now you don't even ask the question. You open up WiFi on your phone, and you have to scroll through a list of access points that are within range. So again, it's not like there's a lack of capability and a lack of a target-rich environment for law enforcement to access. And I don't think that's going to change. So it's difficult to see anyone complaining that they don't have the access that they want.

Leo: By the way, Steve, as long as we're talking about Internet access, you are breaking up periodically. Not so badly that I'd want to start over, but every once in a while I get a little blip, a little hit on you. It could be us, could be you, don't know. Don't know.

Steve: And how did that compare to what happened with Renee after about an hour?

Leo: It's very similar.

Steve: Okay.

Leo: And I guess FLOSS Weekly was having problems this morning. So it may well be us.

Steve: Well, and remember - well, remember, too, that Microsoft has redefined the way Skype connects. We used to be able to get a direct point-to-point connection.

Leo: Oh, I know, yeah.

Steve: And they shut that down. We're now routed through Skype servers.

Leo: Huh? FLOSS was Randal, okay. So, yeah. Yeah, it could be that. But the weird thing is, there are some hosts we never have problems with. So I just don't know what it is. I really don't. We've tried all sorts of things. But anyway, just a note.

Steve: Yup.

Leo: Nothing to do about it.

Steve: Okay, so I have this in my show notes: "Why we can't have nice things." And I said: "Or take our nice things traveling with us." We finally got some interesting details about those increasing restrictions which have been imposed on traveling with electronics. And essentially what we learned was that Israeli hackers reportedly got into ISIS networks and found they were building laptop bombs.

Two reporters, David Sanger and Eric Schmitt, reported that top Israeli cyberoperators penetrated a small cell of extremist bombmakers in Syria several months ago, and that was how the U.S. learned that the terrorists were working to make explosives that could pass through airport X-ray machines and other screening by looking exactly like batteries for laptop computers. And according to two American officials that the reporters used as anonymous sources who were familiar with the operation, the intelligence obtained was so complete that it enabled the United States to understand how the weapons could be detonated. The information helped prompt a ban in March on large electronic devices in carryon luggage on flights from 10 airports in eight Muslim majority countries to the United States and Britain.

And of course it was also, unfortunately, part of the classified intelligence that the U.S. President Donald Trump is believed to have revealed to the two Russian officials, foreign minister Sergey Lavrov and the ambassador to the U.S., Sergey Kislyak. It was the disclosure of that classified intelligence that reportedly upset, greatly upset Israeli officials because it revealed the fact that the security surrounding this very small cell of extremist Syrian bombmakers had been successfully compromised, thus putting future intelligence gathering at some unnecessary risk.

So in any event, we now know a bit more about what's going on. And of course, as an engineer who travels with electronics, I've always been a little bemused, you know, because like for years the TSA agents would say, "Turn that on." And it was like, what, really? And the second the screen lit up they would say, okay, that's enough. And it's like, so as an engineer, the whole issue that laptops are a risk if they won't power up, but they're not if they will, I mean, it just never made any sense to me because you'd need to be extremely incompetent and way less technical than anyone you could find to believe that such a weak verification would make any sense. I just don't get that.

And in another little weird anecdote, I last week ordered a high-capacity capacitor. It was a multi-farad supercapacitor. And I didn't note that it had lithium as an ingredient. I ordered it online from my favorite supplier [audio dropout]. And I got a phone call from them saying, "Hey, you know, you asked for this to be sent to you via priority mail, but this has lithium in it." And I said, "It's not a battery. It's not going to explode." And she said, "Well, I'm sorry, but it's got lithium, and you can't send anything with lithium through the mail." And I said okay. So anyway, it's coming to me via, I don't know, FedEx or UPS. Either of those two carriers are able to take it.

So again, this is because the word, it's got the "L" word in it. Even though it doesn't have lithium-ion chemistry, it still spooks people, and so we're being put through unnecessary inconvenience as a result. Although I'm not saying that lithium batteries don't explode. They do. But lithium capacitors do not.

Okay. So earlier this year, it was in April, actually, couple months ago, we talked about the serious problem with printers, that in this case it was HP printers that are widely distributed around the globe and had some unknown vulnerabilities that HP was fixing in

a firmware update. There was no information, no additional background about that. But after HP's detail-lacking April security bulletin, some guys at the security firm Tenable decided to take a closer look under the hood of HP printers. So they purchased a pair of HP OfficeJet Pro 8210s. They bought two so that they could leave one without updated firmware, and then update the firmware of the other one, and then do some comparison.

Well, it turns out that - get this. In the printers, auto-updating of the firmware was disabled by default. So immediately that suggests that most users of HP's printers that have been known vulnerable since April, and now we have a complete disclosure as a result of this research, will not automatically receive fixes for the problems that have been found. We'll have a takeaway for the listeners of this podcast in a moment. But I took a screenshot from Tenable's reporting, showing that the firmware in one of these printers was dated April 28th of 2016, so a year old. And also showing down at the bottom "Do not check for updates" is the default setting. So that means that, globally, assuming that this is the default setting for HP printers, at least of this firmware family, which we can assume, these machines will never be updated unless users are proactive, which is what I hope our listeners will be.

So the Tenable guys manually updated one of the two identical printers' firmware in order to have, as I mentioned, both before and after patched images. But it turned out they didn't need that. They first used NMAP to scan the printer for open ports and found an unsurprising set of ports - 80, 443, 8080, and 9100 - 9100 the so-called "JetDirect" port, which turns out to be hosting many problems. And it is present on all HP printers. It's sort of the default means for the HP printer driver to talk to a networked printer.

So by using a PC-based instance of the very powerful netcat utility, they experimented connecting to port 9100 and sending a bunch of different commands in. And one of the things they played with was the old-school path traversal exploits, where you prepend a directory list command, for example, with /../../.., the idea being that, if a server isn't protected against that, you're able to walk back to the root or upstream of the directory which is your normal logged-in directory for that service, essentially in order to escape from what weak containment that server provided. So by doing this they were able to explore within - and this is all [audio dropout] over the network. They didn't have to open anything up or pry any chips loose or anything. This is just talking to port 9100. They found the linux/bin directory, demonstrating that it's possible to traverse into that printer's Linux directory.

Okay, then, using three PJL commands - this port 9100 supports several different protocols. One of them is called the Printer Job Language. And there's an FSQUERY, FSUPLOAD, and FSDOWNLOAD command which provides them with read/write access to the printer's file systems. So then they demonstrated that using two of those, FSQUERY and FSUPLOAD, combined with a directory traversal, they're able to retrieve the contents of, for example, the printer's /etc/password file. Which is, again, another standard Linux component. And then, by using the FSDOWNLOAD command, they discovered that, after they had surveilled the exposed file system, they were able to add a static invocation of the netcat command upon boot-up.

Okay. There's no reason that printer firmware should have the netcat command in its binary directory except that someone just didn't care. They just took a standard Linux build and put it in this printer, which is insane because with netcat you can, I mean, there's no purpose for the developer to use netcat. Maybe it would use it with a script to go fetch firmware updates. But that's lazy and sloppy because netcat is, as I mentioned before, a very powerful tool, which among other things allows you to create servers, sort of ad hoc servers, just from a command.

So they added to the startup script an invocation of netcat that would create a fully remotely accessible command shell on any available port of their choose. So after doing that, they then rebooted the printer. It came up, ran the startup script. Netcat was launched, listening for incoming connections on the port of their choosing, which would then allow anyone that knew where the port was to remotely connect to and have full shell access to the printer.

Now we know what was found two months ago, and we know that the world is full of remotely network-exploitable HP printers containing seriously vulnerable and exploitable firmware, which HP has no ability to remotely update, assuming that the default across a large population of those printers is the same as it was in this case, which is it will not update its firmware by default. Which means that this install base of printers makes perfect hosts for the insertion of advanced persistent threat malware within both consumer and enterprise networks. So if our experience teaches us anything, we know that these highly vulnerable printers will continue to exist on networks forever until they finally die and are decommissioned. But to the degree that they are alive, they will never go away.

Leo: And they could be used to, what, spread malware? What kinds of stuff?

Steve: Well, they could be used as a persistent outpost for any sort of threat actor. For example, it could reach out from inside the network to establish a connection to a remote server [crosstalk]...

Leo: So in a foreign country don't, "Thank god, an HP printer." Somebody could compromise it and then have full access to our network, essentially.

Steve: Correct. And persistent access. That is, even if you shut down all the power and then brought it all back up again, this thing would come back up and reinstantiate itself and reconnect to the remote command-and-control server.

Leo: It's all the Jetdirects?

Steve: It's, I would say - so the takeaway for our listeners is everyone within range of this podcast should proactively update any HP printer firmware within their control and responsibility as soon as possible.

Leo: Ugh.

Steve: So just fire up the printer manager that gets installed when you install an HP printer and just go and update its firmware.

Leo: Has HP pushed the update?

Steve: They can't because the...

Leo: No, but, I mean, but if you asked for it, there is a fix?

Steve: Yes, yes, yes. For the last two months.

Leo: Okay.

Steve: And this is the problem is the printers aren't updating themselves.

Leo: They're not updating; right.

Steve: And so the printers in the closets, the printers next to the water cooler, I mean, again, our listeners need to update their HP printers. But unfortunately, not everyone listens to this podcast. And there's going to be just a massive install base of HP printers.

Leo: We know the NSA will be safe, and that's - thank god for that.

Steve: Ah, yes, we do.

Leo: Update your printers, gentlemen.

Steve: I'm sure they are. GitHub hosted a fun analysis. They took the top 32 million passwords and ran some analysis of them. I have [audio dropout] in the show notes and a link to the GitHub page that has two additional graphs. But this is fun. So this is the distribution of password population by length. So, for example, and I don't even know who has a four-character password, maybe that's a PIN, but 0.265% is four characters. 0.612% is five. 2.47% is six characters. Fewer, 2.06% is seven. Okay, then the big one.

Leo: We like even numbers.

Steve: More than any other. Huh?

Leo: We like even numbers.

Steve: Is eight.

Leo: Yeah.

Steve: Oh, you might be right, is eight, which is 23%. So 23% of the top 32 million passwords which were analyzed from this repository had eight characters. And then the

chart just sort of falls off from there: 16.74% have nine characters; 16.16 had 10; 11 characters were 12.89; 12 characters was 10.68; 13, 7.68; 14, 4.66. So now with 14-character passwords we're down to less than 5% of them. Impressively, there were some 15-character passwords. Now, these are LastPass users or 1Password or, you know, something...

Leo: Yeah, I do like 20 if I can, 24, 38, 70.

Steve: Exactly, exactly.

Leo: You have 64-character passwords.

Steve: But still, 17 characters is as far as this goes. And so we're back to 0.26%. And as we know, unfortunately, there are many sites that will say, oh, sorry, you can't use more than 15. And so it's not surprising that there are not that many that have such long passwords. But so basically the sweet spot, such as it is, is eight characters. And what this does tell you, you have to know that anyone brute-forcing is - because remember, all you get is a go/no go after you try, after you make a guess at a brute-force password. So the brute-forcing people know this distribution well. And that means they're going to focus on all possible combinations of eight characters as their first choice, and then go to nine, 10, 11, 12, 13, and so forth. Which does not suggest that you should use four, five, six, and seven characters.

Leo: No.

Steve: Because it just takes no time to blast through the total possible brute-forcing of such a small number of characters per password. So it's certainly the case that longer passwords are better. But it's interesting that almost a quarter of all passwords are eight characters.

Leo: Did you see the next chart? Nearly 90% of the passwords used only lowercase letters and numbers.

Steve: Yup.

Leo: So you want to help, put a little punctuation in there.

Steve: Just throw a little something unexpected in there.

Leo: Right. Hit the shift key.

Steve: Makes a big difference, yes.

Leo: Yes, hit the shift key. Adding a single special character to a password composed of lowercase letters makes it theoretically 15 times less common. So there.

Steve: Nice.

Leo: That's where LastPass really saves you.

Steve: Yeah, it does. So, okay. We all know that the WannaCry worm malware - oh, and by the way, the creation of that has recently been attributed to a cyberwarfare group operating out of North Korea.

Leo: Ah.

Steve: So attribution is always difficult.

Leo: That's what we thought.

Steve: Yup, attribution is always difficult, but that's where things are pointing. So WannaCry leveraged the no longer, and I would argue not for a long time, mainstream, hasn't been mainstream, v1 of Microsoft's Server Message Block, the SMB, also known as Samba, protocol. And we also know how difficult it has always been to remove support for legacy protocols because there's always something somewhere that is no longer supported, cannot be updated, is mission critical, and only understands the legacy protocol. Thus these things tend to never die unless they're just forced, finally, to die. Microsoft has finally stated that, finally, in the future, even though they've been trying for five years, they're going to disable the support for SMBv1.

Ned Pyle, who is the principal program manager in the Microsoft Windows Server high availability and storage group, told the guys at BleepingComputer that plans to disable SMBv1 have been in the works at Microsoft for the past five years. He said that the security issues of SMBv1 were the main factor in deciding to disable the protocol - yeah, after WannaCry forced you to back-patch Windows XP - but the fact that SMBv2 was released nine years ago was also a factor. Meaning that we've already had the successor for nearly a decade. Pyle also said Microsoft would prefer everyone use SMBv3, which is five years old, released in 2012, as the standard.

As we have similarly seen, for example, with the earlier insecure SSL versions, if SMBv1 is available and enabled, even if it's not in common use, if it's available and not disabled, attackers can force a downgrade. They can perform a so-called "downgrade attack" from the use of the newer and improved protocols to the known-exploitable protocols. Remember that one of the reasons we finally shut down all earlier use of SSL in favor of TLS was that, for a long time, for the sake of backward compatibility, even though we had newer versions of our secure HTTP tunnel protocol, TLS, servers still supported SSL. But when offered a choice, clients were able to say, oh, no, no, we don't know the new stuff, in order to force a downgrade to the use of the older and typically less secure fallback protocol, and thus subject servers to victimization through their willingness to

support the older protocol.

So anyway, given that running SMBv1 is no longer necessary for modern enterprise users, and having it around opens up a significant security vulnerability, this Ned Pyle says it's time for it to be put to rest. He claimed the ubiquity of SMBv1 had made taking action more difficult. But he finally confirmed that, when Windows 10 Redstone 3 is released, both in the user and the server variants, SMBv1 will be disabled by default for the first time in Microsoft's history, since it was created. And we've had file and printer sharing since, what, Windows 3? I mean, it's like, it's always been there. So, yeah, sayonara. And good riddance.

Leo: Yeah.

Steve: Oh, my goodness. And the biggest ransomware payday of all time. A South Korean web host named Nayana, N-A-Y-A-N-A, was hit by the Erebus cryptomalware. Although Erebus was originally targeted only at computers running Microsoft Windows operating systems, it was later modified to work against Linux systems. Now, it's unclear how Nayana became infected with Erebus. But an examination of the largely unpatched software the web hosting service appeared to be running allowed Trend Micro to presume that the attackers exploited a well-known vulnerability.

Trend Micro wrote: "As for how this Linux ransomware arrives, we can only infer that Erebus may have leveraged vulnerabilities or a local Linux exploit. For instance," they wrote, "based on open source intelligence, Nayana's website runs on Linux kernel 2.6.24.2, compiled back in 2008. Security flaws like Dirty COW," they wrote, "that can provide attackers root access to vulnerable Linux systems, are just some of the threats it may have been exposed to.

"Additionally, Nayana's website uses Apache v1.3.36 and PHP v5.1.4, both of which were released back in 2006." So both 11 years old. "Apache vulnerabilities and PHP exploits are well-known; in fact, there was even a tool sold in the Chinese underground expressly for exploiting Apache Struts. The version of Apache Nayana used is run as a user of nobody," which is the UID 99, the nobody user, "which indicates that a local exploit, and subsequent privilege elevation, may have been used in the attack."

Okay. So now, as for the ransom paid to obtain the decryption key for essentially their entire enterprise, the fee was high due to the fact that all of the data stored on 153 Linux servers and 3,400 customer websites had been encrypted. Nayana's own blog posting stated that the initial ransom demand was for 5 billion won worth of bitcoin, which is roughly $4.4 million U.S. Company negotiators later managed to get the fee lowered to 1.8 billion won and ultimately landed a further reduction to 1.2 billion won, or just over $1 million, which ransom they did pay.

In an updated post last Saturday, the Nayana engineers said they were in the process of recovering the data, cautioning that the recovery was difficult and would take some time. So a $1 million bitcoin ransom payout, a big payday for the ransomware people. And that's the sort of news you don't want to see going widespread because that really paints a big target on any other hosting providers whose security may not be up to par <shudder>.

I did want to note that Google Drive is adding a feature which, as I mentioned at the top of the show, does not compete, completely at least, with the feature set offered - actually its minimal feature set does not compete with the feature set offered by

Carbonite. But the Google blog states that on June 28th - which is, what, Wednesday a week from tomorrow - they said: "We will launch 'Backup and Sync from Google,' which is a new tool intended to help everyday users back up files and photos from their computers, so they're safe and accessible from anywhere." Which is a little bit of an oxymoron, but we'll discuss that later. "Backup and Sync is the latest version of Google Drive for Mac and PC, which is now integrated with the Google Photos desktop uploader."

So essentially what this does is I have a picture of the UI in the show notes, which shows Desktop clicked showing that this particular desktop had 220MB on it; the Documents folder checked, and it had 712MB in this instance; the Pictures folder checked, and it had 2.2GB; and the Photo Library under that had 1.9GB. And so this Backup and Sync tool will replace the current Google Drive uploader client for Mac and PC and will also be integrated into the desktop Google Photos uploader.

And so what's different about this is, if anyone has used Google Drive, rather than creating new Google Drive folders on a user's system, the tool allows users to select the standard system drives that their system already has - Desktop, Documents, Pictures, Photo Library and so forth - and then it will clone those chosen folders up to Google Drive and then keep them synced. So the system is targeted toward, I would argue - because this will not recover a crashed system. So it's targeted toward more typical consumers who just want a backup solution for a limited set of the system's entire content, and typically just their own work product because, as we know, Google gives you 15GB for free. So if you have your typical storage on lots of machines, you will overflow that quickly, and then you would need to augment the free storage provision and start paying Google for the privilege of having all of this content synchronized. But so it's a nice step forward. And in eight days that should go live.

Leo: Kind of like iCloud. But it does have that advantage. I'm trying to think, there's not a lot of services like this that let you choose the folders. OneDrive, iCloud, and Google all use their own kind of special Dropbox, special folders. It's kind of nice.

Steve: Yeah, as long as - from a security standpoint, I'm nervous about synchronizing to a cloud provider where I'm not providing, I mean, this is - we originally coined the phrase TNO. And PIE, Pre-Internet Encryption, where we're encrypting our contents, and that encrypted blob is then being sent. I mean, there are problems with doing that in a bandwidth-friendly fashion, which is why Google's able to do this. That is, the initial cloning would require a large transfer of data. I'm sure they're compressing and doing smart things [audio dropout]. But then they are just able to do incremental maintenance of that blob by looking for changes.

But again, I would say to users who are thinking about this, don't put the keys to the kingdom in there because we don't know how safe this ultimately is. I mean, we're sure Google is good with crypto and doing what they can. But again, you're trading convenience and not having to deal with this yourself for absolute security. I'm not using it for my stuff, but I could see that it would be very useful for casual users who want to be able to synchronize the major folders where their own work product is, their documents and the desktop. There I think it makes sense.

Leo: All right, Steve. We've still got - we've got a ways to go. I'm looking at your show notes. We've got business to do still.

Steve: Oh, we do. This is from the "but of course it is" department.

Leo: But of course.

Steve: PC Magazine reports that it's possible and fairly easy to hack a PC with a vape pen.

Leo: Now, that's just weird.

Steve: So, well, and in retrospect, it's not surprising. Researchers at a recent London security show warned and demonstrated that USB-rechargeable e-cigarettes could be modified without much effort to infect a victim's PC with malware.

Leo: Do you mind if I charge my vape pen in your PC? I just need a few minutes. It'll charge really fast.

Steve: Let me take a hit off your PC; then I can take a hit off my vape pen.

Leo: Wow.

Steve: So remember, as we've covered here in the past, a USB device is automatically registered either as a USB keyboard, or I should say can be automatically registered as a USB keyboard or, more cleverly, as a network adapter which, when it is enumerated by the USB system, will be queried for its DHCP configuration information. That allows it to declare itself to be the system's network gateway and thereby reroute all subsequent network traffic through itself.

So our podcast followers should already be highly resistant to allowing anyone to plug anything into their machines' USB ports, but enterprise environments may have less control over such interactions. So the takeaway here is that any USB thingy, no matter how apparently benign and innocent, could be exchanging more than USB power with any USB port. And as we know also, the solution, if you must "charge," is a USB condom.

Leo: I carry it with me everywhere, yes.

Steve: Yup. It's just so easy and simple. I like this one, the, what's it called? It's called the PortaPow, P-O-R-T-A-P-O-W. It's a little red plug. It comes in a two-pack. And so if you have that around, and someone wants to stick their vape pen into your machine, you say, uh, hold on a second, let me just slip this little condom over your vape pen, and then they're welcome to suck power. And this thing protects the data because only the - a USB is a four-wire interface. It's got ground, it's got 5V power, and it's got a send and receive, send-and-receive lines. So two of the four just are terminated in the condom so that only ground and power are able to go through.

Leo: And knowing you, you took this thing apart to verify that; right?

Steve: Yup.

Leo: Because people are going to say, well, who are these PortaPow people? Why should I trust them? Because Steve took it apart and knows that only two of the lines are connected. Why did I know that you did that? I just knew you did that. That's great. Well done.

Steve: Okay. So a bit of miscellany, and then some "closing the loop" feedback with our listeners. Last week I tweeted what I thought was a very on-point and humorous video about the problems of using chip cards. And my tweet said: "It's unfortunate that this humorous video about using chip cards is not that much of an exaggeration." I mean, there was some exaggeration there; but again, my own experience in the U.S. allowed me to relate to this.

Now, I wanted to follow up and just mention that the majority of responses from my Twitter followers, who are mostly Security Now! followers, was, "What? Huh? Chip-and-pin works great here. What's wrong with the U.S.?"

Leo: Yeah. Because we don't use chip-and-pin.

Steve: Exactly. Which was interesting to me since my experiences, as I've said, have been largely similar to those in the video. So the conclusion would be that U.S. implementations, because they're new and kind of not yet ready for primetime, are much more finicky than in those countries where credit card chips have had a lot of time to mature. Because, I mean, I see, for example, many chip-enabled machines do not yet accept chips. So you'll see one that's got the slot, and you stick it in, and then the person says, "Oh, no, no, you have to swipe." It's like, oh, okay, fine. And, I mean, sometimes there's duct tape over the slot. Or you'll try to swipe the card, but then they go, "Oh, no, no, you have to use the chip if you have one." It's like, okay, fine. And lord help you if you insert the card before you're told to.

Leo: You've got to leave it in there and, oh, man.

Steve: Yeah. Or if you take it out, like, and it takes a long time in the U.S.

Leo: Mm-hmm. It's a lot longer, yeah.

Steve: It's like, what the heck is going on? And what's really sad is that what we also know is that this doesn't actually provide measurably more security.

Leo: Why not, Steve? Why not?

Steve: Are you watching the video?

Leo: I'm watching the video, yeah, yeah, yeah.

Steve: Yeah.

Leo: She's having all the problems you would expect, yeah, with one of these things. [Crosstalk] follow Steve's Twitter.

Steve: For anyone who doesn't follow, I've got the link to the YouTube video in this week's show notes. And it is pretty funny. But I did want to - I wanted to acknowledge all of our international listeners who think that there's something wrong in the U.S. You're right. There's clearly something wrong over here. We haven't figured out how to do it.

Oh, and this week's Darwin Award winner: NBC, actually, I noted from my - I used to be in Northern California. So KRON is the local NBC affiliate station.

Leo: Not anymore. You haven't been here in a long time. They were.

Steve: Ah, okay.

Leo: Now they're just independent.

Steve: So anyway, they carried the story of a group of not-too-clever thieves who stole a bunch of GPS tracking devices from a tech manufacturer. But they were not too difficult to track down.

Leo: Why is that, Steve?

Steve: Because they were GPS tracking devices that they stole.

Leo: So they just followed the device and...

Steve: That's right.

Leo: Yeah, yeah.

Steve: I have two short, fun notes about SpinRite.

Leo: Actually, it is from an NBC affiliate, not KRON, but WCMI TV Columbus.

Steve: Oh, interesting. Maybe it was picked up...

Leo: Now maybe they [crosstalk] KRON.

Steve: I think it was...

Leo: That's what it was. I see KRON on it. Yeah, yeah, yeah.

Steve: Right.

Leo: That's funny. Okay.

Steve: So anyway, yes, the Darwin Award winners. Do not steal something that can track you after you have stolen it.

Leo: Whoops. Whoops. Whoops.

Steve: That's not good.

Leo: $18,000 worth of GPS tracking devices.

Steve: So, yeah, I think that you don't want to steal trackers because trackers are trackers.

Leo: They put it in a storage locker that contained a lot of other stolen stuff, including drugs. So we won't...

Steve: Doh.

Leo: ...be seeing much of them for a while.

Steve: So James Mudd, who is in Oxford in the U.K., said hey. He said: "Hi, Steve and Leo. I really enjoy the podcast and look forward to it every week. I've been listening for years and just started listening again from the beginning." Well, you have 617 episodes to catch up on.

Leo: That's a lot of listening.

Steve: He says: "I often SpinRite drives," which of course is a verb now, "before moving them between systems and formatting them. So I have a question. Is it better to SpinRite the drive, then format? Or format first, then SpinRite?" He says, "I usually SpinRite first, somehow feeling that having data on the drive is better. But logic tells me it shouldn't make a difference." And James, I would agree with your logic. I thought about this for a while, but I just really - I can't see either way. I would say go for convenience. If it's, for whatever reason, easier to SpinRite it where it is before you move it, then do that. If it's easier to SpinRite it after you move it and establish it and format it, then do that. So I would opt for whichever just makes the most sense from a convenience standpoint. Logistically, or in terms of what SpinRite's doing, it doesn't matter at this point.

And secondly, Matthew Norton in Northwest Indiana. Now, I don't think that SpinRite can take credit for every miracle which is coincident with its use, although we do see it often doing things that are unexpected. In this case, the subject was "Another random thing that SpinRite fixed." And he wrote: "I'd been having an issue with my NumLock not turning on when I booted my computer, even though it was turned on in the BIOS and in Windows. I did a SpinRite check of my drives, and ever since then the NumLock has turned on at boot. Thanks for the great product. Eagerly awaiting SpinRite's future. Thanks for the podcast. I've been listening since Episode 1." Now with NumLock. I can't explain that. I mean, maybe...

Leo: You fixed his NumLock.

Steve: Maybe. Maybe something about the way the system was booting, there could have been a little glitch in the boot process that clicked the NumLock off. Who knows? But Matt, I'm happy that SpinRite was up to the [crosstalk].

Leo: I think you should put this on your website in your ad copy.

Steve: Not guaranteed to fix NumLock.

Leo: No, but might.

Steve: But you never know.

Leo: Might fix your NumLock, yeah.

Steve: You never know.

Leo: I think that'd be a good name for SpinRite 6.

Steve: If your Lock is Num, then this will fix it.

Leo: Right.

Steve: So a couple feedback from our listeners. Dan Sidor asked, he said: "Ubiquiti EdgeRouter X looks great. Do you also have experience with their UniFi access points?" And I wanted to remind Dan that, yes, the Ubiquiti EdgeRouter X looks great. But we recently covered the fact that all of - unfortunately all - of the Ubiquiti wireless products did need to get their firmware updated because there was a recent exploit that affected them all. The good news was it did not affect the wired routers, which we like and have been actively suggesting our listeners use. But all of the various wireless ones did have that problem. So I would, I mean, their hardware is nice. I know that you've been, at some point, Leo, you were a Ubiquiti WiFi user, I think; right?

Leo: No, I never used their WiFi.

Steve: Oh, okay.

Leo: But they were like the first to do mesh. It was a commercial version.

Steve: That's right.

Leo: And it required - we might have tried it here. It required at the time, no longer, a PC running Java to control it.

Steve: Oh, lord.

Leo: Yeah. They fixed that. And actually they make - Ubiquiti now makes a wireless WiFi system called the AmpliFi that I have used, just briefly, for review purposes.

Steve: I like their naming - UniFi, AmpliFi, Semper Fi. It's like, okay.

Leo: Semper Fi. Burke says we did try it at the Brick House. But I think we ended up using Ruckus equipment, I believe, is what we use here.

Steve: Anyway, so Dan, I would just say proceed with caution. Make sure that the firmware for it has been updated in the last couple months and that you're running that updated firmware because we were watching them at the time, and they were a little slow in reacting. And so it was like, ooh, I hope - I was hoping it wasn't going to be affecting the wired products also. So there's a bit of a caution there.

And then "Kevn" tweeted: "What was that switch/router you and Leo recommended a few months back?" And there it is, the Ubiquiti EdgeRouter X. And I think I've got it

linked to, in the GRC Linkfarm, if you just put "linkfarm" into Google now, for me at least the first link that comes up is GRC. And I think I've got a link there to it.

Leo: And it's not wireless. It's a $50 just six-port simple little switch and router with a lot of sophisticated software.

Steve: Yes.

Leo: It's very cool.

Steve: What I like about it is that, whereas our typical router has a router core connected to a switch, which creates the ports, like if it's a four-port router or a five-port router, where there's one main port, like a WAN port, and then four LAN ports, normally the typical router is a switch that runs the four LAN ports. This router has individual interfaces, individual network interface controller (NIC) interfaces per port. And that allows you to give each port its own IP range to block the interacting traffic among ports. And there's a lot of power in the UI, even more power at the command line, that really allows you to do things like create an IoT segmented network and really get lost in feature land. So a very neat little router. And again, 49 bucks, and it's cute. Even Elaine got one because she's been listening to this podcast and wanted to improve their security.

So the last couple weeks [audio dropout] talking about SQRL. And it was in the context of various discussions about two-factor authentication and so forth. And I got some feedback over in GRC's Security Now! newsgroup saying, okay, Steve, enough about SQRL. So I wanted to recognize that feedback and assure people that this is not going to become the SQRL podcast. But at the same time, as a consequence of my talking about it, it did raise a couple questions, that I want to answer briefly, from our listeners.

One question asked: "Are there any safeguards in SQRL against DNS spoofing?" And the answer is yes. When I was talking in the last couple weeks about the increased emphasis we have just put in the last month, it's what I've been doing, essentially, is bringing the so-called CPS, the Client Provided Session, bringing it to the forefront and making it a mandatory feature. It absolutely protects against DNS spoofing attacks when you are using SQRL on the same system you're logging in. That is, remember, you could either use it in the same-device or cross-device login. So yes to DNS spoofing.

And then another question: "If the malware has taken control of your DNS, would your mitigation on man-in-the-middle attacks still work against SQRL?" And again, yes. So we are safe against any kind of DNS attack as a consequence of the way this works.

Another listener asked: "Listened to last SN podcast about dynamic pass and two-factor authentication spoofing." He said: "One more reason to use a password manager. It will not recognize wrong address." And to that I respond, true, but password managers will be completely fooled by DNS spoofing attacks. So as I noted in the previous two questions, SQRL cannot be, but password managers will be. So if you go to the legitimate-looking website with a URL domain that exactly matches what the password manager shows, your password manager will populate those fields. But if your DNS has been intercepted and spoofed, you could be taken to a different physical server than where you believe you're going, and your password manager will populate the fields. And script running on the page, as we have already seen, is able to immediately capture that

information, so could steal your identity for that site.

And, finally, Chris Taylor asks: "Could a hacker kill SQRL localhost port and run their own hijacker?" And the answer is yes, absolutely. One of the things that it is important to understand is the attack environment. And there is absolutely no practical protection for a system that has malware on it. And to believe otherwise is just fooling us. Windows is not a secure operating system. None of our PC operating systems are sufficiently secure to allow us to create software that malware running on that machine cannot subvert.

So I did not intend to suggest that anything that we're doing here is proof against a local compromise of the system. There just is no known for any of this technology. But the big attacks are the network-based attacks, something remote, a website losing control of their database, of user accounts. Or DNS spoofing or man in the middle or anything remote network. And for all of those we have that nailed, but not for local. And nobody does. I would argue it's not possible to protect against a local, essentially an internal attack.

Someone whose handle is Le French Fab said: "Hi, just listened to SN-616." So that was last week. "Do you think Apple's two-factor authentication is in any way better than the way used by Google/Microsoft? Thanks." And I thought about that, and I think it is. Whereas the other companies are forced to use text messaging through the mobile cellular text system, Apple has the significant advantage of having their own proprietary, closed, and encrypted messaging system in the form of iMessage, which allows Apple to get those second-factor tokens to their intended recipients without fear of man-in-the-middle or other on-the-fly interception. So it is a significant advantage.

Again, I still would argue that the use of TOTP, the time-based auth-style authentication, is by far more secure. But if you need a per-authentication transmission, then Apple's ability to send that to you through their own encrypted proprietary messaging platform makes that much more secure than having it go and be received as a text message over the cellular system.

Leo: Although what happens if it's your first Apple device, or you don't have any other Apple devices? Because it uses another Apple device to authenticate. What if I buy an iPhone, I don't have a Mac or an iPad?

Steve: So it doesn't send it to the same device? The one that you've got...

Leo: Well, that would be dopey. Oh, let's authenticate you on this device. Here's the code. Why bother? No, it doesn't send it to you on the same device. It sends it to you on another Apple device. I presume that they then offer it via text or some other...

Steve: They must, yes.

Leo: ...bad channel.

Steve: In order to get you bootstrapped the first time.

Leo: Yeah. It relies on you having a bunch of Mac or Apple products. It's very typical.

Steve: Yeah. And in fact that's what happens for me is when I'm - in fact, it just happened when I was setting up the new iPad Pro, is that it said oh, you know, and I got little pop-ups everywhere saying that I was using my identify on a new device. It's like, yeah, okay, fine.

Leo: But they do make you turn it on now, which you've got to commend them for that.

Steve: Yeah.

Leo: You have to use two-factor now.

Steve: Oh, Bill sent a tweet saying: "Yesterday" - I thought this was a great question. "Yesterday a friend was asked by TD Bank if they could keep the recording of her voiceprint for security purposes." And he asks...

Leo: Hmm. Schwab does that, too. They have voice identification login.

Steve: And he asks: "How unique is it?" And my response is, okay, it's not unique enough to be the sole identifier. But it is good as an additional factor.

Leo: Right.

Steve: So like a PIN, you know, a PIN can't identify you uniquely. But it can be - it's a valuable additional - it's a disqualifier if it doesn't match. And so if someone is pretending to be this friend of his, and it's a gruff male voice, it doesn't even - it's not even in the ballpark of sounding the same. It's like, uh, we aren't really convinced that's you. So I think...

Leo: Yeah, it's me. I have a cold.

Steve: Absolutely valuable as a disqualifier, but not as a qualifier.

Leo: My mom, and I don't know how Schwab does it, but they said, "Can we do voice authentication?" And I just said, "Don't do it, Mom. I don't know what they're doing." But you're right. If it was a second factor, that'd probably even be better than texting you a number; right?

Steve: Yup.

Leo: Yeah.

Steve: Again, as a disqualifier, but not a qualifier.

Leo: Right.

Steve: I think that makes a lot of sense.

Leo: Let me in. Hey.

Steve: And again, not perfect because you could imagine surreptitiously recording a sample of the person's voice saying something that you want. And in fact we were talking a couple weeks ago that we're now seeing AI-ish software that can listen to someone talk and then synthesize them saying anything that you want them to say. So it's getting very spooky out there.

Leo: What about people like me, whose voice is all over the darn place?

Steve: Yes, you're hosed, Leo.

Leo: Okay.

Steve: We can't ever believe anything we hear someone claiming that you said any longer because the software is out there to synthesize it. And me, too, for that matter. With 616 podcasts, I've probably used every word in my vocabulary.

Leo: Exactly. There's no word they can't duplicate.

Steve: So listener Ian Beckett, who's often tweeting, said: "Tell me why every password interface doesn't have a 'three times and you're locked out for X hours' as standard?" Well, and of course we know the answer to that.

Leo: Because people get locked out.

Steve: Yes. People are like, uh, which password did I...

Leo: No, it's monkey1234.

Steve: Wait, did I use my sister's name backwards last time?

Leo: Yeah.

Steve: And unfortunately it would just be a nightmare for customer support. I will mention that GRC's email server has a zero tolerance guessing policy.

Leo: Oh, I like that.

Steve: After I watched spamming servers connect up and just run through a ridiculous list of names, I implemented some technology where one single mistake, and that attempted connection is blacklisted for quite a while. In fact, we've never had any problem with receiving email. As long as you send it to an account that exists, it comes right through. But if you're a spammer, and you're just hooking up and guessing, sorry, that's just not going to work for you. So there are places where that kind of "one strike and you're out" policy can work; but, unfortunately, not in the password space.

Leo: A company that I still work for has - I don't want to give away any secrets. But a company that I still work for requires every three months training in FCC rules. And I have to log in, but they change the password every two months. So that means I never actually - because I don't ever use it otherwise, I don't actually know my password ever. And now I guess they're so strapped for tech support people that when you go online, and you call the tech support to reset your password, they say, "If you're calling to reset your password," which obviously is a common practice, "use our online service." Except that the online service doesn't seem to know who I am. So it says no, there's no user by your name. So I don't know what to do. Geez, Louise. Anyway, this is a problem. And we've already said changing your password by a calendar is not more secure, it's less secure; right?

Steve: And the good news is that the NIST guidelines were finally revised to state that.

Leo: Hallelujah.

Steve: So with any luck, that'll percolate out into the IT space. And it used to be that no one could get fired for choosing IBM, even after they stopped offering...

Leo: It's more secure, boss.

Steve: Yes. And so now no one can get fired for following the official NIST guidelines...

Leo: Good point.

Steve: ...which now state there is no security benefit, and it reduces security for

compulsory password change for no reason other than, oh, it's been a while.

Leo: Well, if they had any IT people, I could tell them. But apparently there's no one there. So I'm kind of, you know, I'm kind of stuck between a rock and a hard place. I can't actually get into my account, and there's no one there to help me.

Steve: Wow.

Leo: Yeah, yeah. It's just - but you nailed it. It's support costs that everybody's really concerned about; right?

Steve: Right. Right.

Leo: That's the ultimate issue.

Steve: So David Benedict took a little exception, I think, to my being harsh with Google and Android about Google's official policy that the "draw over" problem would not be fixed. And he raised a good point. He said: "Google not fixing does not mean they won't scrutinize apps more than before." And I would imagine, in fact, they will increase the depth of their app scrutiny in order to prevent abuse of draw over. So David, that's a very good point. Thank you for bringing it up.

And lastly, this week's laugh-out-loud tweet, courtesy of a retweet from our listener Morgan Speck. He retweeted Lesley, whose Twitter handle is @hacks4pancakes. She tweeted, or he tweeted, I don't know if that's, I don't know, Lesley said...

Leo: That's a man's spelling, L-E-S-L-E-Y. So we'll say it's a guy, yeah.

Steve: Okay. He tweeted: "Personally, I think this Windows 7 thing is overhyped, and I shall be switching back to XP since it has a regular security patch cycle once again."

Leo: Sounds like you, Steve.

Steve: Last couple of months, Microsoft has been updating XP every month, so let's all go back.

Leo: Were there more than just for WannaCry? There've been some other patches?

Steve: Yes, the last two, the last couple months. And then there was an emergency out-of-cycle patch also.

Leo: Wow.

Steve: So, yep, we're getting our XPs all updated, thank you very much.

Leo: I think we should send @hacks4pancakes some pancakes for that tweet.

Steve: And as they say, Leo, that's the show.

Leo: It's a wrap, ladies and gentlemen. Steve Gibson, he's at GRC.com. That's where you can find information about SQRL. You were on Daily Tech News Show with Tom, I saw, so you can listen to your explanation, yeah.

Steve: Yup, a little piece on Thursday, yup.

Leo: But there's a lot more stuff at GRC.com, including Steve's bread and butter, which is SpinRite, the world's best hard drive maintenance and recovery utility. If you have a hard drive, even if it's not a spinning one, an SSD, you've got to have SpinRite. Go to GRC.com to get it. Use ShieldsUP!. That's free. In fact, everything else is free. He's got lots of great stuff over there, including this show, audio versions and human transcriptions by Elaine Farris.

Steve: Yes. Heat willing. We're hoping that Elaine is still online. It's 111 where she is.

Leo: Oh, my god.

Steve: So she did mention that she might have a problem. So cut us both a little bit slack if she's a little bit later than usual. We'll hope that things are going to work out okay.

Leo: I had an interesting experience on Sunday. It was so hot, over 100 degrees in Petaluma, that my solar panels stopped working. You'd think this would be like a golden time for them, but no, no, it was too hot.

Steve: Yeah.

Leo: So they just - they took a little break. But they're back now. You can also find the show on our site, TWiT.tv/sn for Security Now!. But you know the best thing to do, and you'll be glad when you (like many of our listeners) start over at Episode 1 that you have them all, subscribe to the podcast. It'll automatically download, and you can listen at your leisure. Do what the NSA does. Listen every single week.

Steve: I was just going to say, I wanted to sign off saying I am flattered and gratified that the NSA has asked for formal permission to copy the podcast into their Intranet. Very cool.

Leo: I love that. That's awesome. That really is. It's very high praise. And, you know, we talk a lot about the NSA, and we maybe mock them a little bit. But I have to say they have the best cybersecurity recommendations on their website. They have really good stuff. They understand that their mission is also to protect American businesses and individuals against cybercrime. And they do a very good job of it. So there's some obviously very smart people at the NSA, and I'm at this point now gone too far kissing up to them.

Steve: And they clearly have good taste.

Leo: They have excellent taste. And I just want to thank them for letting me back into the country. So, you know, it was amazing. It was like I didn't do any of the things I thought about, wiping the thing, bringing burner phones and stuff. And it's good I didn't because I just scooted right back in the country. No reason to.

Mr. Steve Gibson, bless you. We'll see you next week. We do the show every Tuesday, 1:30 Pacific, 4:30 Eastern, 20:30 UTC. If you want to join us live, or even in studio, we can put you in here if you email tickets@twit.tv. We have a recent graduate from computer science at Carleton, up in Ottawa, and he's visiting with his mom as a celebration of his graduation.

Steve: Very cool.

Leo: And he's going into tech. So that's a good thing. He's going to be a full-stack programmer. Tickets@twit.tv, we'd love to see you in the studio. Thanks for joining us, and we'll see you next time on Security Now!. Bye-bye, Steve.

Steve: See you, my friend. Bye.