LostPass

Description: Leo and I cover another busy week of security news. Then we focus upon the recent "LostPass" phishing hack of LastPass, revealed at ShmooCon, and discuss the Internet's serious problem with phishing of all kinds.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-543.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-543-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. We're going to have a great time talking about some major flaws in Internet of Things devices like the Ring Doorbell, and even our beloved LastPass. Is nothing sacred? Don't worry. It's all going to be fine, next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 543, recorded Tuesday, January 19th, 2016: LostPass.

It's time for Security Now!, the show where we cover your security online with this guy, our Security Guru in Chief, Steve Gibson from GRC.com.

Steve Gibson: Hey, Leo.

Leo: Are you sleeping better? You sent me a graph of your sleep. It didn't look good.

Steve: Oh, boy, is it good.

Leo: Oh, it is good now.

Steve: Nine and a half hours? Nine and half hours of uninterrupted sleep. I got up three times.

Leo: That's what I saw. And I thought, but, you know, we're old. We have to pee. Let's face it.

Steve: Well, a total of eight minutes awake during that. The sum of those three events was eight minutes of awake and went right back to sleep. An hour and a half of slow wave deep sleep.

Leo: Nice. Oh, I'd love that.

Steve: Yeah. Anyway, so I've been focused on sleep for about 90 days. Actually, almost exactly 90 because it was the middle of October that I decided I was going to really address the issue of insomnia, which is a huge issue for a growing number of people as our society ages. And it's been an interesting, all kinds of fits and starts and dead ends. But I'm zeroing in on what I think will be a very practical formula. And you will be among the first to give it a shot.

Leo: Good. And you're using the Zeo still? Is that how you're monitoring this?

Steve: Yeah, all of those diagrams that you saw...

Leo: Yeah. I still have mine.

Steve: ...are from the little - from the Zeo headband.

Leo: But just to give you a comparison, folks, he got an hour and a half of deep sleep. Typically I'm, like, 10, 15, 20 minutes in an eight-hour night. And I sleep well.

Steve: Right.

Leo: But I don't get a lot of that deep, deep, deep sleep. And so that's pretty impressive.

Steve: Right. And that's what releases growth hormone. There are pulses of growth hormone release during deep sleep. And it's, you know, it's something you want a lot of. So anyway, as soon as I have some results, we'll talk about it further.

Leo: Good, good, good, because I want to know how to do that.

Steve: In the meantime, there's probably been, I mean, I'm interrupting myself. There's probably never been more tweets about a single question than I've had since ShmooCon's presentation of LostPass, which is a look at a phishing attack, you know, P-H-I-S-H-I-N-G, phishing, basically a spoofing attack on LastPass. And, you know, that's to be expected. We've got a bunch of listeners, and LastPass is the password manager that we've chosen, the one I'm using, the one you're using, the one we recommend. And certainly not the only one. And there's nothing worse about LastPass than the others in this regard. It's because it's the number one password manager that it's got the biggest

target painted on it.

Anyway, Twitter feed just went crazy. And so, and finally, yesterday, I tweeted that this will be what we're talking about. Just to hopefully sort of stem the tide so that people wouldn't keep saying, hey, Steve, have you found it? Do you know about this? Anyway, so...

Leo: That's my favorite one. Did you read this? Three weeks afterwards. Yeah. Yeah.

Steve: So we're going to talk about LostPass as our main topic. But it's part of a broader discussion that I want to have about phishing in general. But all kinds of things happen. It's like IoT day, or IoT week, the Internet of Things. We've got the Ring Doorbell question that again was another popular tweet because they're a sponsor of this podcast and the TWiT network, D-Link webcams, Amazon sending their users' WiFi passwords to the cloud. And there is a chant that is just going to be part of our discussion of IoT from now on. I've said it before. I'll have an opportunity to say it about seven times today.

Malvertising's in the news. We've got another backdoor was discovered in a major Internet appliance, very much like the Juniper problem. A little simpler than that one. That one was super high tech. This one is like, duh, but still difficult to explain and a little bit uneasy-making. An Assembly bill that's been reintroduced into New York State. Some Microsoft and Windows 10 news. And of course some errata, some miscellany, and other stuff to talk about, in addition to what is this LostPass? What does it mean? How has LastPass reacted? And sort of more broadly, what can we do in the industry because the problem with phishing is something that's persistent in the Internet.

And in fact, I never talked about it, but last summer we spent several months over in the SQRL group, it's one of the reasons that, like, okay, it's like, wait, what's going on? Well, I came up with an idea that we pounded on for several months, and it ended up evolving into the spec somewhat, although we didn't end up implementing what I had hoped we could. We've got hooks now in the spec for the future, which absolutely forecloses, sort of preemptively, exactly these kinds of problems. So anyway, lots of good stuff.

Leo: You saw that the Amazon Dash now is a platform. That's the button, by the way. Here's a little security tip. You know, so the Dash Button, you know, it's $5, and it's a button, and it's assigned to a product, so you just push the button, and more product comes. And I got one for toilet paper. I thought, what better? But I put it in the pantry, kind of at eye level for a 13 year old?

Steve: Mmm. Hard not to push that button.

Leo: We have a lot of toilet paper. It won't order unless - until the order comes. But, you know, with Amazon Prime, that means every other day we get another case of toilet paper. So I moved the button. But they're planning to put these in, Amazon's announced they're going to put these dash buttons in washing machines, in microwave - everywhere.

Steve: Oh, my goodness. You mean they're going to be incorporated by the OEMs.

Leo: Yeah. The OEM can set it up to automatically order resupply.

Steve: Okay. Now...

Leo: Is that wild?

Steve: I will begin with the refrain on that note.

Leo: What could possibly go wrong?

Steve: The refrain is, "All of our IoT devices need their own isolated WiFi network."

Leo: Yeah.

Steve: I've said it before. And that is the history of the first few stories in today's podcast, starting with the Ring Doorbell, which we love and is, as you know, well designed, well engineered. What happened is some penetration testing guys said, "Eh, let's take a look at this Ring Doorbell." And it's funny because their blog about this - which was titled "Steal Your WiFi Key from Your Doorbell?" and then it says "IoT WTF?" - their own blog posting starts off like an ad for the Ring Doorbell.

They start off saying: "The Ring is a WiFi doorbell that connects to your home WiFi. It's a really cool device that allows you to answer callers from your mobile phone, even when you're not home. It's one of the few IoT devices we've looked at that we might even use ourselves. It acts as a CCTV, automatically activating if people come close to your home. You can talk to them, to delivery couriers, to visitors, et cetera. It can even hook up to some smart door locks so you can let guests into your home. It's genuinely useful." And then they say, "Unlike most IoT devices."

So these guys are no generic fan of Internet of Things connected stuff. But then they took the Ring apart. And what they discovered was - and I don't know, I don't understand what the sequence of events is. This may be a delayed posting because Ring's technology, as we'll get to in a second, already nailed this. I mean, Ring is an example of, in my opinion, doing this as right as it can be done. But what these guys explained is that, from the outside, as we know, using a Torx T4 driver, you unscrew the two screws on either side of the underneath, and that allows you to remove sort of the front half. That then allows you to dismount it from the door. And on the backside is an orange button which is part of the setup process.

And what they discovered was that, when you press the setup button, it essentially brings up an access point over WiFi which is easily discoverable. And if you then bring up the URL /gainspan/system/config/network, that's an XML file containing a wealth of information including your WiFi password, in the clear. And they show this in their blog post.

So of course the whole point of this post was here's a device mounted on the outside of your home which can be disassembled and, if disassembled and activated and then

probed, would allow somebody who never entered your home to obtain the WiFi password that this device was using.

Now, they say, after explaining all of this, they say, "HOWEVER," in all caps, "kudos is due to Ring for responding to our vulnerability alert within a matter of minutes. A firmware update was released earlier this week that fixes this issue, just two weeks after we disclosed it to them privately." And they said, "Good job, Ring."

Leo: So it was fixed before they disclosed it publicly? Is that correct?

Steve: Correct. Yeah. So these guys acted responsibly. They contacted the vendor, Ring, and they said, hey, you know, with just a Torx T4 and a laptop, we were able to obtain the WiFi password which you've got in your - which they have to have somewhere in their device.

Leo: Plus they'll have video of you doing this, by the way, but that's okay.

Steve: Approaching the door.

Leo: Approaching the door, yeah. Should have a nice clear shot of you trying to get into the thing.

Steve: Yes. So what they appreciated was that, unlike, you know, how many stories have we shared where vulnerabilities of even a much more dire nature were communicated to the manufacturer, and nothing was ever heard. I mean, just like, dead zone. Yeah, we tried to contact them every week for the last four months, and we're going to go public with this because we never heard back anything. Instead, Ring responded in two minutes and said, yikes, thanks for that, we'll get on it, and we will let you know as soon as we have an update. And that update was available two weeks later. Now...

Leo: By the way, more than available because - and this I did not know about the Ring. They can push out an update. So they pushed it out.

Steve: Well, exactly. I was just going to say. So here's Ring's response to this. The title of Ring's response was "100% of Active Ring Video Doorbells Keep Your WiFi Password Secure." And this was addressed to the Ring community, saying: "You may have seen a report that Ring customers' WiFi passwords are currently vulnerable. This is false. We became aware of a potential security issue regarding WiFi passwords last year." And this is why I'm a little confused about the timing, but I guess technically here we are only, what, a little over two weeks in.

Leo: Yeah, yeah.

Steve: So I guess very late last year, to have all this timing make sense. They said:

"...last year, and promptly developed a solution to ensure WiFi passwords are secure with all Ring Video Doorbells. This fix was automatically pushed to all active Ring devices via a firmware update within 24 hours of us releasing the update. No user action was required. This means 100% of Active Ring Video Doorbells are currently operating on a secure version of our firmware, and your WiFi password is secure.

"Every day your Ring video device automatically checks for new firmware updates. There is a chance that some Ring devices currently on store shelves have firmware that does not contain the fix. But as soon as those devices are set up, the firmware will automatically update to latest version," which at the time of this posting was 1.6.39, "and there will be no WiFi vulnerability. If you'd like to double check that your Ring is operating on the most up-to-date firmware," that is, v1.6.39 as of this moment - "you can simply open your app, click on your Ring device, and go to its settings page to view the version of firmware your device is running." Then they have some screenshots.

"We at Ring, they say, work every day to keep your home, neighborhood, and community safe. If you have any concerns or would like to speak with a Ring representative for more information," blah blah blah. And this was Joshua Roth, their CTO, the Chief Technology Officer. And I should mention that these Pen Test guys were, I thought, very evenhanded. Because they noticed that the Ring Doorbell used a WiFi module from Gainspan, and that the URL was /gainspan/, you know, blah blah blah, they presume that maybe this was just sort of built into the module which Ring incorporated.

So on one hand they say: "This is quite a fail: walk up to a door, remove doorbell, retrieve user's WiFi key, own their network." And then they continue: "Did Ring ever intend to expose this functionality?" Well, we know they didn't. "Or was this just default functionality that Gainspan have in their firmware? As it's a standard Gainspan URL, it looks like they just hadn't disabled the configuration." And then they continue: "The WiFi key is still stored" - and this is an important point that's where I want to go with this after I'm through. "The WiFi key is still stored in the doorbell somewhere. How well protected is it now? It's most likely stored in the module. Somebody with a soldering iron could possibly get it. Having physical access to the doorbell means we might be able to upload modified firmware." And then they say, "Your doorbell becomes a backdoor?"

Now, so two things. This is a fundamental problem with, as they mention, any physically exposed, WiFi-connected device. From an engineering standpoint, I could imagine a few things they could do. They could actually arrange not to store it in the device, but pull it from a Ring server. But then that's problematical, too, because then your WiFi password, encrypted, no doubt, but still it's off-premise. Or it could be buried inside a chip that cannot be read from. And we know there are all kinds of ways to do that. There are ways that it would be possible to have the WiFi password there in a way that, like, on the same chip as the WiFi radio itself so that at no point is it exposed in any sort of transaction on any bus that's there. But, you know, we don't know that that's what they're doing.

And what this takes me back to is the conversation we've had many times about how it was impossible for DVD players or even Blu-ray to decrypt an encrypted disk in a viewer's living room and ever think they could retain control of it. Everything had to be there to decrypt the disk in order to display the movie. So it was inherently an impossible problem.

So there's an aspect of this where sufficient engineering for this or any similar device - and I'm not in any way picking on Ring. They've demonstrated, I mean, more responsibility than we've ever seen from anyone else in the industry. And the service they're offering, the device they're offering has to be on the outside to do what it does and has to be on your WiFi network to do what it does. So the best they can do is to

make it really difficult, I mean, up to the level of effectively impossible, by embedding the WiFi password in a way that it cannot be read back. We don't know if they're doing that.

And so that brings me to my second point, the refrain, the IoT, the Security Now! IoT refrain: All of our IoT devices need their own isolated WiFi network. I just, you know, I've said it before. Routers with split WiFi are becoming now commonplace, you know, so-called "guest WiFi" access. The one I most recently set up was some Netgear. And it offered me to have that, and there was a setting there. Do I want to allow the guest WiFi to have visibility to the primary WiFi? No. I don't. I want the guest WiFi to have access to the Internet and not the rest of the internal network, whether wired or the primary WiFi. I no longer think - I never did think this was an option. It really isn't an option to put these sorts of devices on your - to have a single wireless network for your entire environment.

Leo: That's a great idea. I didn't even think of that. So you set up the guest WiFi, and you put all the IoT things on that.

Steve: Yes.

Leo: And then the best an attacker could do is access that.

Steve: Exactly. So they get, what, free WiFi. Well, you can get that from Starbucks.

Leo: Right.

Steve: So, you know, big deal. I mean...

Leo: Right. That's interesting, yeah.

Steve: Yeah. So, I mean, and I just - these guys have acted responsibly. Now, another example is our second story, and that is that a group called Vectra Threat Labs took a close look at a generic $30 off-the-shelf D-Link webcam. So IoT. And I'll just summarize what they said because they put it together beautifully, as well as I could.

They said: "Reports of successful hacks against Internet of Things devices have been on the rise." Yeah, because Internet of Things devices are on the rise. And apparently we're going to have buttons, Buy It Now buttons on all of our things from Amazon. "Most of these efforts have involved demonstrating how to gain access to such a device or to break through its security barrier. Most of these attacks are considered relatively inconsequential because the devices themselves contain no real data of value," you know, no credit card information or privately identifiable information, so forth, personally identifiable information.

They continue: "The devices in question generally don't provide much value to a botnet owner, as they tend to have lots of bandwidth, but very little in terms of CPU and RAM. However, these devices get more interesting to sophisticated attackers when they can be

used to establish a persistent point of access in a network. Putting a callback backdoor into a webcam, for example, gives a hacker full-time access to the network without having to rely on infecting a laptop workstation or a server, all of which are usually under high scrutiny and may often be patched. On a tiny device there's no antivirus and no endpoint protection. In fact, no one thinks of the device as having software on it at all. This makes these devices potentially inviting for persistent attackers who rely on stealthy channels of command-and-control to manage their attacks. The downside for the attacker is that this class of devices doesn't usually have any persistent storage that is really usable."

So, for example, the malware that users are typically downloading on their PCs, it's megabytes, but they've got terabytes of hard drive. So that's not a problem. These things are typically really lean.

So these guys continue: "Instead they use NVRAM (nonvolatile RAM) to store configuration and the flash ROM to store the running code. So the attacker's hope for real persistence rests on being able to control what will be in the flash ROM.

"In this blog we will explore how difficult it is to create a new flash image that could contain all the tools we need to have a real persistent backdoor to the network on which the device is installed. Once we have such a flash image, putting it in place would involve 'updating' an already deployed device, or installing the backdoor onto the device somewhere in the delivery chain" - remember, this is sort of - this is one of the things that Snowden talked about years ago - "in other words, before it is received and installed by the end customer. For this experiment to be meaningful, it's imperative that the device continue to perform its normal function. Otherwise it would immediately raise suspicion or cause the customer to replace the device with a working version."

Now, I've skipped most of their blog posting, but Kaspersky picked up on this and summarized it in a few lines, saying: "The report explains the attack against a $30 D-Link WiFi webcam, starting with the researchers being able to dump the contents of the device's flash memory chip for analysis. This particular device's firmware included a U-Boot and Linux kernel and image. They were also able to dump the contents of the Linux image and access its file system" - and this all sounds very much like what we know people are doing with routers all the time. So here's something of sort of similar power that just looks like an appliance with much less sophistication than a router, but it's running Linux - "where they found," writes Kaspersky, "an executable file used to verify and update the firmware. By analyzing the process by which the firmware is updated, they were able to remotely add a connect-back Socks proxy to the Linux system."

So essentially this says that this particular $30 IoT webcam can be remotely hacked and a backdoor added to it by updating its firmware because taking one device which allows all of its contents to be dumped, and now we're seeing this is a recurring problem, that is, sort of a recurring theme of Internet of Things devices is that, if you can dump them, you can reverse-engineer them. And so they figured out how the update system is protected and broke its protection in order to install whatever they want.

So it's doubtless the case that it would be possible to make this more secure, to actively thwart this kind of attack. And, you know, we see, for example, that our iOS devices, they've got all kinds of strong protection against malicious updates. This webcam doesn't. It's a little $30 gizmo that you plug into your network. And so the refrain is we don't want this on our primary WiFi network. Give it its own network. We're still in the early days of Internet of Things. And they're just not secure yet.

I think we know that there's some work being done by various standards committees on

establishing some security operability standards for Internet of Things devices. That's good. But it'll take a few years for that to happen. And then we know how non-rapidly the industry tends to adopt new standards. Just look at any of them, IPv6, SHA-256 and what a problem that's been, and so forth. So I just - the standard operating procedure is going to have to be either get a split network WiFi router or a second WiFi hotspot, set it up with its own network, and use that for your Internet of Things stuff.

And hot on the heels of this, somebody tweeted me somebody else's tweet, so a retweet, showing a screenshot from the - and I won't say the name of the app, which is Amazon's Echo name, where they explain about how they save the user's WiFi passwords to Amazon's servers. And in the FAQ they say - oh, and it is optional. But they're painting it as a benefit, which many users may feel it is. They ask themselves the question in the FAQ: "What's the benefit of saving my WiFi passwords to Amazon?" The answer: "Once you save your WiFi passwords to Amazon, we can configure your compatible devices" - your compatible Amazon devices - "so that you won't need to reenter your WiFi passwords on each device."

So, and the way the Amazon supply chain works, when I buy an Amazon Fire TV box, it already is associated with my Amazon account. So presumably it's able, maybe, to have my WiFi password in it because Amazon has it because I had previously shared, I used some other Amazon device, and they were syncing through the cloud. So again, this is classic tradeoff of convenience versus security, and it is optional. So it's good that it is, but it's something that users should be aware of.

And again, better to have it on its own network. Who knows what will be revealed about the security of any of these devices over time. I mean, we've spent years following the security of a mature family of operating systems, struggling, where security has been a huge focus, and a big deal, and often a selling point. And so compare that to the infancy of all these gizmos that are in a big hurry to get into the market and get themselves installed and establish a foothold. You know, they're just at the beginning of a decade that we've just gone through on desktop computing systems.

So the good news is a lot has been learned by the industry that doesn't have to get relearned, much the way Google was able to learn a lot of lessons from the browsers that preceded it when they did Chrome, so they had a lot less pain to go through in the beginning. But still, as we know, security is not easy. So I just, you know, the number one recommendation has got to be these gizmos, all of these IoT things, need their own WiFi network.

So we've talked about the whole advertising, adblocking, malvertising and so forth. In the last week the Forbes website had an interesting event occur. The Forbes readers are now being asked to turn off adblockers when they visit the Forbes site. And unfortunately, last week, when people did that...

Leo: Oh, no.

Steve: ...it immediately put a pop-under behind their browser, which all of our listeners would be immediately suspicious of. It was the "Your Java version is out of date. Click here in order to update." And on Engadget a columnist who uses the pen name, I assume it's a pen name...

Leo: No, that's her real name.

Steve: Violet Blue is?

Leo: Yeah.

Steve: Okay, cool. Anyway, she said: "The real reason" - now, I have to understand she's way off, she's way in the anti-advertising side. She said, in fact, her column was titled, "You Say Advertising, I Say Block That Malware."

Leo: Mm-hmm.

Steve: She writes: "The real reason online advertising is doomed and adblockers thrive is its malware epidemic is unacknowledged and out of control." Now, I think that's overstating the problem dramatically. I wouldn't say that it's a malware epidemic we have. But it's a concern. And so we all are aware that we're unfortunately safer if we block ads because it is now an active delivery conduit for malware.

She writes: "The Forbes 30 Under 30 list came out this week, and it featured a prominent security researcher on the list. Other researchers were pleased to see that one of their own was getting positive attention and visited the site in droves" - okay.

Leo: Oh, boy.

Steve: Maybe that's a little much. I'm not sure there are droves of...

Leo: Security researchers?

Steve: ...security researchers - "to view the list. On arrival, like a growing number of websites, Forbes asked readers to turn off adblockers in order to view the article," she writes. "In doing so, visitors were immediately served with pop-under malware, primed to infect their computers and likely steal their passwords, personal data, and banking information." And in fact it was that, it was the trojan we've talked about often that does those things.

She says: "Or, as is popular worldwide with these malware exploit kits, lock up their hard drives in exchange for Bitcoin ransom." And I have a link to a tweet of the person who saw this. If you want to, Leo, you can click on the link, and you'll see something that is very familiar to us. I said in this instance it was a spoof of the familiar "Your Java is out of date and must be updated" message. Which our listeners would know not to pay attention to. And again, if we did fall back on the adage or the advice, never install anything you didn't go looking for, this certainly qualifies as something you did not go looking for.

Leo: And speaking of phishing, they're even kind of duplicating a true Java update warning.

Steve: Yes.

Leo: Yeah. Although the site that the warning comes from is fugupdates143 dotcom.

Steve: Yeah.

Leo: So I'm not - I don't know if any of our listeners would click on that. Apparently I just did, so I apologize. [Crosstalk], yeah, mm-hmm.

Steve: Yeah. Just another example of, unfortunately, the fact that sites are, as we predicted, this was the foreseeable consequence of adblocking, with sites detecting that ads were not being pulled and saying, hey, please consider supporting the site by lowering your adblocking shields. And unfortunately, in this instance, it was very public; and a lot of security researchers - a "drove" of them - were then exposed to pop-under malware. Or at least an attempt at that.

Okay. So we talked a couple weeks ago about the sort of jaw-dropping Juniper exploit, where an elliptic curve was modified in such a way that it really was suspicious and looked as though it was done in a way that would allow this router essentially to create a hidden backdoor in the router. Well, another one has been found that's much less high tech.

There's a company, Fortinet, F-O-R-T-I-N-E-T, that's another one of these big-iron corporate security appliance companies. And this is very reminiscent of the Juniper router backdoor. In this case, what was discovered in the firmware was a hardcoded SSH, that's the secure shell remote login, essentially, password. And it's just, it's a very nice-looking password, FGTAbc11*xy+Qqz27. So not something that you're going to guess. But it was built into the firmware so that anybody who knew that had remote access to this equipment. That's a backdoor.

So Fortinet, of course, rejected the characterization of this hardcoded password as a backdoor. They responded in writing, saying: "This issue was resolved, and a patch was made available in July of 2014" - okay, so that is a year and a half ago - "as part of Fortinet's commitment to ensuring the quality and integrity of our codebase. This was not a 'backdoor,'" they have in their response, "vulnerability issue, but rather a management authentication issue." Okay. What?

"The issue was identified by our Product Security team" - and that's in caps, by the way, so I guess that's an official thing, their Product Security team - "as part of their regular review and testing efforts. After careful analysis and investigation" - okay, how careful did it have to be? It's a hardwired password. "After careful analysis and investigation, we were able to verify this issue was not due to any malicious activity by any party, internal or external." Okay. So that means it was on purpose?

Leo: It was accidental. We didn't mean to do it.

Steve: I mean, none of this makes any sense at all. "All versions of FortiOS from 5.0.8 and later" - okay, and that's on their version 5 track - "as well as FortiOS 4.3.17 [on their version 4 track] and later are not impacted by this issue." Okay, meaning that's when we changed it. But what's weird is they didn't eliminate it. We'll get to that in a second.

So from what they said, and based on there is some version history available online, so that means that the hard-coded SSH password was active in FortiOS through at least 2013 and through the first half of 2014, when apparently for some reason they fixed it. And we don't know how far back in time, maybe even earlier, it goes. No advisory from Fortinet about this was ever published. So for some reason a year and a half ago they changed it. And why I say they changed it is a researcher told Dan Goodin, who of course writes for Ars Technica, that while the exploit no longer works as it once did - meaning hello, here's the password, and oh, look, I got root - the later firmware is still suspicious because it contains the same hardcoded string. Which you've got to think is like, what?

Okay, so now what I'm immediately thinking is that they've added some port knocking. Right? They've put something in front of the open port that accepts this password. They didn't take the password out, or even change it. But now it's no longer exposed.

Leo: But everybody knows it.

Steve: I wouldn't use this crap. I mean, yes. So probably what we now need is a full reverse-engineering of the firmware. And somebody is probably going to find that, if you send SYN packets in a certain sequence to closed ports, it will notice that, and that's called port knocking. And then that will authenticate you to then access the secure shell from that IP and give it the password that we all know and is now in the show notes. So, wow. Uh. I'm just speechless.

Leo: Yeah.

Steve: And this is starting to feel a little creepy, that for reasons we don't understand, that no one explains, that are just sort of like, oh, well, I mean, these guys are saying more even than Juniper. Juniper was saying, we don't know how this got into our source. This was never meant to be here. The moment we discovered it, which unfortunately wasn't quickly, but we fixed it. These guys are saying this was a management authentication issue, which says we deliberately built a backdoor into all of the equipment we ever sold to all of our commercial customers and never told them.

Leo: Ugh. Horrible.

Steve: Yeah. I mean...

Leo: Unbelievable.

Steve: ...these guys need to be out of business. This is just so wrong. And...

Leo: [Crosstalk] name, too. I think there are a lot of people use their products.

Steve: Yes. And they've apparently simply obscured it. How else could you explain...

Leo: Didn't even fix it, yeah.

Steve: Yeah, how else could you explain that the string is still in the firmware? And it's like, so it doesn't work the way it did, right, because now it's harder to get to the door. But apparently they still want remote access, and they didn't remove it from themselves. Believe me, this is - so my point is that here's two major players, both with serious remote, remotely accessible, persistent backdoors into their hardware. We're not getting an explanation about how this got in there. And so far it's like everywhere we've looked we've found this problem. It's frightening.

So, okay. I saw this last week, and I blew it off because I did a little digging, and it was legislation that was first proposed in, like, June or July. I remember it was a "J" month, the middle like of last summer of 2015.

Leo: Wait a minute. Now I have to challenge you. In your head it's stored, the month began with "J." I don't know which month, but I just know it began with a "J."

Steve: Yeah, and it's down there at the bottom of the circular calendar.

Leo: Your brain works weird.

Steve: It was a "J." And it's like, eh. And in the verbiage of the bill it says - it starts off: "Relates to the manufacture and sale of smartphones on and after January 1, 2016 that are capable of being decrypted and unlocked by the manufacturer or its operating system provider." And I thought, well, okay, that deadline got past. So I just thought, eh, you know, and it didn't make it into last week's conversation. But someone else tweeted to me that it had been resubmitted.

Leo: Oh, lord.

Steve: And indeed it has been. Now, I've heard of Walter Mosley and Patricia Fahy. They're both honest-to-goodness politicians. And so this is New York State legislation proposing a ban on the sale of encrypted smartphones. Now, when you dig into this deeper, this is actually - it would be a ban on the sale of smartphones that the manufacturer cannot encrypt upon receiving a court order...

Leo: Decrypt.

Steve: Exactly, which the manufacturer cannot decrypt upon receiving a court order requiring them to do so. So this is one of the thrusts of, you know, one of the potential thrusts of legislation. I did hear that there was some entourage from Washington that went to Silicon Valley recently, and that they were rebuffed. And I have - that was just some talking head that said that, and I haven't had a chance to figure out what that was about.

Leo: You've been rebuffed.

Steve: Yeah, sorry, but we're not interested in talking to you. You guys are idiots. We've already said no.

Leo: Yeah.

Steve: So anyway...

Leo: Well, and of course, if it had, if that passed in New York State, will, that would be the end of it because that's a big market.

Steve: Yes.

Leo: So it's not only insulting to the people of New York, it's insulting to everybody else in the country. And the world. Crazy. Crazy.

Steve: Yeah, yeah. I mean, and again, to me, a really fascinating contest that we're in the middle of and will doubtless be looking at this year and next year to see how this shakes out because, as we've talked about it before, the whole problem of what right do people have in the U.S. under our Constitution, where we have this whole issue of protection from unlawful search and seizure, yet a legal right for a search warrant to then breach that under certain terms and conditions. Is that the way it's going to fall out? And, wow, I just - it's going to be really interesting to see.

Meanwhile, in sort of a related story, I just got a - I thought this was interesting. Up in Canada, in Toronto, a woman's elderly husband died, taking with him in his head the Apple UserID for the iPad that they shared. He had a Mac that he used exclusively, but they shared an iPad. And she had a card game on it that she liked. And she knew what the unlock code was for the iPad, so she was able to unlock it, get past the lock screen and play cards until something happened that required her to use her Apple ID. Maybe it needed to be updated or renewed or who knows what. And she couldn't make any headway with Apple, so she asked her daughter to see what the daughter could do.

As the daughter said from her story, after many phone calls and two months of what her daughter describes as her runaround - daughter was named Donna - provided Apple with the serial numbers for all the items, her father's will that left everything to his wife Peggy, and a notarized death certificate, then was told it wasn't enough. Donna said, "I finally got someone who said, 'You need a court order.'"

And she says, "I was just completely flummoxed. What do you mean, a court order?" she said. "I said that was ridiculous because we've been able to transfer the title of the house, we've been able to transfer the car, all these other things, just using a notarized death certificate and the will." To which a Toronto-based estate attorney noted that there is not currently any clear law about this, and that Apple is asking for a court order as a means of protecting themselves against any repercussions from disclosing this information. So this of course follows on our discussion last week of the LastPass security of assigning people whatever they call it now, emergency access.

Leo: Emergency access, yeah, yeah.

Steve: Yeah, exactly. So again, what we're seeing is more and more of the Internet is going into our devices. And that's requiring more security. Yet security requires that people know passwords. And here's an instance where it wasn't known. And my first thought was, well, just reset your pad and create a new account. And of course the answer, it was covered in the article, is like, well, then she'd have to rebuy all of the things that she and her husband had purchased over time. So it's like, eh, okay, well, [crosstalk].

Leo: What would you do with SQRL?

Steve: Actually, SQRL - she and her husband would both know, would both share their SQRL password.

Leo: Right.

Steve: And so she would be able to authenticate herself.

Leo: But he neglected to share his password with her. That's the problem; right? He didn't share his Apple ID with her.

Steve: Correct. Correct. So, right, it is not, you know, at that level it doesn't offer any solution. We still have that problem.

Leo: Right.

Steve: Although SQRL does have the rescue code specifically for this purpose. And so that would typically be, that's the kind of thing you would have in your will or in a safety deposit box or something because that is your ultimate get-out-of-jail card if you forget your password. It is for password recovery. And so that's built into the system.

Leo: And if you put that in LastPass, in your emergency contact - the problem is it's not so much people who listen to this show are going to have this problem.

Steve: Right.

Leo: It's going to be everybody else.

Steve: Right. Well, and as we know, LastPass does have the ability to preassign a one-time password, a one-time password or passcode that you're then able to sequester somewhere and only get it when you need to.

So last week, or sometime between now and last week, I'm not sure exactly what day this was, Microsoft capitulated a bit on this Get Windows 10 backlash and has created an official Get Windows 10 blocker. That is, they've added the technology for 7 and 8.1 to formally stop those operating systems from pushing you to upgrade. I think this is aimed at Enterprise customers who just said, look, we need to control this somehow.

I created a bit.ly link, which I tweeted with this news when it came out late last week, bit.ly/no-gwx. So that's bit.ly/no-gwx, no Get Windows 10, which just takes you to Microsoft's support page. Now, the bad news is there's no Fixit button, where you just click that and it fixes it, because Microsoft still really doesn't want people to do this. But they've begrudgingly created a means. So, and in Microsoft Speak, the title of this is "How to manage Windows 10 notification and upgrade options." And then they explain that qualified - yes, and Leo's still scrolling down the page.

Leo: This is ridiculous.

Steve: It's crazy. "Qualified computers and devices that are deployed in your organization and that are running Windows 7 Pro or Windows 8.1 Pro are eligible for" - and apparently not Home - "are eligible for the free Windows 10 upgrade offer and will be able to update through Windows Update." And then it says "This offer is not available to customers who are using Enterprise or Embedded editions of Windows 7 and 8.1." Okay, so the Enterprise editions never were doing this. This is just for Pro users.

So I'll let people go to the link if they're interested. I've already played with it. It works. I played with it on a brand new Windows 7 install that did present the little white offset windowpanes icon. You install, essentially, either one of two, depending upon which versions of pre-10 you have, 7 or 8.1. That is, Windows Update. So you install a Windows update. Doing that adds the feature of being able to formally shut down presumably all future attempts. Microsoft of course has always had the ability to go around this, and they have in previous I-don't-want-Windows-10 efforts. So we'll see how sticky this is.

But then, as this page explains, you need to go into the Group Policy Editor and add - or actually a new item has appeared named "Turn off the upgrade to the latest version of Windows through Windows Update." So you enable that to turn it off. And that's buried five levels down in Group Policy. And then they also say you can do it with the registry, but it's not clear whether you can do one or the other. And I think the change in Group Policy pushes the change to the registry because then when I went to the registry it was already there. And that's a DisableOSUpgrade set to "1" under Microsoft\Windows\WindowsUpdate. So I think you can do either one of those.

But apparently neither of those removes the icon, which is a separate problem. So then they give you a registry change which is DisableGwx = 1, set down underneath Software\Policies in the registry. And then, with any luck, you're good to go.

Alternatively, you can just run the GWX Control Panel, and it pops up. And by the way, it was updated just yesterday, for those of you who are using. And I know many people who are following us do because I've had a lot of tweets about it.

As of January 18th, the author writes, he says: "I've just uploaded version 1.7.1.0 of the program. It has lots of usability enhancements, particularly with Monitor Mode. This version should reduce or eliminate the occasional 'false alarm' alerts that happened in earlier versions and also includes a preferences option where you can select the kinds of alerts you'd like to receive." And he says this user guide is now up-to-date.

And he did solicit some input. He said: "Also, I'm looking for information on a new kind of Windows 10 notification that Microsoft appears to be pushing out. If you have ever experienced the kind of Windows 10 desktop pop-up shown in the following picture" - on his page. And remember you can just google "gwx control panel" in order to find his UltimateOutsider.com blog posting. Anyway, he shows it and asks, if you do see it, to let him know because that's something which he believes might be getting around his latest update.

And I have to say that I did install that, and it was a little noisy. It was, like, complaining after I'd already disabled things. And I thought, eh. You know, and I'm not one to install things I don't need to. So for me, when I go to 7, I will be using this official Microsoft solution. But, boy, it's not the kind of thing you want your aunt to try to do. So you could just tell her to use this GWX control panel and just say, yeah, protect me.

Leo: I doubt that Microsoft will still be doing this in 2020, when you upgrade to Windows 7. I'm sure by then they'll have stopped.

Steve: Well, actually, they have another strategy, Leo.

Leo: Yeah?

Steve: Thank you for the segue. They've just announced that the next version of Intel's chips, the so-called "Skylake platform," will not be backward-compatible with previous versions of Windows. And I'm not kidding.

Leo: Wow, wow.

Steve: I'm just - I'm just stunned. It's like, okay.

Leo: So another way of saying that is future Windows versions will require Skylake or later?

Steve: Yes.

Leo: That's really a more accurate - that's a crazy way that they said that because it

implies it's Intel's fault.

Steve: Well, what's different is that Intel has always cared about being scrupulously backward-compatible.

Leo: Yeah, no, it's not Intel's fault.

Steve: Right.

Leo: Right?

Steve: Right.

Leo: It's Microsoft.

Steve: So The Verge covered this. And they said: "Microsoft says new processors will only work with Windows 10. Windows 7 and 8.1 won't be updated for future processors, starting with Intel's Skylake platform. Soon," writes The Verge, "when you buy a new PC, it won't support Windows 7 or 8."

Leo: What? How the heck - what?

Steve: I know.

Leo: So it isn't what I said. It's not that Microsoft is requiring something in Skylake or later. Somehow they're breaking compatibility.

Steve: Yes. "Microsoft has announced a change to its support policy that lays out" - this is The Verge - "that lays out its plans for future updates to its older operating systems, and the new rules mean that future PC owners with next-generation Intel, AMD, and Qualcomm processors will need to use Windows 10."

Leo: That's bizarre.

Steve: I know. "It's not usual for old PCs to fall short of the minimum requirements of a brand new operating system."

Leo: But this is the [crosstalk].

Steve: "But in this case, the opposite is happening," writes The Verge. Microsoft and its partners will not be putting in the significant work necessary to make new hardware work with older versions of Windows. The old operating systems, at best, will merely lack the latest updates; at worst, they may not function properly.

Leo: It seems like you'd have to backwards patch the old versions to make them not work. I don't understand.

Steve: Or do some - or literally...

Leo: Unless it's Intel doing something.

Steve: ...sacrifice backward compatibility.

Leo: I mean, is Intel doing, I mean, this sounds like Intel's doing it.

Steve: But it's all three manufacturers. So on January 13th, Microsoft's blog posting was titled, and get this, "Windows 10 Embracing Silicon Innovation." That's the way they sell this. And Microsoft writes: "Going forward, as new silicon generations are introduced, they will require the latest Windows platform at that time for support." This is huge.

Leo: The only way they could do this is if, for years, they've been putting into older Windows versions a CPU check. And if it doesn't check, like if it said, well, are you a Core 2? Okay. If you're - wait a minute. What is this Skylake? You've never heard of that? Don't run.

Steve: You're right.

Leo: They must have done that.

Steve: You're right. And they're [crosstalk]...

Leo: Because Intel's still x86. This is not - they're not abandoning x86.

Steve: The second line of their posting says Windows - oh, wait a minute. It doesn't have to be all along. It just has to be in the last few months.

Leo: An update went out.

Steve: Yes, a security, a, quote, "security"...

Leo: But you know what will work? XP.

Steve: Yes.

Leo: XP should work, if that's the case.

Steve: So the second line of their blog, of Microsoft's blog, says: "Windows 10 will be the only supported Windows platform on Intel's upcoming Kaby Lake silicon, Qualcomm's upcoming 8996 silicon, and AMD's upcoming Bristol Ridge silicon."

Leo: Okay, now, the chatroom's saying, no, no, no, it's just optimization. It'll still run. You're saying it won't run. Like I got a new Skylake processor, I try to put Windows 7 on it, and it won't work.

Steve: Okay. So The Verge says...

Leo: What is it we're saying?

Steve: The Verge says: "This new policy doesn't mean that Windows 7 and 8.1 are no longer supported in general. The two operating systems will continue to get updates through January 14, 2020," okay, "and January 10, 2023." That's their standard updates. "But that's only if you're using hardware that was contemporaneous with those operating systems."

Leo: So you're just not going to get updates.

Steve: "For current PC owners, the detail to note is that Intel's current sixth-generation processors, known as Skylake, are the first that won't support either of the older versions of Windows." So you're going to have to ask Paul about this.

Leo: This is really unclear. That implies that Intel's doing it.

Steve: This says "Intel and Microsoft say that the platform and Windows 10 were designed for each other."

Leo: Yeah, yeah. I know that. And they made a big announcement that they had been working together. And it sounds like they're colluding. I would go right to court. They're colluding, if that's the case, because...

Steve: I'm speechless.

Leo: Well, I want to know more. I'm not ready to jump on the hangman's noose here. Scott Michaud in the chatroom says they're just saying, if we release a patch that breaks it, then we're not going to fix the patch. Sorry, but it sounds like they're going much farther than that. I don't understand.

Steve: Yeah.

Leo: I don't understand. Okay. I'm going to have to part - yeah, I'm going to ask Paul. He'll probably say, oh, it's no problem. I want to read - the problem is The Verge, now, it's Tom Warren, probably, who knows what he's talking about. But I'd like to read...

Steve: Well, and Microsoft's own posting, yeah. At your leisure...

Leo: Yeah, I'm looking at it right now. All right.

Steve: ...read what Microsoft said.

Leo: It's Terry Myerson, who knows what he's talking about. Okay.

Steve: Yeah. Yeah. And speaking of talking what they know about, I have an errata because I jumped the gun with my heavy sigh last week over the end of XP's support. It's the Embedded version of XP whose support is ended, which is different from the point-of-sale, the POSReady. It continues for another happy three years, through April 19th of 2019. And sure enough, my little XP machine that I use for weighing and printing stamps, it got some updates on the second Tuesday of January. So indeed, that's all still alive and well.

So thank you, people, for catching my mistake, and I'm correcting it. The little hack to add the POSReady still works. I even actually used it over the weekend on a different XP machine, and it happily continued to update itself. So it all works.

Leo: Here's a relevant paragraph.

Steve: Yeah, yeah, good.

Leo: "For Windows 7 to run on any modern silicon, device drivers and firmware need to emulate Windows 7's expectations for interrupts, processing, bus support, and power states because Windows 7 was designed 10 years before any x86 or x64 systems on a chip existed. This is challenging for WiFi, graphics, security, and more." So what they're saying is, all along, in order to keep older versions of Windows running on new processors, we have had to send out patches, firmware updates and device drivers, to make it work, and we're not going to do that anymore.

Steve: Well, and they clearly don't want to. I mean, is there any stronger message that we've had, you know, since last summer about how Microsoft feels about Windows 10? I mean, so it's like, well - so anyway, I will, you know what I'll be doing, I'll be buying some really fabulous state-of-the-art heavy iron hardware for my next machine, which will be running Windows 7, and I won't wait until I really need it. I'll buy it now because who knows what the future holds. I mean, what it ultimately holds is me moving away from Windows, but not till SpinRite is done.

Leo: It's a fascinating issue. I hadn't, I mean, this is the first time I've ever heard that, when you're running Windows 7 or Vista or XP on modern Intel processors, you have to do some sort of emulation and modification to make them run, that they wouldn't run otherwise.

Steve: Right. It's certainly the case that you might not be able to run a current operating system on old hardware. That we're all aware of.

Leo: That's fine. I understand that.

Steve: But so far, Intel has always given us backward compatibility so that, when newer hardware comes out, it runs on older OS.

Leo: Well, maybe not. It sounds like Microsoft saying, no, we had to write software for compatibility reasons.

Steve: Well, one thing we can do as a canary in the coal mine is see what happens with Linux. If Linux doesn't have any problem, then that says, okay, why does Microsoft's Windows 10 have a problem?

Leo: I have to say it's pretty typical, when you install Linux, if you want to install it on an old processor - oh, it's the other way around, though, isn't it.

Steve: Yeah.

Leo: If you want to install an old Linux on a new - well, Linux, you don't have to worry about it because it's free, and you just install the latest version. Why would you install an old version?

Steve: Well, but my question is, that allows us to determine if it's actually a problem, or if this is something Microsoft...

Leo: Could you run an old version. Okay. Could I run an old Linux kernel on Skylake.

Steve: Yes, yeah.

Leo: Because it never heard of Skylake.

Steve: And all of its peripherals and drivers and things, if it just goes, oh, yeah, fine, no problem.

Leo: Hmm. An interesting conundrum.

Steve: Yeah.

Leo: Yeah, we'll be talking about it tomorrow, I'm sure.

Steve: Yeah. Okay. So people keep asking what happened to Episode 540? So I just wanted to say that was our Christmas episode. We jumped from 539 at GRC...

Leo: Didn't we number it 540?

Steve: Yeah. But the problem is on my page, I guess I need to put it in page.

Leo: Didn't put it out, yeah. I think we put it out. Right.

Steve: I didn't, yeah, I didn't submit anything. And so people see on my page it goes from 539 to 541. And so I guess what I'll have to do - I'll do that when I post today's podcast on the 'Net, I'll just add something to say, look, go to TWiT if you want this. It's a rerun of the Vitamin D episode.

Oh, and Leo, we were talking last week about the cool, interesting, Bragi in-ear Bluetooth headphones.

Leo: Yeah.

Steve: I got a kick out of this. They were of course making a big splash at CES. And as a backer I received a note from them that I thought our listeners would get a kick out of, as would you: "Dear Backer, all units that were in transit and about to be delivered were held back by UPS, our freight forwarder. In an inspection of the goods, they discovered that the LED of Dash is blinking in the packaging. They thought that Bluetooth was therefore active while the Dash was blinking and stopped all shipments. All goods are going on aircraft, and no Bluetooth is allowed to be active during flight, especially when you have thousands of devices," all blinking away on a pallet.

"UPS was correct in holding back goods. We were able to convince them that the Dash is in its power save mode" - I hope the LED wasn't blinking often - "and not in active Bluetooth mode just because it is blinking. UPS has accepted to ship the goods after documentation on power modes from Bragi - we had to get an employee to Hong Kong to

clear up the situation - and will resume shipping tomorrow. The units that were supposed to be shipped already are being shipped to EU hub tomorrow and on Monday," blah blah blah.

"We're incredibly sorry. This is really our fault, but we didn't know that the blinking could be mistaken for active units and didn't declare that Bluetooth isn't active during blinking." So I just got a kick out of that little whoops, you know, unexpected snafus. Which, and this is the kind of thing that we see with Indiegogo and the DIY manufacturing sites.

Leo: Guy Smiley is saying in our chatroom he ran Ubuntu 8.04, which is pretty old - we're at 15 right now - on Skylake last week.

Steve: Imagine that, Leo.

Leo: Shocking.

Steve: Incredible. Shocking.

Leo: How dare you?

Steve: Without any problems.

Leo: How dare you run an old version of an operating system on new hardware? That's just horrible. I don't, you know, I, yeah, I'm really curious about all that. It's very interesting, yeah.

Steve: Yeah, we'll find out.

Leo: That's why you use Linux, frankly, is because you don't have to worry about shenanigans.

Steve: Well, and, yeah, you don't have Microsoft forcing you to do what they want you to do.

Leo: That's a seven-year-old operating system.

Steve: Wow. So I got a note, a nice note, which is only sort of tangentially about SpinRite, more about archiving, but I thought our listeners would find it interesting, from a Jeff Rocchio in Charlotte, North Carolina. The subject was "Archiving Data: Better to keep running with SpinRite or to power off?" And he said: "This isn't so much a security question as an availability question. I've been listening to your show for about a year now, and I've been enjoying the SpinRite stories, which have prompted a question.

"I had kids in the era of the Sony 8mm camcorder and have a bunch of videos on tape. About two years ago I bought two 1.5TB hard drives, configured a Linux workstation with the necessary video software, and captured all the videos off the tapes, digitized them, and now have two copies of them all on the two 1.5TB hard drives.

"So my question: How do I best guarantee long-term storage of these? I thought about a cloud service, but I think the capacity I'd need to buy is a bit much. It would take two many writeable DVDs to store them that way, and those can also be questionable long-term. So then I thought I'd take them out of my PC, put them in thick plastic bags, and store them in the classic 'cool dry place.' But then I began to wonder about the parts degrading over time, or even the magnetism losing its strength so they'd become unreadable. But leaving them running in the PC for years seems stressful, as well. But if I did this with SpinRite watching them, would that be better than powering them down and just leaving them sit on a shelf? What do you think?"

So a good and classic archival data storage question. Remember that the problem we've talked about before, for example, with DVDs is that those need to have a drive to read them, and at some point in the future it may be hard to get one. So make sure you have a DVD reader, if you were going to use DVDs, with the latest interface. It doesn't want to be, probably doesn't want to be IDE. It wants to be SATA now. And if that changes, or maybe USB 3.0, I mean, who knows? The problem is all of this is a moving target. And archiving really is a challenge.

I did, after seeing this question, jump over to Amazon Glacier and see what their pricing for putting things in cold storage in the cloud is. And they charge $0.007 per gigabyte month. So that's $7 per terabyte month, which would be about $10 for a not-quite-full 1.5TB drive. And I'm assuming he's duplicated this on two drives. It wasn't clear whether each drive is a copy of the other, or he's got actually nearly 3TB of data. But still, $10 per month is a lot of money. That's $120 a year for, what, 12 years, $1,200. Who knows?

So I guess probably the right thing to do is the thing that's the biggest pain, which is I would say you don't want to leave them powered up and running, just because you sort of have a wear-and-tear problem on the bearings. But neither do you want to let them sit for a decade in their plastic bags. You sort of want a compromise. You want to dust them off or take them out of their bag, you know, annually, and put them in a machine, and then do give them a SpinRite. SpinRite will - and you want to run Level 4 because that rewrites the data. So it reads it, inverts it, reads it, inverts it, and writes it a final time, and then verifies it. So that sort of exercises it and refreshes it to make sure that it's all still readable.

You know, six months or a year even sitting quietly isn't going to cause much problem. But then you'll know that it's still good. The other thing you'll know is that you still have a system that can run that drive. I mean, like everything required, because the lord knows, maybe tomorrow's chipset won't be compatible with old hard drives. Who knows? So something you care about, it'd be nice if you could absolutely forget it. And I would argue sending it to the cloud probably allows that with reasonable cost, but not for free.

So the alternative is that you have to become a little bit of the maintainer. You really want to do like an annual reminder to, like, get them out, give them a SpinRite run, and then seal them up again and put them away. And I'd hold onto that Sony 8mm camcorder and all the tapes, while you're at it. I think that's a digital technology, so imprinting would not be a problem over time, which analog tape storage tends to have.

Leo: Oh, that's interesting. Yeah, I mean, Hi8 could be analog or digital.

Steve: Okay.

Leo: And I have a lot of Hi8 tapes, and I've been really worried about them aging out. But you're right, that's a good point. The digital ones are probably fine, will be fine for a while; right? Until the mylar flakes off the iron-oxide.

Steve: That's the problem.

Leo: Then I'm screwed.

Steve: I have some of the old - of course I do - PDP-8 DECtapes.

Leo: Oh, wow.

Steve: Back from there. And a good friend of mine who's sharp this way noted that, you know, mylar on really old mag tapes is a problem...

Leo: Because it ages, yeah.

Steve: ...because it can delaminate, the oxide can delaminate from the mylar. What's interesting about the DECtape is their mylar sandwich with the oxide in the middle. So for some amazing reason, they're just meant to be really durable. They're still running on people who have them running on really early '70s-era DEC equipment.

Leo: All right, LostPass.

Steve: Okay. So here's what this amounts to. We've talked often about the fundamental problem with phishing, where typically email, very convincing-looking email, gets sent to someone. And oftentimes it's specific to them, like a focused attack. It's an administrative assistant at RSA, and the email is, like, focused on their business. I mean, it seems, you know, the targeted attacks do everything they can to look as convincing as possible. And we're just human. We go, oh. It's like, maybe it's something you're expecting. Or it's like the email that you've been receiving. Of course then the other hook for this kind of attack is where someone you know gets infected, and you receive email from someone you know. In that case it's you're trusting the sender implicitly, even though they didn't send it to you, malware sent it.

So now what we have is the first highly publicized phishing attack against LastPass. And this was a security researcher, Sean Cassidy, who's the Chief Technology Officer of Praesidio, presented this attack at the recent ShmooCon in Washington. And he called his presentation "LostPass." What he did was essentially clone the UI of LastPass, which is

entirely cloneable because it exists as web page elements. That is, it's a dialogue that's displayed by the browser using HTML and style sheets. And so you can capture that. And another site can display the same-looking dialogue. And these are the dialogues that LastPass uses for soliciting your username and password, and even your second-factor authentication.

So the whole exploit was you go to a site which is either malicious itself, or a good site that has a server weakness that allowed some page injection, the idea being that the "you are currently not logged in" bar which LastPass owners are familiar with, it's a red bar that shows in the page, at the top of the page, it comes up and says, hey, you know, you're not logged in. Log into LastPass. This, of course, in this case is fraudulent. It's a spoofed presentation, not from LastPass but from the attacker, injected into the page.

One of the other things that's possible, because LastPass the plugin needs to communicate with LastPass the HTML, that is, these dialogues that are running, there's a plugin API. So that allows the bad guy who's managed to inject some code into the page of a site you trust, or has tricked you into going to a site that you don't know not to trust, that code on the page can actively log you out of LastPass so that you are now actually logged out. Then the bad guys presents you with, essentially overrides LastPass's presentation of the login prompts, and you provide your credentials to the bad guy through this browser-based UI.

And the problem is, because it's browser-based, it looks the same as LastPass's authentic one. That means that the bad guy is able to acquire your username and password. And when the bad guy submits that to LastPass, the LastPass server API says, oh, you need now to provide your second-factor authentication. So then the bad guy says, oh, this guy has second-factor authentication, pops up the two-factor authentication, prompts you for that, intercepts that, returns that to LastPass, which is valid second-factor authentication.

And this of course is a man-in-the-middle attack. So this is a phishing man-in-the-middle attack. And as we've talked about before, nice as second-factor authentication is, it is not protection from a dynamic man in the middle that can intercept what you put in on the fly and then forward it on the bad guy's behalf to the authenticator. So that's what this is.

Sean contacted the LastPass guys, probably Joe - although he refers to a GM, I guess the General Manager, and maybe that's Joe, I don't know whom he spoke to, he doesn't use any names - and says that he contacted them. In Sean's presentation FAQ on his page he says, or he's asked: "Why did you develop this attack?" And he says: "I think that the security industry's view of phishing is nave at best, negligent at worst. Phishing is the most dominant attack vector and is used by everyone from run-of-the-mill CryptoLocker types to APTs," the persistent threats.

"The standard refrain is that we need better user training. That's simply not good enough," he writes. "The real solution is designing software to be phishing resistant. Just like we have anti-exploitation techniques, we need anti-phishing techniques built into more software. Security software evaluations should also include how easy it is to phish the software." And that's a really good point. That's not something which is typically done in a security evaluation.

And then his FAQ asks: "Did you tell LastPass?" And he says: "Yes. I informed them in November, and they acknowledged the bug in December. This has been a long and confusing issue," he writes. "At first LastPass understood this bug to be mainly a result of the logout [cross-site request forgery] CSRF," the cross-site request forgery. And that's

the part where part of this is his ability to actually force a logout so that you are logged out of your LastPass client, and then he's able to operate as a man in the middle for the re-login process.

And he says: "Then they suggested it wouldn't work because of the email confirmation step." And what LastPass was doing was, if you were not using two-factor authentication, and you were logging in from an unknown IP, they would then do email confirmation. So they said that would be a mitigation. The problem is that, if you are using two-factor authentication, LastPass felt that was strong enough, better even than the email loop. So they didn't perform an email confirmation from a different IP.

Leo: Interesting. So you're actually more vulnerable if you use two-factor.

Steve: Yes. Yes.

Leo: How interesting. Hmm.

Steve: He said: "One of the fixes they implemented to fix LastPass" - or, sorry to fix LostPass - "was to warn users when they type in their master password to some website. However" - meaning to some website as opposed to their dialogue. So what he's saying is that they've modified the LastPass plugin to watch what you do on any website you visit and to catch you putting your LastPass password into any website rather than into them. So that's a clever mitigation.

He said: "However, they display a warning message in the browser viewport, like all of their messages." And the point being they really don't have a choice. They're a browser-based plugin. "On an attacker-controlled website, it's trivial," he writes, "to detect when this notification is added. Then the attacker can do whatever. In LostPass, I suppress the notification and fire off a request to an attacker server to log the master password. We as an industry do not respond to phishing attacks well. I do not blame LastPass," he writes, "for this. They are like everyone else. We need to take a long look at phishing and figure out what to do about it. In my view it's just as bad, if not worse than, many remote code execution vulnerabilities and should be treated as such."

Now, LastPass of course immediately responded. And they explained everything that they had done to change LastPass back in December, well in advance of Sean's presentation just last week at ShmooCon. And so, for example, they now prevent logout. They write: "The first line of defense that LastPass has introduced is preventing the malicious page from actually logging the user out of LastPass. Even though the malicious page shows a fake LastPass notification saying the user has been logged out and needs to log in again, the user can see that the LastPass extension itself in their browser toolbar is still logged in."

Well, okay. That's kind of a weak mitigation. Unfortunately, I mean, I do look to see if my little LastPass icon is dark gray or showing that nice LastPass red. But, you know, I think if you get a big banner across the top of the page saying you're logged out, you're going to tend to fall for that. But still, again, they've done everything they could.

Then, what if the user misses that they're still logged into LastPass and clicks on the fake LastPass notification to log in again? So LastPass says: "Warning that the master password was entered on a non-LastPass page," which again is a nice mitigation. "Last

Pass will detect if the user enters their master password on a non-LastPass page and pops a strong warning, even before the user submits it to the page. The user will know immediately that their master password may have been compromised and can change it."

And then they also made a change to requiring verification for logins from unknown locations or devices: "LastPass," they write, "has a verification process that is required whenever a user attempts to log in from an unknown location or device. Cassidy claims in his research that it is possible for the malicious page to suppress any message LastPass tries to show in the viewport, thereby potentially preventing the user from seeing the above master password warning. So if the user does not see the warning and still enters their master password and their two-factor data, the attacker could then attempt to remotely log into their LastPass account. However, upon attempting to log in, they would be unable to gain access to the account without also completing the email verification steps. This requires access to the user's email address, or their security email address if enabled in their LastPass login."

So what LastPass did in response was that they removed the convenience of the email, or the inconvenience of the email loop in the event of two-factor authentication. That is no longer an exception. You will always be prompted for the email loop verification, even if you're using two-factor authentication. And they now also have added a warning in case your master - because they're checking now to see if you, by mistake, enter your LastPass password into a website that would probably be malicious, rather than into their own UI, they also have to make sure that you're not reusing your LastPass master password on any other sites.

So they now do that. They alert users when it detects that their master password is being used as a password on other websites because, of course, they want to warn you that you're using your LastPass password, probably in a way you don't intend, to log into some other site. But I could imagine users who wouldn't have understood the importance of keeping them separate.

So anyway, the problem is that this is a plugin that inherently can alter web pages, but cannot do things outside of the so-called browser viewport. They did ask the Google guys four years ago for some plugin API enhancement that would give a plugin special powers, like some other way of notifying other than an in-page, sort of an inline, in-page notification. And that's not something that for whatever reason the Chrome guys have moved on yet. But LastPass is still hoping for that.

And I ought to also, just to put things in context, as I mentioned at the beginning of the show, this is, you know, LastPass was the target of this because they're the big guy. I would argue that, because they're getting tested like this, they're now even stronger than they were, and much stronger than any other solution. So, for example, I'm not changing. I'm not going anywhere. I'm glad Sean did this and poked at this solution and came up with some clever ways of fooling the user, and then LastPass's response is, okay, thank you, we've added mitigations to those. Glad you brought it to our attention. And all of this was fixed long before this went public.

So this is the way the system is supposed to work. I'm glad that LastPass is able to update this on the fly. I'll note that all of the problem here is because this is entirely in the browser. A standalone LastPass app doesn't have this because then the bad guy's not able to cause the standalone app to do anything the way, you know, to emulate the browser-based behavior. But that's the whole thing. That's the story of LostPass.

In general, this is a problem. Phishing in general, the idea of bad guys being able to

emulate anything, whether it's email or a website we trust, emulate it maliciously, inject content into something we trust, or even pretend to be a password manager which we trust. This emulation problem is, and I completely agree with Sean, a huge problem that doesn't have an obvious, easy solution.

Leo: Ah.

Steve: Yeah. But, again, LastPass, those guys responded, I think cleverly, and addressed the things that Sean brought up, and essentially preemptively foreclosed on his attack. Which, by the way, he has published on GitHub, so anyone who's interested can experiment with it.

Leo: Take advantage of it. Is it fair to call it a bug in LastPass? Doesn't seem really - it's not like a flaw.

Steve: I wouldn't call it a bug, no.

Leo: A failure to do something correctly.

Steve: No.

Leo: It's a vulnerability, I'll agree with you, but it's not a bug.

Steve: Yeah. It is a vulnerability that was identified and responsibly disclosed and fixed before...

Leo: Mitigated.

Steve: And mitigated, yes, before it went public.

Leo: And it's because it's a Chrome extension. Is it the same issue on Firefox?

Steve: Yeah, yeah.

Leo: It is.

Steve: Yeah. In fact, in Sean's posting he shows - he says that Firefox was a little less easy, for some way that I didn't quite follow because I didn't dig in. But he shows his dialogue versus the real one, side by side. And he says, "Guess which one is real?"

Leo: You can't.

Steve: I mean, they're identical looking. You can't tell. Yeah.

Leo: Yeah. Phishing is the issue. In the past we've always said in phishing scams, just check the URL, the browser URL bar. But of course, because I realized, I said that on iOS Today yesterday. And I realized, no, no, that's actually not going to work because it's a Chrome extension that says "chrome colon." It doesn't give you a certificate or anything.

Steve: Yes. And in fact he got chrome-extension.pw. He bought that domain name so that it would even look like an extension domain.

Leo: They look the same. And there's no - can you check a certificate?

Steve: Yeah. But who's going to, is the point.

Leo: Okay. So you could still say, oh, wait a minute, yeah, I understand a phishing scam, you know, people are being proactive. I could have been bit by this easily because I never thought to check the veracity of the URL. If it looks right, it looks right.

Steve: Yeah.

Leo: Yeah. All right. And the mitigation, what does that mean for us as LastPass users? Do we not have anything to fear, or should we still be aware?

Steve: Well, we should always be aware. I mean, I do look around when I'm being prompted for things. Does everything look right? Does the URL look right? Do things make sense? In order for this to work, you had to be entering your LastPass master password into something other than LastPass. But because LastPass is there, it can monitor that. So it has completely shut this down. It has blocked this problem. I don't see any way around that.

Now, he says, and they didn't really address this, that their notification can be blocked by his malicious page, and maybe that's still true. So maybe, I mean, maybe this is an arms race, and he's upped the ante. But it's still possible for an updated attack to block LastPass trying to notify you that you are entering your master password into something that's not them. So, I mean, so this is just a weakness of the fact that it's browser hosted. But that's of course the great convenience of LastPass.

What we need, and we don't have it, is for plugins to be elevated to a higher level. The whole elegance of the plugin is just, you know, it participates in the browser space. And if it needs to say something, then it just uses the same browser viewport, which is what LastPass has been doing. But we need to make them a higher class citizen. We need to

make the plugins' presented content special so that no malicious page or server can emulate what our plugins are showing us, and we don't have that today. But really it's something that browsers ought to immediately provide.

Leo: Yeah. Okey-dokey. I appreciate it, Steve, and I guess I'll keep using LastPass. Although somebody makes a good point. As soon as you've put all of your passwords and your life into something you don't fully control, you're at risk.

Steve: Yup.

Leo: And I'm wondering if I should start looking at another - because really everything is in there, including passports, driver's licenses, social security numbers, I mean, it is a rich target.

Steve: Yeah. Well, the thing to do would be to find something multiplatform that is a standalone app. And it's not going to give you the integration that we enjoy with LastPass.

Leo: I could live with some inconvenience, knowing the risk involved.

Steve: Yeah, cutting, copying, and pasting. But it needs to be multiplatform because it's got to go on Android and iOS and Mac and Windows. And I don't know if it'll be compatible with the next generation of Intel chips. That's a problem.

Leo: Nothing is, including Windows. Oh, dear. Oh, dear. We'll talk about that on Windows Weekly tomorrow with Paul. I'm sure he'll have something to say.

Steve: I look forward to it.

Leo: Thank you, Steve. If you want to watch Security Now! live, you can. We do it every Tuesday, 1:30 Pacific, 4:30 Eastern, 21:30 UTC. It's a good live watch. You can watch me choke on a lentil, gasping for air, come back, recover - oh, I'm sorry, we edited all that out, so you never saw that if you watched the recorded version of it. You can get those recorded versions at Steve's - I didn't really - at Steve's site, GRC.com. He's got audio. He's got transcripts, nice transcripts.

And of course once you're there you might as well pick up a copy of SpinRite. Why not? It is the world's best hard drive recovery and maintenance utility. And really, if you've got a hard drive, you need SpinRite.

Steve: I have a very short slogan for it.

Leo: Oh, good, what?

Steve: It works.

Leo: It does. It does. It does. You should. He also has lots of freebies there. And find out about SQRL and Vitamin D. It's all there. And sleep. Do you have a sleep page?

Steve: It's a smorgasbord.

Leo: It's a smorgasbord. Do you have a sleep page?

Steve: I'll be doing a sleep page shortly.

Leo: Good. You can also get it from our site, TWiT.tv/sn for Security Now!, or wherever you get your podcasts. You should subscribe. You don't want to miss an episode. This is one show where really it's an encyclopedic look at computing, at technology, not just security, but everything. If you listen to all 543 episodes, you've got everything.

Steve: Sort of the whole gestalt.

Leo: The whole thing is there. The whole enchilada, if you want to use...

Steve: Yeah, we have, we've covered every base.

Leo: We have. And I love it.

Steve: Many times.

Leo: I've learned many things from listening to this show, from doing this show with Steve. Thanks for joining us, and we'll see you next time on Security Now!.

Steve: Thanks, Leo. See you next week.