SECURITY NOW!

Transcript of Episode #842

The More Things Change...

Description: This week we share some welcome news about Windows 11. Leo gets his wish about REvil. Microsoft improves vulnerability report management, attempts to explain their policy regarding the expiration of security updates, and prepares for the imminent release of the next big feature update to Windows 10, 21H2. Zerodium publicly solicits vulnerabilities in three top VPN providers. Three researchers disclose their new and devastating "Gummy Browser" attack, which I'll debunk. Another massively popular JavaScript NPM package has been maliciously compromised and then widely downloaded. We close the loop by looking at "Nubeva's" claims of having solved the ransomware problem. We touch on a new annoyance spreading across websites, and also briefly touch on four sci-fi events: "Dune," "Foundation," "Arrival," and "Invasion." I briefly update on SpinRite. Then we'll take a look back to share and discuss a conversation Leo and I had more than 20 years ago. What's surprising is the degree to which "The More Things Change..." how little, like nothing, actually has.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-842.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-842-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. There's a lot to talk about, including a maybe less-than-desirable way to get around ransomware. It seems like it perhaps is promising more than it can deliver. Why Gummy Browsers aren't really the threat that their discoverer claims them to be. And we're going to talk about REvil and what really happened to it. Plus then Steve's going to take us back in time 20 years to a visit he paid to "The Screen Savers." It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 842, recorded Tuesday, October 26, 2021: The More Things Change...

It's time for Security Now!, the show where we protect you, your loved ones online, protect your privacy, discuss how the Internet works, and maybe recommend a sci-fi book or two. That's the guy right here does it all, Mr. Steve Gibson of GRC.com. Hi, Steve.

Steve Gibson: Leo, great to be with you again.

Leo: Don't put your thumb to your - do the live long and prosper. That's much better, yeah.

Steve: Yeah, Lorrie gets upset when I talk about our final resting place. She's oh, no, don't, no, don't talk about that. Or anything. She's...

Leo: I'm with you, though. As you get a little bit older, you start thinking about these things, don't you. I mean, you've got many years left, I'm sure. You're very healthy.

Steve: I'm reconnecting with an old friend of mine after many, many years. And we were trying to figure out where to get together for dinner, and I suggested a Chinese place, figuring - because he's also a coder, and I figured, oh...

Leo: Coders love Chinese; right?

Steve: Exactly. And what he wrote was love Chinese, can't eat beef any longer, but pork, chicken, and whatever it was, you know, is fine.

Leo: This is sad, yeah.

Steve: And I thought, wow, it's going to be fun to catch up and compare our various...

Leo: Aches and pains. It's so funny, you know, because when you're young you kind of go, oh, those old people. But then suddenly you're one.

Steve: Yeah.

Leo: And you understand a little bit.

Steve: Yeah. And one of the things I really appreciate is the degree to which, you know, the human body just keeps on limping forward.

Leo: Yeah, yeah.

Steve: It's, you know, stuff begins to fall off, it's like, oh, well, what was that?

Leo: Looks like I left some gears back there.

Steve: Hope that wasn't an important piece, yeah. Well, and this is apropos, actually, of our topic. The title of the show today is "The More Things Change...," of course the first half of the famous phrase, "the more they say the same." This happened when one of my Twitter followers stumbled on a video which, given that it's exactly the same size that I originally created, and I've had links to them on the GRC site forever, it's made its way to YouTube. I didn't put it there.

Leo: Oh, yeah. Viewers do, yeah.

Steve: But someone calling themselves TechTV put it there. It's only about five and a half minutes long. The first three are shocking. It's you and I on Monday, April 9th, 2001, talking about security in the wake of something that has happened. And what is - I played this for Lorrie yesterday, you know, I mean, she's peripherally aware of what's going on because she's been with me for about four years, and so she's heard a lot of this. She was like, oh, my god. Oh, my god. I mean, and again, this is from 20.5 years ago. We'll play it at the end of the show and talk about it because, again, the more things change, it's just amazing how little has changed. But that's at the end.

We're first going to share some welcome news about Windows 11. Leo, it turns out you get your wish about what happened with REvil.

Leo: Oh.

Steve: Microsoft improves vulnerability report management. They also attempt to explain their policy regarding the expiration of security updates. Okay. And they prepare for the imminent release of the next big feature - I've got "big" and "feature" in air quotes - update to Windows 10. I know Paul and Mary Jo are kind of scratching their heads, too. This is 21H2. Zerodium has publicly solicited vulnerabilities in the top VPN providers, three of the top VPN providers, one of whom is a sponsor. Three researchers disclose their new and devastating, Leo, devastating Gummy Browser attack, which I will then proceed to debunk. We have another massively popular JavaScript NPM package which has been maliciously compromised in a supply chain attack, and unfortunately then widely downloaded.

We're going to close the loop by looking at a company called Nubeva, or Nubeva, I guess, and their claims of having solved the ransomware problem. Then we're going to touch on a new annoyance that has been annoying me - I just thought it would be fun to see if it hits you, too - which is spreading across websites, and also briefly touch on four sci-fi events: "Dune," "Foundation," "Arrival," and "Invasion." After a brief update on SpinRite, then we're going to play something that was recorded more than 20 years ago. And there isn't a listener who will not be thinking, oh, my god. So I think another great podcast.

Leo: Among other things, oh, my god, those two look so young.

Steve: Steve has hair. You look pretty much the same, my friend.

Leo: I don't know about that.

Steve: You're weathering pretty well.

Leo: And I might be a little distracted throughout the show. If I don't respond immediately to you, just go "Leo, Leo, put the MacBook down." Because Lisa brought my new MacBook over.

Steve: Well, just mute your mic so we're not hearing strange erotic sounds of glee as you open the box.

Leo: I promise. I promise. This is a good picture, I think, yeah.

Steve: Yeah. It's a great picture. I scanned through the video and found a representative moment in there where we were facing each other and talking.

Leo: What does that say? Patch War? PatchWork?

Steve: PatchWork. That was what invited me onto the show. The FBI contacted me, along with SANS Institute, and asked if I could create quickly, and it took two days, to create something which SANS could offer to allow anyone to quickly check whether their IIS servers were running with all of the - there were four critical patches. Anyway, and I only know any of that because I watched the video before our listeners have. And we're going to play it at the end of the podcast because, as I said before, what was - well, I've said enough. It was just startling to listen to what I was describing to you of what was going on then, and what all of our listeners know is going on today. So we'll have fun at the end of the podcast.

Okay. But first, something happened that I think is interesting for Windows 11 users. The good news is that Microsoft has jumped right on those pesky Win11 problems which we enumerated at some length last week, and will reportedly and hopefully, I mean, you know, hopefully because we've heard some of this before. Oh, we've got the printer fixed now. It's like, oh, wait, next month we'll get the printer fixed. And I heard you at some point, Leo, talking about people calling your weekend show with printing problems. It's like, oh, yeah.

Leo: I have a T-shirt that says "Don't ask me about printer problems. I don't want to talk about it." It's the worst. I hate it.

Steve: Okay. Oh, I know. So anyway, hopefully they're going to have them fixed up two weeks from now, on November's Patch Tuesday. However, anyone who's beset with the problems that next Patch Tuesday's updates are slated to fix, may jump the gun and preinstall the update without waiting. It's packaged as KB5006746. And googling that magic incantation, KB5006746, will take you right to it. I also have a link to it in the show notes. And looking at this link, when I was pasting in thought, you know, I guess Microsoft has just given up on the idea of a short URL. I mean, okay, Microsoft.com/en-us, right, the language.

Leo: Okay, okay. You could leave that out, probably, yeah.

Steve: Right, the language. Then /topic. Okay.

Leo: Okay, you need that.

Steve: Then now we need to have a date. So we've got October 21, 2021. Then we've got that magic KB5006746 number. And it's for OS Build, so we've got that, OS Build 22282; right? And it is after all a preview, so we've got to put preview on there.

Leo: Oh, yeah. Oh, yeah.

Steve: And then for lord only knows why, after all of that, which is entirely unambiguous, we've got a GUID, you know, a 03190705-0960-4BA4-9EE8-AF40BEF057D3. It's like...

Leo: They do love their GUIDs, don't they.

Steve: Certainly you're not going to type that in. So it's funny, too, because I had an elderly friend for a long time who was never able to enter the Windows Activation Code correctly. And I thought, you know, Microsoft has invented copy protection for old people. Because he'd just, he'd say, "Steve, you gave me the wrong code." I'd go, "No, Gary, I'm sure it's right." "No, no, no. I tried it 12 times. It doesn't work." And I'd go, "Okay, read it back to me." And sure enough, you know, a J was a K or something. It's like, "Okay, Gary, here you go." He would just say, "Oh."

Anyway, okay. I was going to enumerate the list of things that that URL, you know, the list is longer even than the URL is. And that's saying something. But oh my god, the list looks like the list of all the things they didn't get into Windows 11 earlier this month because someone on high said, "We shall ship on schedule." And I'm not kidding. The page's list is - and you click that link, you get a page. It's split into Highlights and Improvements and Fixes. There are 13 highlights for that link, and 64 improvements and fixes. I mean, it now shines your shoes. It's on there.

I scanned the list. And after listening to the podcast for a few weeks, it felt like home. It appeared that everything we've been grumbling about for the past month or two is present and accounted for there. So this fix should go a long way toward dealing with all those many edge cases. Okay. And specifically, it appears that Microsoft believes that printing is finally fixed. We'll wait and hear. They've confirmed that this update fixes Windows 11 known issues causing printer installation fails and prompts for admin credentials before every attempt to print on systems commonly found in enterprise environments, as we discussed last week. That's those HTTP connections, installing over the IPP protocol, and the inability to display custom print properties, all that, fixed. And you can have it now, everybody.

But hold on. The trouble with gaming on AMD chips, which reportedly got even worse after this month's patches, those are believed to be resolved. And the problems with slowly responding Bluetooth mice and keyboards have also been resolved. And that was really upsetting gamers. Although no true gamer uses a radio connection to their mouse. That's just - you don't do that.

Now, normally I would not recommend that our listeners jump the gun by installing a preview update. In the entire history of this podcast, I have never suggested that would be a good idea. But if you already jumped the gun by installing Windows 11, you're obviously afraid of nothing. And once you've scanned through the list of the 77 things that have been highlighted and fixed, this might just be another gun worth jumping. And besides, it feels like someone just pressed the "Ship It!" button a bit too soon on Windows 11, and this is just the stuff that didn't quite make it through the door before it slammed closed. So it's sort of the Windows 11 that you were meant to get. So I would say you could probably go ahead and do it two weeks early. If not, wait for two weeks, and then it'll appear in your, oh, look, we have some improvements to Windows 11. What do you know? Yeah.

Okay. Leo? This is where you get your wish.

Leo: Oh, yes?

Steve: REvil was recently retaken down by law enforcement.

Leo: Hacked by law enforcement.

Steve: Yup. Last Thursday, Reuters news service was the exclusive reporter that, according to three private sector cyber experts working with the United States, and one former official, the ransomware group REvil was itself hacked and re-forced offline in a multi-country operation.

Tom Kellermann, who is VMware's head of cybersecurity strategy and an adviser to the U.S. Secret Service on cybercrime investigations, he said that law enforcement and intelligence personnel stopped the group from victimizing additional companies. He said: "The FBI, in conjunction with Cyber Command, the Secret Service, and like-minded countries, have truly engaged in significant disruptive actions against these groups. And REvil was the top of the list."

As we detailed last week, the new apparent leader of REvil, who was calling himself "0_neday," you know, numeric 0_neday, who had helped restart the group's operations after its first shutdown, which took everyone by surprise - well, maybe not everyone - said that REvil's servers had been hacked by an unnamed party. Recorded Future reported that a Russian posting which they had translated into English, 0_neday wrote: "The server was compromised, and they were looking for me. Good luck, everyone. I'm off."

So we now also learn a bit more about what was behind the FBI's deliberate, and questionable at the time, withholding of that universal decryption key which would have helped victims of the Kaseya attacks. Remember that we found out that they had had it for a while, and it was like, hey, why didn't they let it go? Well, they needed to keep their cards close. That accounts for the delay. Following the attack on Kaseya, it turns out that, as we learned, the FBI did obtain a universal decryption key that allowed those infected through the Kaseya vulnerability to recover their files without paying a ransom. They got it by hacking.

The FBI later acknowledged that law enforcement officials had initially withheld the key as they quietly pursued REvil's staff. According to three people familiar with the matter, law enforcement and intelligence cyber specialists were able to hack REvil's computer network infrastructure, obtaining control of at least some of their servers.

Then UNKN, remember that guy U-N-K-N, UNKN disappeared; and later, this 0_neday guy and a few remaining team members returned and restored those websites from a backup last month. But in doing so they unwittingly restored and restarted some internal systems that were already under the control of law enforcement.

Leo: Oh, that's funny. Oh, whoopsies.

Steve: Yup, they restored from an infected backup.

Leo: Oh, my god. How's it feel? How did it feel? Good? How do you feel?

Steve: Yeah, how do you like them apples, yes. Oleg Skulkin, who's the deputy head of the forensics lab at the Russian-led security company Group-IB, he said: "The REvil ransomware gang restored the infrastructure from backups, assuming that they had not been compromised."

Leo: Is going to be good. Don't worry. We got everything. We saved it all.

Steve: That's right. "Ironically, the gang's own favorite tactic of compromising backups was turned against them."

Leo: Mm-hmm, mm-hmm, mm-hmm.

Steve: Officials have repeatedly declined to comment on the record. A spokesperson for the White House National Security Council declined to comment on the operation specifically. The FBI also declined to comment. But one person familiar with the event said that an unnamed foreign partner of the U.S. government carried out the hacking operation that penetrated REvil's computer infrastructure. And a former U.S. official, who spoke on condition of anonymity, said the operation was still active.

VMware's Tom Kellermann said: "The success stems from a determination by U.S. Deputy Attorney General Lisa Monaco that ransomware attacks on critical infrastructure should be treated as a national security issue akin to terrorism." And in June, Principal Associate Deputy Attorney General John Carlin told Reuters the Justice Department was elevating investigations of ransomware attacks to a similar priority. Tom Kellermann explained that: "These actions" - those I just named - "gave the Justice Department and other agencies a legal basis to get help from U.S. intelligence agencies and the Department of Defense."

"Before [this]," Tom explained, "you couldn't hack into these forums, and the military didn't want to have anything to do with it. Since then, the gloves have come off." So in other words, the U.S. military was finally engaged, and apparently getting into the hacker's inner sanctum wasn't so difficult.

Leo: That's awesome.

Steve: So score one for the big, lumbering U.S. bureaucracy. As we have observed before, these crypto cretins need to keep their heads down and under the radar. They made a big mistake when they poked the bear with a sharp stick.

Leo: Yes, yes, yes.

Steve: And, you know, it is this oft-quoted slogan that we are a country ruled by laws. Well, we could not legally do this until the nature of what was needed, that is, that we were combating, was officially assigned as a matter of national security at the level of terrorism. And that then created the legal basis by which the other departments that had had to have their hands off officially, they could roll up their sleeves and say, ah, thank you very much. That's what we wanted to hear.

Leo: Got 'em. Got 'em.

Steve: Yup.

Leo: Love it. Love it.

Steve: Done. So let's hope all of that underworld is listening because, you know, the sleeping giant can awaken. And when it does, whoops, there's one fewer top-tier cyberterrorism gang loose.

Okay. So Microsoft said, and this is good news: "We're Excited to Announce the Launch of Comms Hub." This is just yesterday. Microsoft's MSRC blog, you know, their security research group, posted the news of a new Comms Hub, a vulnerability reporting and research portal. Paraphrasing what their announcement was just for the content, they wrote: "We are excited to announce the launch of Comms Hub to the Researcher Portal submission experience." That's right. So researchers now have a portal submission experience.

"With this launch," they said, "security researchers will be able to streamline communication with MSRC case SPMs." And I looked everywhere. I googled SPMs. There's a lot of things it isn't. But I don't know what it is. They called it, they said in parens "(case managers)." So M is probably for Managers. I don't - security, okay, security...

Leo: Something.

Steve: Something, a P, and it's bad. So a bad thing...

Leo: Security bad thing manager. That's it, yes.

Steve: Right. Anyway, SPMs. So you can streamline your communication with these SPMs, whatever their Ps are, attach additional files, track cases and bug bounty status all in the Research Portal.

Leo: Ooh.

Steve: They said: "Currently" - yeah, woo. Currently - maybe it's got dark theme, too. I hope. That's very popular. "Currently, security researchers who submit via the portal communicate with MSRC via email." Oh. Who wants to do that? Maybe your mail was lost. Maybe that's why you don't think we responded to you. Unh-huh. Right. "To create a better user experience for the security researcher" - because as we know it couldn't be much worse - "we're excited to introduce the Comms Hub feature to the Researcher Portal. With Comms Hub, you will be" - you may not know what an SPM is, but you'll know what the Comms Hub is. "You'll be able to streamline communication" - oh, here we are again - "with your case SPM." They're really driving that fact home.

Leo: It's apparently the opposite of PMS. Whatever it is.

Steve: That's good.

Leo: Yeah.

Steve: You don't want that to happen.

Leo: No.

Steve: To your security submission.

Leo: Yes.

Steve: Anyway, view case status, add file attachments, and track the lifecycle - the lifecycle. Hopefully it's not a long lifecycle. We want this to die. We want it to be resolved and be like, okay, put to bed. Comms Hub provides chat functionality allowing asynchronous communications between researchers and the SPM. Wait. Asynchronous? Chat's not asynchronous. Chat's supposed to be synchronous. Maybe you just...

Leo: Well, you ask a question, an hour later they respond. It's asynchronous, yeah.

Steve: Okay, that's good. And the SPM, whoever they are, with all the relevant case data readily available, all within the Researcher Portal. Okay. I'm not even going to bother with the rest of this because everyone gets it; right? It's got a Reports page where all of your reports could be viewed. And you can click on one of those because it's got line items. And then it takes you to the View Case Details page where you can look at a single one. So hopefully, you know, certainly I think it's all good that Microsoft is working to improve upon and better manage their communication with security researchers who find and report problems with their software offerings.

What I'm hoping, I hope we can assume that the Comms Hub is the public-facing surface of a much deeper and significant mechanism within Microsoft for organizing and being responsive to reports of serious defects. For Microsoft, the story of 2021 was, more than anything else, an indictment over their horrifyingly poor response to the known security shortfalls of their products which enabled successful attacks upon many of their own customers. Perhaps there were some serious meetings last spring, after the mishandling of, for example, the Exchange Server flaws had become so apparent, with the result being that these new systems have now been put in place to prevent a repeat in the future. Let's hope.

Microsoft also has attempted to explain their policy for expiring updates. I encountered an interesting post by Microsoft, a somewhat shorter URL, but still two lines, regarding their policy surrounding the expiration of old updates. And I should preface this by noting that I've never had any idea how Microsoft manages the incremental updating of this operating system as well as they do, or at all, for that matter. As someone who builds projects from a large number of small files, I'm quite familiar with the idea of dependency trees and dependency resolution. But Windows has become so mind-numbingly sprawling that I can't even imagine how they keep the dependency definitions straight, let alone deal with the binary results of all of that. And as we know, it's an imperfect system; right? I mean, right now I have a system or two where update no longer works. It's like, okay. It broke, as it does.

In any event, it has always seemed to me that there's no point in installing a Windows update if a subsequent update is going to be replacing what the earlier update updated. On the other hand, if you don't wind up installing the subsequent update, or need to later back out of it, then that earlier obsoleted update starts looking pretty good. And speaking of backing out of updates gone wrong, it's one thing to install these things sequentially. That's at least conceivable. And then to later back out of them in a strict reverse order, right, just by putting back what each one replaced backing out.

But if you really want your mind blown, think about reaching in and removing some arbitrary update from the middle of a much larger batch, which Windows has somehow always allowed. Watching Windows Update run, I've often noted that the system's mass storage drive spends a lot of time not being in use. In other words, Windows is quite busy thinking. So perhaps individual Windows clients are spending a lot of their own time working out for themselves what to discard and what to roll back and what to keep. That wouldn't surprise me. But, boy, you know, I really do, tip of the hat to Microsoft for even attempting to do this on a consumer system, which is such a catastrophe. I mean, it's not like it's a beautiful blob of code; right? I mean, it's being updated constantly.

Leo: Well, its Mommy and Daddy think so. You're such a beautiful blob of code. You're so beautiful. I'm sorry.

Steve: Okay. So back to Microsoft's attempt to clarify this. They wrote: "Microsoft produces two to three updates per supported Windows platform monthly. This results in a backlog of updates and potentially increases the size of update packages. Many of these updates, however, are cumulative and include all earlier updates that have been published for that platform." God help us. Really? "That means..."

Leo: Well, that's the new thing, yeah, the cumulative rollup.

Steve: Yeah, right. "When older packages expire," and this expiration is a new idea, "you still receive the updates contained in those packages by installing the cumulative update." So they said: "By expiring older redundant packages, you get better performance, shorter scan times, a faster user experience, and reduced risk of deploying older updates which have been superseded with newer, more secure ones."

Leo: Also it's painful, you know this, when you install a new system.

Steve: Oh, Leo.

Leo: And you have to reboot 18 times and install, install, install.

Steve: Well, you're about to go on a two-week vacation, so you want to start Windows Update.

Leo: Now.

Steve: As the garage door is rolling up.

Leo: And just tell Michael, every once in a while just go hit ENTER and let it go ahead. Yeah. Maybe by two weeks it'll be done.

Steve: That's right. So they said: "Here are answers to common questions we receive about our Windows Update expiration policy." And of course it's no surprise that there are questions. Now, these are questions they've asked themselves; right? So they ask themselves: "How often are update packages expired?" Their answer to, now, remember a question they asked themselves: "Our published packages are evaluated for expiration on a regular basis."

Leo: We don't know.

Steve: No, we don't know how regular or irregular.

Leo: It just depends.

Steve: But, you know, we're going to do that. Then they said: "Once a large enough quantity of candidates have been found" - we don't know how many.

Leo: One, two, many, we don't know.

Steve: That's right. What's that straw with the camel? Anyway, "An expiration will take place."

Leo: Oh.

Steve: So again, they ask the question, how often are update packages expired?

Leo: Well, you know, it depends.

Steve: Yeah. So apparently as often as needed, or we feel like it, or the guy who does it came back from lunch. We don't know. Okay. "Why aren't older updates expired?" Again, they're asking themselves why aren't older updates expired? To which they answer:

"Some older packages may not have yet been evaluated." What? "Or may not have met the criteria for expiration" if they have been evaluated, apparently.

Leo: Somebody's still using them.

Steve: Whatever that means. "So it is also possible that they have not yet expired because" - now, this is the one thing that makes sense - "of existing dependencies on that specific update." So in other words, we expire older update packages when we want to and can. Okay.

Leo: As long as [crosstalk].

Steve: Right. Finally: "Are there any packages that cannot be expired?" So here we finally get some meat. "Security-only update packages for Windows 8.1, Windows Server 2012 SP2, Windows Server 2012, Windows 7 SP1, Windows Server 2008 R2, and Windows Server 2008 SP2 do not expire as they are not cumulative and hold only one month worth of fixes." Thus, Leo, the experience anyone who tries to install one of those things and update them - and you know I do occasionally. I've moved on, but, boy. You are literally - there is no concept of a cumulative update. You must go through a step at a time, one by one, and install every single one.

In other words, notice that all of that is up to Win10. They're saying that until Windows 10, monthly security update packages were not cumulative. They only contained the changes for the current month. Thus all previous updates always needed to be installed first. And you can't expire any of those if some crazy person - you know, guilty - wants to update one of those Windows offerings. I mean, there are still valid reasons to run those; right?

Leo: Sure, yeah.

Steve: Like for developers who have to make sure their stuff runs on those older packages. So, yeah. Anyway, it wasn't until Windows 10 that any single month's security update package could be used to bring any system current. And that's the good news. You could have - in fact, I've seen this happen where - because Lorrie has a stack of 20 laptops that she uses for remote neurofeedback, which clients do at their home.

Leo: Oh, that Windows Update must be a fun day for you at that place. Holy cow.

Steve: But that's the point. They are, we are running Windows 10. And so I can dust one of those off. And even if it hasn't been turned on for six months...

Leo: Right, one update.

Steve: ...it only installs the most recent month. And it is made current.

Leo: Yeah. This is a huge, I think, a huge improvement in how they do this.

Steve: Yes.

Leo: They needed to do this.

Steve: Yes. And so, and then the last question: How can I find out if my update was expired? It's not hard. If an update was expired, you will see the word "EXPIRED" appended to the title of the release note article associated with that specific update on support.microsoft.com.

Leo: I was going to say sniff it and see if it smells bad. I don't know.

Steve: Okay. So anyway, that's basically, if something new has completely replaced something old, and it's for Windows 10, yes, then they're going to just say, okay, this is expired. You should not be installing something old and stinky. Just make yourself current.

Okay. And while we're on the subject of Windows Updates - in Windows 10, not 11, but that applied to both - those who have chosen to remain with Windows 10 will probably be interested in knowing that the next big feature release, known as 21H2, will be rolling out in a few weeks. It's now available to Windows Insiders in the Release Preview Channel. Microsoft's John Cable, VP, Program Management, Windows Servicing and Delivery -and I guess he's the guy who slammed the door and kept those other Win11 things from making it into the release, but now you can add them.

He said: "Windows 10 version 21H2 will have a scoped" - I don't know what this language means - "a scoped set of features focused on productivity and security, prioritized to meet our customers' needs based on feedback." Or as Lorrie would say, "Blah blah blah blah blah." Anyway, he said that 21H2 would include WPA3, that's cool, H2E standard support for enhanced Wi-Fi security. So you get that, if there's anyone for it to talk to who also has WPA3. "Windows Hello for Business," he said, "introduces a new deployment method called 'cloud trust' to support simplified passwordless deployments and achieve a deploy-to-run state within a few minutes."

Now, hold onto that thought because then he contradicts himself. GPU compute support in the Windows Subsystem for Linux (WSL) and Azure IoT Edge for Linux on Windows deployments for machine learning and other compute intensive workflows. So the Windows subsystem for Linux is getting some boosts. But then Microsoft just said yesterday that they were still finalizing that Windows Hello for Business cloud trust deployment method, and that it would be subsequently launched in a monthly update. So apparently not in 21H2. That didn't make it, either. Boy, they're slamming doors on things.

Anyway, once it's out, 21H2 will receive 18 months of support for Home and Pro editions, and 30 months for Enterprise and Education editions. And just for what it's worth, I do recall Paul and even Mary Jo ho-humming this 21H2 update and being anything but excited, even to the point of Mary Jo asking Paul if there was any there there. I'm sure everyone who wants to remain current with Windows 10 will want it. But there doesn't appear to be anything new and exciting.

Leo: No, no.

Steve: For Linux, yes. But for Windows? Not so much.

Leo: Linux has been updated, yeah.

Steve: Wow. Oh, and the corners are still quite pointy.

Leo: Oh, well, that's no good. We've got to round those off.

Steve: Yeah, well, that's where you jump the shark and...

Leo: You don't have your Start Menu on the left like an animal, do you?

Steve: It did get fixed, by the way. Remember the Start Menu that didn't update for users who wanted it to, now they're updating, so that's good.

Leo: Oh, thank you.

Steve: And Leo, we're going to discuss - I heard you on MacBreak Weekly talking about, and this was freaky, I didn't realize there were two anniversaries on the same day. You were talking about on MacBreak Weekly the 20th anniversary of the iPod.

Leo: That's right, yeah.

Steve: Yesterday.

Leo: Yeah, October 25th, yeah.

Steve: There was a different anniversary, 20th anniversary, we'll talk to after you tell us who's paying for this.

Leo: Things were hopping 20 years ago.

Steve: That's right.

Leo: Including us. Usually when you mention an acronym, the chat room, we've got two of them, we've got the Discord in our Club Twit, we've got our IRC, comes up with a name. No one has yet figured out what SPM is. The closest anyone came, and this is from Microsoft's AllAcronyms.com, Shared Property Manager. I don't think that's right. I don't think that's correct. Anyway, no one knows it. Typical; right? Great acronym. No one knows what it means. And everybody's probably too scared to even ask; you know? Oh, yeah, it's SPM.

Steve: And, in Microsoft's own posting, they put parens afterwards and said whatever it was, account manager or something.

Leo: They didn't even give you the right thing. Oh, wow.

Steve: Right.

Leo: They don't know either.

Steve: So the other birthday that occurred yesterday, Windows XP, 20 years. The 20th anniversary of Windows XP.

Leo: And people are still using it.

Steve: Do you know, one in 167 machines are running XP. That's 0.6% of all Windows, I mean, that's not nothing.

Leo: It's better than I thought, to be honest. But still it's way too many. It's probably millions; right?

Steve: Well, I'll bet they're in, you know, they're keeping ATMs and kiosks alive. You'll see it crash on some stadium screen. It's like, oh, look, they're still running XP. And, you know, it occurs to me, as I think about XP now being 20 years old, that I've always been grumpy about Windows being changed. I've always wanted Microsoft to just please leave it the you know what alone. You know, fix it, yes. But stop constantly changing it just for the sake of having something new to sell.

I recall on the occasion of XP's birthday complaining at the time that they had just taken the very utilitarian and extremely functional Windows 2000, there was nothing wrong with Windows 2000, it was rock solid, you know, it was the evolution from NT. And they added, as I described it, a thick candy-colored sugar coating to Windows 2000's UI, I mean, just made it all pretty colored, and with the same operating system underneath. And in fact that of course was a bone of contention because it also brought the raw sockets that Windows 2000 had...

Leo: Oh, that's right.

Steve: ...over to a consumer OS.

Leo: Wow, right. You were really inveighing against that, I remember.

Steve: It was a mistake. And, you know, it took a while...

Leo: They backed down, yeah.

Steve: ...for them to say whoops, that's what he was talking about. But it took them getting attacked to see the light. Anyway, speaking of attacked, last Tuesday the 19th, Zerodium tweeted, and I have a picture of their tweet in the show notes. On October 19th: "We're looking for #0day exploits affecting VPN software for Windows." And they enumerate the three: ExpressVPN, NordVPN, and Surfshark. They said: "Exploit types: information disclosure, IP address leak, or remote code execution. Local privilege escalation is out of scope."

Leo: Huh.

Steve: Meaning they don't want that. They don't want just any exploit.

Leo: No, they want to get in.

Steve: They want to identify is what those...

Leo: Oh, identify, yeah, yeah.

Steve: Yes.

Leo: Or remote code execution, which is always nice.

Steve: Yes. If you can run code, identification is then not a problem.

Leo: We should mention ExpressVPN's a sponsor. But we should also this doesn't - this actually could be encouraging. It means they don't have them right now; right?

Steve: Correct. And sadly, it also means there's a demand.

Leo: Somebody's looking for them, yeah.

Steve: Yes.

Leo: Guess who? What do you think? Yeah.

Steve: Uh-huh. So as we know, Zerodium's in the business, unfortunately, of reselling software vulnerabilities. Literally. Let me say that again. They resell software vulnerabilities. It's like, what? They appeared in 2015, headquartered in Washington, D.C. That's convenient. And we've been following their exploits, if you'll pardon the pun, ever since. Their sleazy business model is to purchase exploits for freshly discovered and unknown zero-day vulnerabilities occurring in high profile and often targeted applications, as is the case here. And then compile, catalog, and resell those exploits to government and law enforcement agencies. And what do we imagine those government and law enforcement agencies do with said exploits?

On this podcast, we spend a lot of time focusing on the good guy hackers, who participate in public Pwn2Own competitions or who responsibly report their valuable vulnerability findings to a bug bounty program, either an independent clearinghouse or directly to the affected company. All of the major companies pay one way or the other now to learn of responsibly disclosed vulnerabilities in their own software. It's become part of what a security responsible company does.

And then there's Zerodium, the fly in the ointment. And they do pay big. Security researchers are encouraged to sell their exploits for up to $2.5 million, depending upon the type and target of their discovery. And from time to time Zerodium has launched limited time bug acquisition drives during which they express their desire to purchase zero-day exploits in non-standard software. Some previous acquisition drives have targeted specific routers, cloud services, mobile instant messaging clients, and even something as niche as the Pidgin app, which is popular with cybercrime organizations. Major VPN providers such as the three now being targeted by Zerodium, manage networks of thousands of VPN servers located across the globe, rerouting their customers' web traffic or other communications traffic to mask their users' physical location, under the premise that where someone is, is no one else's business.

What's interesting is that these VPN services work with VPN clients residing on any OS platform, right, Windows, macOS, Linux, Unix, iOS or Android. But Zerodium's solicitation last week plainly stated that they were only interested in exploits targeting Windows clients, and specifically exploits that can disclose a VPN user's personal information, that can reveal the user's real-world IP address, or exploits that allow remote code execution on the user's computer. This suggests that there's a market among governments and law enforcement for the targeted penetration and determination of the identities of VPN users who are proactively protecting their privacy and identity using the services of these major VPN providers.

We know that not everyone who uses a VPN does so merely to geo-relocate themselves for the purpose of accessing locally embargoed media content, or to keep their nosy ISPs out of their business. There actually was a story that I looked at it, but it didn't quite make the cut, about how much more data ISPs are collecting on their own customers than is normally understood. Anyway, it's certainly the case that criminals also use VPN services to evade law enforcement. So, yeah, as always it's a double-edged sword. But something still feels very slimy about having an agent of the government and other three-letter agencies, which is exactly what Zerodium actually is, actively soliciting for vulnerabilities in products designed to protect their users.

Leo: Do you think Zerodium is - they're not run by the U.S. government. You're not saying that.

Steve: No. No. I don't think...

Leo: I think that they work for a variety of - they work for whoever pays the most; right?

Steve: Yes. So I'm sure they're selling their stuff, well, that's how they can afford to pay $2.5 million...

Leo: Yeah.

Steve: ...for something juicy is that essentially they're a subscription service; right? The various governments subscribe, and they're collecting taxes, and some of it goes to Zerodium. Three-letter agencies subscribe. So the idea is they're generating a cash flow from across the globe, or rich, well-monied organizations that have an application for unknown vulnerabilities in...

Leo: Usually governments.

Steve: ...software across the board, yes.

Leo: Yeah, nation-states or their agencies.

Steve: Well, you have to be to have that much money, to be able to subscribe and say, yeah, you know, tell us about anything you find. We want it all.

Leo: Well, we just saw that The New York Times tech reporter was hacked. His iPhone was hacked...

Steve: Yup, over and over and over.

Leo: ...by Pegasus, which is the NSO Group, which is an Israeli company.

Steve: Yup.

Leo: And probably at the behest of Saudi Arabia or one of the countries he's reporting on.

Steve: Yup.

Leo: And, yeah. The good news is that these are so expensive, you're not going to see these in day-to-day exploits against you and me.

Steve: No. Well, and that's the other thing, too, is they're only valuable until they're known. So certainly part of the agreement that Zerodium has with their buyers, no, obviously their seller cannot ever tell about the thing that they're selling. But their buyers have to exercise extreme care in using them. So, yes, targeted attacks because the moment anyone finds a vulnerability, just like Apple, you know, they jump on these things immediately and work to shut them down, the moment that they figure out how the NSO Group has managed, got Pegasus running in their iPhone again.

Leo: Right, right.

Steve: Okay. So this is fun because this is not serious. Despite the fact, well, I mean, it is serious, but it shouldn't be. The article, the paper describing this devastating attack even has your beautiful lines pointing, numbered lines pointing in every direction. Visit the attacker. Number two, acquire user's browser fingerprint. Three, users' browser information. Four, visit, I mean, going around and around.

Okay. So in preparing each week's podcast, I survey the news of the past week, selecting those items that I think are important and that our listeners should be informed of and/or would enjoy. And I typically skip over dumb things that don't merit our time. But in this case...

Leo: Good.

Steve: Yes, exactly. I was caught off guard by the exaggerated descriptions of this new and reportedly devastating attack. These are the headlines in the tech press. One of the things that heightened my expectations was that the story was widely picked up across the tech press. So it was with some anticipation as I had acquired a whole bunch of tabs that I clicked this tab to turn my attention to see what was going on. This might have been the title article.

Leo: Huge. Huge.

Steve: The title story of the podcast.

Leo: Yes.

Steve: The paper was authored by three researchers, two from Texas A&M University and the other from the University of Florida. And it's titled "Gummy Browsers: Targeted Browser Spoofing Against State-of-the-Art Fingerprinting Techniques." Its abstract reads - that's only the first half because I couldn't tolerate going any further. The abstract reads: "We present a simple yet potentially devastating and hard to detect threat called Gummy Browsers" - and I had to make sure this wasn't published on April 1st, but no, I mean, they're serious about this - "whereby the browser fingerprinting information can be collected and spoofed without the victim's awareness, thereby compromising the privacy and security of any application that uses browser fingerprinting." Okay.

"The idea is that the attacker A first makes the user U connect to his website or to a well-known site the attacker controls and transparently collects the information from user U that is used for fingerprinting purposes just like any fingerprinting website W collects this information. Then A, the attacker, orchestrates a browser on his own machine to replicate and transmit the same fingerprinting information when connecting to website W, fooling W to think that user U is the one requesting the service rather than attacker A. As a consequence, if website W populates targeted ads for user U based only on fingerprints, attacker A can now start seeing the same or similar ads on his..."

Leo: Ooh.

Steve: I know, Leo. Oh, my god.

Leo: He can see your ads. Oh, no.

Steve: He can see and he might get the same ads you got on his browser as user U would see. This will allow the attacker to profile user U and compromise U's privacy.

Leo: Oh, lord.

Steve: I know.

Leo: Terrifying. Now, I'm interested because it sounds like you could also use this to fuzz your fingerprinting. So you could use it defensively, I would imagine.

Steve: Well, so in other words, if a website uses advertisers who only employ browser fingerprinting rather than cookies to identify their advertising targets - which is, of course, very fuzzy identification, certainly browser fingerprints we know are not unique - then it would be possible to capture a victim's browser fingerprint by causing their browser to request an asset from an attacker-controlled web server. Then that attacker-controlled web server could query the original website while deliberately echoing and presenting all of the features of the original browser's query which are fingerprinted by that site's advertisers.

Now, of course, that assumes that the attacker was also querying and reproducing the identical set of browser fingerprintable features, and that's unknowable. As we know, sometimes they do weird things like illumination level or battery level, right, which is captured via JavaScript. So the attacker doesn't know how the advertisers are fingerprinting in the first place. So all they can do is a best guess, which probably adds some additional fuzz.

And in this way the attacker would, yes, be spoofing the website's advertisers into believing that the attacker is actually the user, which - and this is the great headline-grabbing concern of these browsers - would allow them to "profile the users." Oh, my. But anyway, you got it, Leo.

Leo: Yeah.

Steve: You know, I originally thought that listening to the audio in a remote room by bouncing a beam of light off a vibrating bag of potato chips was of questionable value. But this one might actually be even less useful.

Leo: I can see your ads.

Steve: In the words of the authors, yes: "We present a simple yet potentially devastating and hard to detect threat called Gummy Browsers." Devastating? Not so much.

But here's a baddie, and this is in all seriousness. This is a user-agent parser NPM package was maliciously altered. Now, what we're seeing is that one by one successive chunks of the technology the world has created for the benefit of everyone are falling to abuse by bad actors. The trouble is security is difficult, and it's not automatic. Attacks on the software industry's software module supply chain are extremely worrisome because that supply chain was never really secured.

And there are all manner of ways for bad guys to get their malicious code into the systems of unsuspecting end-users and packaging developers. We've discussed a few of these various means of subversion, if you'll pardon the pun, in the past. Like posting something malicious under the name of something real, but having a higher version number than the latest real version. Insecure packet managers may encounter that higher-numbered malicious package, believe that they no longer have the latest and greatest, and so download the malware for incorporation into their next builds. It's a mess. That has happened before, as we've described.

Okay. So in that vein, we learned just last Friday that a massively popular browser user-agent header parser named UAParser.js, which is packaged as a JavaScript NPM and is routinely downloaded - get this, Leo - six to seven million times per week.

Leo: Wow.

Steve: Yes, on average a million downloads a day. It was compromised. Of course naturally you'd want to target something that was that popular. It was compromised and, yes, then massively downloaded. I mean, and this is enough for CISA to make an announcement. We'll talk about that in a second. The compromise installs a password stealer, a cryptocurrency miner, and worse on systems where the compromised versions were used. According to the official UAParser.js official site, the library is used by companies such as - we've heard of them - Facebook, Apple, Amazon, Microsoft, Slack, IBM, HPE, Dell, Oracle, Mozilla, Shopify, Reddit, and many of Silicon Valley's elites. The compromised versions were 0.7.29, 0.8.0, and 1.0.0. So obviously he's maintaining three major version threads. The patched versions are 7.30 rather than 29, 8.1 rather than 8.0, and 1.0.1 rather than 1.0.0.

The library's author, Faisal Salman, wrote: "I believe someone was hijacking my NPM account and published some compromised packages which will probably install malware." Yeah. Probably, indeed. A few hours later, after discovering the hack, Salman pulled the compromised library versions to prevent users from accidentally infecting themselves, and he replaced them with clean copies, updating their version numbers.

Subsequent analysis of the malicious code revealed extra scripts that would download and execute binaries from a remote server. The binaries were provided for both Linux and Windows platforms. On Friday, a GitHub user said: "From the command-line arguments, one of them looks like a cryptominer, but that might just be camouflage."

But on Windows systems, the scripts also download and execute an info stealer trojan, which might be a version of the DanaBot malware. According to another GitHub user's findings, it contains the capabilities to export browser cookies, thus allowing for browser session logon hijacking; also exports browser passwords and OS credentials. Because of the large number of downloads and the big-name corporations that relied on the library, the U.S. Cybersecurity and Infrastructure Security Agency (CISA), also the worst named agency there is, published a security alert late Friday night about the incident, urging developers to update to the safe versions. They just wanted to make sure the word got out.

GitHub's security team also took note of the incident and issued its own advisory, urging immediate password resets and token rotations from systems where the library was used as part of development processes. They wrote: "Any computer that has this package installed or running should be considered fully compromised. All secrets and keys stored on that computer should be rotated immediately from a different computer. The package should be removed. But as full control of the computer may have been given to an outside entity, there is no guarantee that removing the package will remove all malicious software resulting from installing it." And as we once said, oh, my god, Leo, at the dawn of this podcast, once a computer has been compromised, you never can really trust it again. You just have to restore from a pre-compromised backup and then move forward.

And just for the record, this was the fourth malicious NPM package found this week. On Wednesday, Sonatype also found three newly released NPM libraries that contained similar malicious code, intended to download and install a cryptocurrency miner targeting Linux and Windows systems alike. So it may very well have been the same attack going against a different package. So, yes. Houston, we have a problem. As I said, we built so much of our world under the assumption that sharing and collaboration would make us all stronger. Without any doubt, it does. But it also inherently opens us to infiltration by those wishing to take advantage of the trust that's inherent in online collaborative efforts. So these are problems we have, as we'll see in a little bit. We apparently still had the same problems 20 years ago. Let's please hope that 20 years from now, from our rocking chairs, Leo, you and I will note, well, they finally got that fixed.

Leo: I am almost certain that will not be the case. These package managers are inherently problematic because people contribute to them. There's not a lot of checking. And so really the burden is on the user to inspect the script and make sure that they understand what the script does and so forth. But these are all over the place. NPMs are very, very popular; but Python has its own system. Linux itself has systems like this. I use a version of Linux called Arch that has an Arch User Repository, and anybody can put anything there. And of course people also download stuff from GitHub all the time. So there's a lot of vulnerability out there.

Steve: The best you can do, I think, is if you're going to be using these, then stay current. Be absolutely sure that you're in the loop to receive notifications because basically that's the price you pay for the otherwise, well, look what I can get for free.

Leo: Right.

Steve: It's like, yeah, but it might bite you in the butt. So if you're going to get it for free, make sure you also get the communications that follow because it may save you.

I found a really interesting post for our Closing the Loop. Tom Andreas, looks like Mannerud, or Mannerud maybe. Anyway, he said: "Steve, have you heard of Nubeva before? I just came across them recently and was fascinated by their technology. Seems they are turning the ransomware game on its head. Their technology intercepts and stores the encryption keys used by ransomware so that you can restore your files without needing to pay ransom or restore from backup." He included a link. And he said: "I would be curious to hear what you think." And oh, boy, Tom, are you going to hear.

Okay. So I was interested, and I went looking to see what was up: www.nubeva.com. Nubeva's claim to fame appears to be what they call "TLS Decryption Evolved." Okay, TLS Decryption Evolved. Think about that for a minute. That's not supposed to be possible. The banner on their homepage says: "Nubeva's patented" - because of course it is - "SKI" - fortunately we're not left to wonder what that stands for - "(Session Key Intercept) software technology delivers a breakthrough solution for modern TLS decryption. SKI decrypts any TLS, with trailblazing price performance and ease of use." Because, you know, if you're going to decrypt TLS, might as well do it in a trailblazing fashion and make it affordable. "Nubeva licenses SKI" - that's the Session Key Intercept - "to fill growing capability gaps in legacy decryption and simplify operations for inline and passive cybersecurity and application monitoring solutions."

Okay. So this claim raises all manner of questions because the entire point of TLS is explicitly to prevent any third party from being able to obtain the communication's session keys. Digging a bit deeper, under their homepage headline, we find "See Into Any Session." And they explain: "To inspect TLS, each session's shared encryption keys are needed to decrypt." True. "With SKI (Session Key Intercept), Nubeva delivers a reliable, secure, scalable, and nondisruptive means to learn and extract session secrets from servers or clients at the time of creation via the handshake, and transport for use on authorized decryption functions. After use, keys are destroyed, thus ensuring the highest levels of secrecy. Nubeva licenses software to get keys, securely handle keys, and use keys to decrypt." Ah, okay.

So now it becomes clear. They said: "...means to learn and extract session secrets from servers or clients at the time of creation via the handshake...." So this patented Nubeva technology is not a man in the middle, it's a man deeply embedded into one of the endpoints. From that vantage point it watches the TLS handshake and captures the symmetric encryption key once it's been determined.

Under product details they say: "Supporting a growing list of platforms and OS including containers, Kubernetes DaemonSet, Windows service, or Native Linux Daemon." Okay. So it's not a universal solution, either. For example, under Windows, they've reverse engineered Windows crypto library, where TLS is always negotiated, that is, unless a pesky third party like Firefox brought along its own crypto library. But in any event, they've built, apparently, a set of hooks into Windows' crypto library so that they can snapshot its working memory to identify and capture any negotiated keys on the fly. And they've done something similar for Linux and Kubernetes with "a growing list of platforms."

Okay, I suppose that's useful, though it's not entirely clear exactly how, since the interception, such as it is, occurs at an endpoint where you also inherently have the pre-encrypted and post-decrypted plaintext directly available. It seems like the hard way to skin that particular cat. And this has nothing to do with ransomware, but it gives us a starting point for understanding their next set of claims, which is on the link that Tom provided under "ransomless_decryption."

On that page they say: "Nubeva for Ransomware Universal RansomLess Decryption." Sounds great. Where do I get some of that? And then they continue: "The RansomLess Decryption is a product development effort by Nubeva to build a revolutionary and systemic solution to this worldwide threat. Not another defense system. Not another backup system. Nubeva enables the reversal of ransomware's encryption with RansomLESS decryption" - and LESS is in all caps - "and recovery. Our solution is an adaptation of our patented" - that's right. Oh, get a patent on that - "Session Key Intercept technology, in which Nubeva has perfected the ability to reliably learn and extract the symmetric keys used in ransomware to encrypt files."

Okay, wait. They've "perfected the ability to reliably learn and extract the symmetric keys used in ransomware to encrypt files." Hmm. Okay. "We can reliably get keys copies of the keys" - a little typo there - "right at the moment of encryption, before they are locked with the asymmetric encryption process or exported to command-and-control servers. And with the file encryption keys available, decryption is simple and immediate. And we can do this not just for old and extinct ransomware variations like many tools on the Internet, we can get keys for all modern and historic crypto ransomware, thus delivering a universal solution." Boy, if only that were true.

Leo: Oh, it's not?

Steve: Well, okay. "When the attackers get through defenses, there is no need for lengthy recovery processes from backups provided you have them, they are current, and weren't turned off or corrupted by the ransomware, too. Instead, simply decrypt and restore without paying, with Nubeva's RansomLess decryption and recovery." Wow.

Leo: I like their name, Nubeva, too. That's so good.

Steve: I know, Leo. And there's something I could say that was off-color. I'm so...

Leo: Oh, no, please.

Steve: But I skipped it. Anyway, their page then shows us three videos in a horizontal grid or alignment, one for REvil, one for Araran - I don't know, I've never heard of it - AraranLocker/Venus, and one for another one I've never heard of, Zariza. In each case, you click the video, they have their solution installed in the system when the ransomware is triggered. And sure enough, their system captures the encryption keys at the time of encryption.

Leo: Yeah? I do recognize Sodinokibi. That's the big one, of course.

Steve: Yeah, of course, right.

Leo: That's REvil, yeah.

Steve: Yeah, REvil. So the end of this page then declares, again: "Not another defense system. Not more storage or system backup services. Decrypt without paying." Well, of course you have to pay them, and remember it's patented. "You already have the keys," they say. And then literally they have "We get the keys!"

Leo: We do.

Steve: "Nubeva's core intellectual property, Session Key Intercept, is software that can reliably, efficiently, and securely discover symmetric encryption keys of application processes and services running on computer systems that are used for bulk symmetric encryption. We have mastered this ability for TLS session keys to enable better, faster, and easier full packet inspection and protection of network traffic. We have proven we can do this for SMBv3 file-sharing traffic. Now Nubeva has successfully applied this IP to ransomware and is working to bring it to market in partnership with the selected leaders in security solutions, business, and government."

Okay. What I believe that they have actually shown is that with a specifically constrained environment such as TLS or SMBv3, on specific platforms for which they are designed, they are able to capture the symmetric keys of those processes that they know. So this leaves us with two big questions. First, how generic can this really be? It would be entirely possible to reverse engineer a specific piece of ransomware for the purpose of building an interceptor for that specific ransomware, much as they did for TLS and SMB. Then, assuming that this Nubeva agent was already running in a system which was subsequently the victim of exactly that same ransomware which Nubeva had been previously trained to observe and intercept, then yeah. It would be just like those videos.

So the question is, as I said, how generic can it be? I think that's to be determined and proven, and that's where I'm exceedingly skeptical. They're claiming that this is an extension of their existing proven and, oh, yes, very deeply patented technology. But calling it an extension, I think, stretches the meaning of the term, probably past the point of breaking.

The second big question is, if you have a software agent that's running in a machine which is already paying attention to what's going on and is able to see that some ransomware running in a given process has just generated a symmetric encryption key in preparation for encrypting a file, why not just immediately terminate that process...

Leo: Yeah. What a good idea.

Steve: ...with extreme prejudice, send an emergency note to corporate IT headquarters, and shut down the machine?

Leo: Oh, yeah. Look to see what the key is.

Steve: Why would you patiently sit there watching the ransomware go about its dastardly business, frantically recording all of the keys it's using to encrypt, and letting it do so? And where are all those keys going to be stored, anyway? Hopefully they don't get encrypted. Anyway, thank you, Tom, for pointing us to what really seems like a harebrained idea. It's unclear, even in the case of TLS or SMBv3 interception, what problem is being solved by implanting an agent into an endpoint to capture the negotiated key for the purpose of decryption when that endpoint also contains the plaintext? Why not just get the plaintext?

And it's not at all clear that this technology can really be extended beyond that somewhat questionable application and made into a generic symmetric key capture utility. When we had Heartbleed, which was capturing snapshots of RAM and, sure enough, was able to discover live server certificates in that RAM, it was able to do so only because it was finding certificates. A certificate is a rigid and fully specified highly structured block of data. So it can readily be discovered, with a near zero false positive rate, simply by scanning through RAM, looking for specific attributes that a certificate will have, then seeing if more of them are present where they should be relative to the ones you saw and confirming that, hey, look, we actually found a certificate.

But a symmetric key has no structure. As we know, it's just a block of 32 bytes, in the case of a 256-bit symmetric key, of maximum entropy random binary data that, from the perspective of an outside observer, could be anything. It's only if you know precisely where it is that you could know what it is. Unlike a certificate, nothing identifies it as being a symmetric key. That's why the only way I can see this working is with a highly customized and targeted agent. So color me skeptical about the ability for this to be made into a generic ransomware solution. But thank you, Tom, for a fun little exercise. Leo?

Leo: Yes.

Steve: Completely off topic.

Leo: Yes.

Steve: I wanted to take a moment to comment upon a new and annoying behavior that I've been encountering on more and more websites and to ask whether you might have been seeing it, too. I'm on a site, typically from following a link from a search engine. I look around and don't see what I was looking for. So as I slide my mouse off the page, toward the browser's Back button, or maybe toward the page's tab in order to close it, the browser's JavaScript, which it turns out has been silently, until now, monitoring my mouse's movements, intercepts my attempt to leave, darkens the screen, and pops up a "before you leave" or "are you sure you want to leave" intercept. It's happening, I'm noticing it more and more. It's a little bit jarring, and it's really annoying.

Leo: Totally annoying, yeah.

Steve: So if it keeps up I wouldn't be surprised to see browsers start blocking this behavior, or an add-on created to do so. So you have had that happen to you?

Leo: Oh, yeah, of course. The other one that bugs the heck out of me, when you're sitting on a page, happens all the time, and you're reading something, and the big thing slides down and says "Subscribe to our newsletter" or some such prose. And you have to click it away. And often, this one I really like, they hide the click-away X for a while. So you're looking, and you're looking, and you go, I have to read this. I don't see the close. How do I get out of it? And then it shows up slowly. Very annoying. People, these are dark patterns, and I hate seeing these things happen.

Steve: Well, and yes, it's either when you've been there for a while or you've scrolled down to a certain distance.

Leo: Right. That's right.

Steve: And they go, ah. We've got them hooked.

Leo: Surely you'd want this, yeah.

Steve: Okay. So you and I, I already know because I've heard you talk about it several times now, feel the same way about "Dune."

Leo: Oh, good. Can't wait to talk about this with you.

Steve: A masterpiece.

Leo: Isn't it? Isn't it?

Steve: Yeah.

Leo: Yeah. I'm so glad to hear you say that. I wasn't sure if it was just me.

Steve: Lorrie was as frustrated as Alex and you and I that - and I really wanted to turn on subtitles, and especially because "Dune" happens to have a lot of, like, deliberate whispering. It's not just like, I mean, like whispering is what they're actually doing; right?

Leo: Yeah, yeah.

Steve: And but it's unintelligible. It's like, what? What?

Leo: Huh? Huh? Huh?

Steve: And I just got tired of it. I'd assumed, first of all, I know I'm going to see it again because now we have to wait two years for the second half of this. But boy, for anyone who has not seen it, first of all, know that it's only the first half of the story. It stops, like at a good point, frankly, because they got a lot of that stuff done. We're sort of at a neat stopping point. But it only is the first half. But it is a good two and a half hours of real fun.

Leo: Yeah. Yeah. I mean, it's not all the book. Couldn't be. But the stuff they put in is great. I really enjoyed it, yeah.

Steve: Yeah, yeah. I just think - and I just - I loved as a point of sci-fi how arrogantly casual they are with the manipulation of gravity.

Leo: I know. That's the one advanced technology they have, is the suspensors.

Steve: Yeah, okay. Good point.

Leo: But it was that way in the book, too.

Steve: And good point. Why is it in the year 10191 that you choose swords? Come on, really? We know they have advanced beam technology because, and this doesn't give anything away for me to say that a beam was used at some point, and it's a nasty-ass beam, to cut through a door. So they've got that. But they're not using any...

Leo: And that is a good beam, isn't it. I never thought about that. That thing, hoo.

Steve: Oh, boy, that's a good...

Leo: They should have just shot that right through Gurney Halleck, and it would have been a lot easier.

Steve: Exactly. Why aren't they shooting those at each other? No, we want swords.

Leo: It's better for the movie.

Steve: It's going to, yeah, make for some better battles, I don't know. Anyway.

Leo: I guess. It's pretty funny they didn't think of that.

Steve: I did want to note that I've not seen any more "Foundation." I'm going to make myself watch it just because, you know, sci-fi. But boy, you put them side by side, and there's just no comparison.

Leo: And we did, and it was like watching an old "Star Trek." And I didn't really think that at first with "Foundation." But when you see it done so beautifully, you know, then it really comes home.

Steve: Yeah. "Dune" is a visual masterpiece. And by the way, its director is the same guy who did "Arrival." And I just wanted to make sure...

Leo: Yes, he's very good. I like him.

Steve: Yeah, I wanted to make sure everyone knows about "Arrival." It's Lorrie's favorite science fiction movie of all time. We watched it twice because it's just, you know, it's got an amazing, really unbelievably cool concept as like the best sci-fi does, you know, it's there for a reason. There's a concept which, I mean, and you've got to really think about it, actually. It's not all just given to you on a plate. But when you get it it's like, oh, that is the coolest thing.

Leo: Yeah. I really liked "Arrival," yeah.

Steve: And we are three episodes into "Invasion." You've not seen it, Leo.

Leo: No.

Steve: You were thinking maybe of downloading it and taking it with you.

Leo: Yeah.

Steve: And I would say only if you need to sleep, or you want your trip to seem a lot longer. This also doesn't give anything away.

Leo: That's so disappointing. The trailer was good. It looked like it might be a great - I love that popular subject in sci-fi of aliens arriving.

Steve: Yeah, yeah. And I was thinking, okay, "Foundation," no. "Invasion," maybe, hopefully. No.

Leo: No.

Steve: And what they're trying to do is tell the story from multiple threads of different plotlines of people who are affected by this.

Leo: Right.

Steve: But they're going way too far. I mean, I don't care if her shoes no longer fit because she's growing too quickly. It's like, oh, get on with it already. You know? And, wow, they're not afraid to kill off people. That's good. So that, like, threads get ended. But some of them it's like, I'm really sorry that your lover died, but gee. We don't really care about you now, do we? It's, wow. So, yeah, don't - it's not worth a subscription. Maybe it's going to, like, when is it going to pick up? I don't know. It's painful. I mean, really, episode three was more of episode two. Anyway, I've said enough.

I did want to mention I'm heading toward the fifth pre-release of SpinRite to the GRC spinrite.dev newsgroup. I found and fixed the problem I mentioned last week which only affected Intel chipsets, and then only when they were operating in their legacy IDE/ATA mode rather than in their modern AHCI mode. But there was another related problem hiding behind that first one which I'm currently pursuing. Since the bug is intimately tied to specific hardware which I only have here at my primary workplace, in the evenings when I'm not here I've been at work on the improvement to SpinRite's benchmarking, which will soon boast a new and really cool feature. So all's going well.

Leo: Mr. Gibson.

Steve: Okay. So the inspiration for this week's title began with a tweet I received in the late morning on Sunday, two days ago, from Eric, who tweeted publicly from @ELHonline. Eric wrote: "As a longtime listener of @SGgrc's Security Now! podcast, I was delighted to stumble across this gem from 20 years ago! It's so funny how much technology has advanced, and yet so many problems remain the same."

Now, on the one hand, it's easy to say, "Yeah, there are still security problems." But I hadn't watched that video, which I've also had posted on GRC since the beginning, for many years. Eric's tweet got me to spend five and a half minutes watching it again. And when I did, I was frankly astonished to listen to my conversation with you, Leo, which took place on Monday, April 9th, 2001, and hear just exactly the degree to which we are still right where we were then.

So I want to play this short audio and video into the podcast, to share with our listeners. Then let's spend a bit of time chatting about the degree to which "the more things change." And the first three minutes in particular, but the other two and a half are fun, too.

Leo: All right. Here you go. Let's go back in time. Set the time machine for the year 2001, and a little show we liked to call "The Screen Savers."

["The Screen Savers," April 9th, 2001]

Leo: Oh, hi. Could you - welcome back. Could you develop an anti-hacking device for the FBI? Could you do it in two days? That's what Steve Gibson of Gibson Research Corporation did, and he's here to tell us all about it. Welcome, Steve. It's good to have you back.

Steve: Hey, Leo. Great to be back.

Leo: Man, we were just talking about your columns in InfoWorld, which I read religious - it was InfoWorld; right?

Steve: InfoWorld for eight years, every week.

Leo: Loved them. Read them religiously. And of course you wrote SpinRite, which is still the definitive disk recovery and file recovery program.

Steve: It's what pays the bills for all the other stuff I'm doing.

Leo: You still sell it.

Steve: Yeah.

Leo: Yeah. Well, that's the neat thing. You also give away a lot of stuff. And I think a lot of people know about ShieldsUP!.

Steve: Right.

Leo: Which is firewall testing software.

Steve: Right.

Leo: I know you've got LeakTest, which goes another step further.

Steve: Right.

Leo: And you've done so many great things. Let's talk about PatchWork.

Steve: Right.

Leo: What is PatchWork?

Steve: PatchWork is a tool designed to quickly tell an NT or Windows 2000 ecommerce site user whether they've applied all the patches they need to in order to keep their systems safe against these Russian hackers. About, what, about a month ago, I guess, the FBI released the news that 40 domestic ecommerce sites had been hacked who were using Windows NT or 2000; that credit card information was stolen by these guys operating out of Eastern Europe, in the Ukraine, I guess. And then after getting the data, they extorted the companies, offering them their Internet security services, you know, saying, well, if you use our services, then these credit cards aren't going to escape.

Leo: It's a classic protection racket.

Steve: Oh, exactly. It was pure extortion. So...

Leo: Now, how did you get involved in this?

Steve: Briefly before the news came out I was contacted by the FBI and the SANS Institute because they wanted to have something that would allow people sort of to go along with this announcement...

Leo: Now, how do they know you, though? I mean, how did they say Steve Gibson?

Steve: Just from GRC.com and ShieldsUP! and all that stuff.

Leo: Really, that's great. That's real great.

Steve: You know, the work I've been doing. So I, like in two days, as you said, I very quickly produced a new little piece of free software called PatchWork to - and you just run it. It's like 25K. It's written in assembler, like all my stuff.

Leo: Now, it's for people who are running the Internet Information Server, the web server in Windows NT? Is that right?

Steve: Right. It's only for NT4 or Windows 2000, and really only useful if you're on the 'Net.

Leo: And running a ecommerce site on the 'Net.

Steve: Well, if you have - even a web server. If you've got any data which is in that server, which is on the 'Net, there are four known vulnerabilities. And what was so screwy about this is the Russian hackers were using exploits that have been known for years. Microsoft has patches on their site. And yet...

Leo: Wait a minute. These holes have been known for years. The patches have been out for years. But people are running ecommerce sites and not taking the most rudimentary precautions of downloading the latest versions?

Steve: Well, and that's, you know, it's really their fault. Microsoft in fact, one of these was so bad, Microsoft re-released the patch a year later, like, you know, to remind people that this thing was a problem, a known problem with Windows.

Leo: This is for corporate users. If you're an individual, this might be of more interest to you. This is the latest. This kind of, it's the next generation of ShieldsUP!, I kind of liken it to.

Steve: Well, the way I think of it is ShieldsUP! tests your security from the outside in, to make sure nobody outside can get in. LeakTest checks your security from the inside out to make sure that your firewall is actually protecting you from internal extrusion of your data, to make sure that it's not leaking out.

Leo: So ShieldsUP! says I can't see anything about your system coming from the outside.

Steve: Right.

Leo: LeakTest is making sure that, if a trojan horse or something were sitting on your system, it couldn't actually - I'm going to run this program right now. It couldn't actually - it's not signatured, but I trust you, Steve. Should I?

Steve: Well, yeah, you can. And in fact I specifically signed PatchWork...

Leo: Nothing's happened yet, 20 minutes later.

Steve: ...because I knew it was going to be downloaded from another site, not from mine. So I wanted to sign it to make sure people knew it hadn't been...

Leo: We'd better fix our firewall. Actually we're not running a firewall, and that's why I'm getting that error message.

Steve: It's just that simple to test.

Leo: And one of the things that's great about this is based on this test, a number of firewall companies have changed their capabilities to respond to your...

Steve: The reason I released it is that every single firewall except one had the problem that this thing was checking for. ZoneAlarm was the only one that was not leaking. Norton's, McAfee's, Sygate...

Leo: How many of them are fixed now?

Steve: All of them.

Leo: Oh, keep up the good work.

Steve: Well, I have Version 2 on the way. So...

Leo: The one last thing we're going to see, we're running out of time, Netfilter. Real quickly, what does this do?

Steve: NetFilter is my next-generation solution both for internal and external information theft and spying.

Leo: This is going to run at the network level and watch for all sorts of nefarious privacy invasions.

Steve: Exactly. It doesn't replace a firewall. It's compatible with them.

Leo: When will this be out? How soon will this be out?

Steve: Oh, lord only knows.

Leo: Well, if we sent you home soon, could you get to work?

Steve: A couple months, probably.

Leo: Really. Okay. You do all your stuff, and I have to say this is really great, in assembler. It's tiny, 40, 50K. Even SpinRite, which is a massive program, 40 or 50K. It's a tiny download.

Steve: It used to be a COM. It was a less than 64K COM program in the DOS phase. Now it's a little bit bigger.

Leo: When are you going to move to C and join us in the real world?

Steve: Well, I've got some more things I have to do first.

Leo: All right. Steve, you're the greatest. Thank you for the good work you've done. When NetFilter comes out, we'll tell the world to get it. Meanwhile, go to GRC.com. Use ShieldsUP! and LeakTest. Make sure you're safe online. And I'm sure the FBI gave you a - did they give you a medal? Anything?

Steve: No, I just did it because it was important.

Leo: They just thanked you. That's great. Steve, we appreciate it. Good luck. Always good to meet you.

[Back to 2021]

Leo: That's nice. That's nice. Few years ago. I think it's, by the way, a little sped up. I just want to say I don't think you and I talk that fast or that high. So I think it's a little sped up. But other than that...

Steve: That's interesting because Lorrie commented that my voice had changed.

Leo: Yeah, it hasn't.

Steve: And I was thinking, really?

Leo: It's a couple of frames faster than normal. For some reason a lot of - maybe it's VHS tapes or something. But a lot of the stuff on YouTube of "The Screen Savers" sounds like that.

Steve: Anyway, like Russians penetrating...

Leo: All the same. It's all the same.

Steve: ...through Windows, extorting companies, extracting their information and holding their data at ransom, patches issued years before that have still not been applied, which if they were applied there wouldn't be a problem. I mean, it was just like, wow, 20 years ago, there we were, with hair.

Leo: Yeah.

Steve: You still have yours. But...

Leo: Monitors have also - both monitors and I have gotten thinner. But other than that. You look great. It's funny how things have changed, and yet they stay the same, yeah.

Steve: Yeah. Yeah. Got a kick out of that.

Leo: Is LeakTest - you can still download it.

Steve: Oh, yeah. But it's of - I don't even know...

Leo: Historic interest.

Steve: I don't even know if it's still - if I have an endpoint that receives the data from it.

Leo: Oh, okay.

Steve: Not sure, yeah. And PatchWork was a little quickie that the SANS Institute was distributing. They asked me to do it and if they could distribute it. And I said yeah, sure.

Leo: Nice.

Steve: And then NetFilter never happened because the more I thought about it, it was the encryption that was a problem, TLS. I wouldn't be able - I was going to do packet-level inspection, but it would have been a real pain to get in there and deal with encryption, which was just beginning to happen. And when I was talking about NT and 2000, that was in April. And as we just noted, that year in, like, yesterday, October 25th was when XP was released. So XP didn't exist at that point.

Leo: Wow.

Steve: It was just NT and 2000. And on the consumer side Windows 98.

Leo: We were still in 98 Land.

Steve: Or I guess Millennium; right? I think that was the last.

Leo: Oh, maybe. I forgot about Millennium, yeah. Wow. Wow.

Steve: Anyway, I thought our listeners would get a kick out of just listening to, yes, that could have been said today, and it would still have sounded completely current.

Leo: Yeah. No changes.

Steve: Which is - it's a sort of a sad statement.

Leo: I guess. You still write in assembler code. That's a good thing.

Steve: Still writing in assembler code.

Leo: Still working hard to get new stuff out.

Steve: Still selling SpinRite.

Leo: Yup.

Steve: Still working on SpinRite. That's still the bread and butter.

Leo: Yeah.

Steve: And giving a lot of stuff away for free.

Leo: Those were the days, before Nubeva.

Steve: Nubeva. Well, I wouldn't hold out any hope. Yeah.

Leo: Oh, Steve. I tell you, always a pleasure. I love doing this show. I will not be here next week, as you know. Jason will be filling in. I'm going to be in Mexico. I'll be back in two weeks. But I'm sure the crooks will still be around, and we'll still have plenty to talk about.

Steve: I have a feeling, yeah.

Leo: We do Security Now! every Tuesday around 1:30 Pacific, 4:30 Eastern, 20:30 UTC. It'll be 21:30 UTC after November 7th. So in a couple of weeks we go to standard time.

Steve: Yay, finally.

Leo: Finally. You know, when they shifted it, the candy makers of America petitioned Congress to not change to standard time until after Halloween.

Steve: Oh, my.

Leo: Because they wanted to maximize, I don't know, trick-or-treating time, I guess? They were concerned about economic impact.

Steve: That, children, is the way government functions.

Leo: It's the story of America, my friends. Oh, my goodness. If you want to watch us do it live you can tune in at that time, TWiT.tv/live. There's live audio and video streams there. If you're watching live, you should chat live. There's a great bunch of chatters in two different places. The wide-open chat available to all is irc.twit.tv. You don't even need an IRC client. You can just use the website for that. But it's nice if you have one, if you plan to come back.

Let's see. What else? If you want on-demand versions of the show, Steve's got them. And we have them, but Steve's got some unique versions, 16Kb audio for the bandwidth-impaired, and he also has transcriptions, lovely transcriptions written by Elaine Farris. And of course 64Kb audio. Those are all at his site, GRC. While you're there go check out LeakTest and PatchWork and maybe some stuff more current, including SpinRite 6, the world's finest mass storage maintenance and recovery utility, soon to be 6.1. You can participate in development and get a free copy of 6.1 if you buy 6.0 now. GRC.com. Lots of other free stuff. You can hang out and visit these forums and so forth.

We have 64Kb audio and video at our site, TWiT.tv/sn. There's a dedicated YouTube channel for Security Now!, actually for all of our shows. And of course the easiest way to get this, I would think, is to subscribe in your favorite podcast client. We should be everywhere. And if your client allows for reviews, please do us a favor and leave a five-star review. Let the world know, everybody needs to know about Security Now!. Steve, again, I won't be here next week. Have a great time with Jason. And I will see you in two weeks on Security Now!.

Steve: Will do, buddy. Thanks. Have a great trip.

Leo: I won't bring "Invasion" with me.

Steve: No.