Makes Ya WannaCry

Description: This week we reveal a miracle mistake made by a hacker more than years ago that saved the world from devastating ransomware. But first we catch up on recent ransomware activities, examine the detailed handoff from the GandCrab shutdown and the Sodinokibi startup, a welcome change in Microsoft's Extended Security Update policy for Windows 7, a nasty zero-day RCE in vBulletin, and a bit of nice SQRL news.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-735.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-735-lq.mp3

SHOW TEASE: It's time for Security Now!. Yes, Steve is back. Yay, we're all back. We're going to do a great show. We're going to talk about ransomware. There's a lot of it going around. And an amazing story about the ransomware epidemic that never happened, but could have very easily. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 735, recorded Tuesday, October 8th, 2019: Makes Ya WannaCry.

It's time for Security Now!, the show where we cover your security online with this man right here, Steve Gibson, who in his time at @SGgrc on the Twitter and at GRC.com on the Internet has become the premier guy for security, but also for hard drive recovery with SpinRite and for checking your router with ShieldsUp. And now I know, Steve, that you are in fact a bona fide, legitimate, absolute superstar because, man. I think you know that, too.

Steve Gibson: Well, yeah.

Leo: You did Dublin. You did Gteborg, Sweden.

Steve: Yup.

Leo: And then we were in Boston. I can't speak for the first two, but it sounds like those were massive sellouts. Right?

Steve: Well, and really it's just - I think it's a consequence of 15 years of trying to really do a good job and having something useful to say. And I happened to be in those

neighborhoods thanks to the OWASP groups that wanted me to tell the SQRL story. And so, I mean, again, in every one of those, just as happened with the LogMeIn/LastPass event, we'd say, okay, how many people here listen to Security Now!, and it's like, whoa.

Leo: All the hands. All the hands, yeah.

Steve: Yeah. Like, yeah, yeah.

Leo: It was amazing. Steve and I did a great panel discussion which you can get at TWiT.tv/specials. You can watch Steve, me, Gerry Beuchelt, who's the CISO at LogMeIn, that's LastPass's parent company, and Bill Cheswick. Had you ever met Bill before?

Steve: I had never met Bill. He is a great character.

Leo: You clicked. You guys are on the same - because you're very similar. I mean, he is a legitimate geek, a security guy, a guru, Bell Labs and all that. But he also is an enthusiast like you. So he does beekeeping. He's got a project to make a poster of a movie with every frame on the poster so you could see the color. It's just like he's got all these crazy fun things he does.

Steve: Deeply into IoT stuff and leveraging the technology, yes, leveraging the technology to its limit and, yeah.

Leo: So it was really, really a great panel. I hope you get to watch it. And thank you to everybody who came, about 250 people. They were glad they came. Open bar, lots of food. They got SQRL stickers.

Steve: Yeah.

Leo: And we stood in line for two hours and took selfies with everybody. And it was so much fun to meet you all, so thank you for coming out. We had people - one guy flew out from, weirdly, from Tustin, which is your neck of the woods.

Steve: Yeah. Oklahoma.

Leo: Austin. Seattle.

Steve: Someone from Texas. Yup.

Leo: It was amazing. People from all over the country. Because Steve never goes out of the house, so...

Steve: I don't, no.

Leo: ...it's a rare opportunity to see the man.

Steve: And it's good to be back in my little cave here.

Leo: Are you happy in your man cave?

Steve: I am happy. I'm trying to get readjusted to the time zone. But, yeah. In fact...

Leo: I have bad news for you, Steve. LastPass wants us to do it again next year. Not necessarily in Boston. But, yeah, we want to do more of these. They're so fun.

Steve: Oh. It was fun. I'm up for it, yeah.

Leo: Good, yeah. It was really great.

Steve: And also we do have a great recording from the Gothenburg presentation. One from Dublin is still, I think, is still - last I heard it was still being converted, so a 4K video, and it takes a while.

Leo: Oh, nice.

Steve: And then you and I are going to do like what I'm considering sort of like the reference, the "SQRL story" presentation on Saturday, November 30th, after the U.S.'s Thanksgiving Thursday and Friday, like, long weekend, which I'm really looking forward to. And that'll be like my final, okay, this is it SQRL presentation.

Leo: So this will be the one for everybody who couldn't make the live presentations. This is going to be very geeky. This is going to be, if you're a developer, and you want to implement SQRL, if you really want to understand the nuts and bolts, we are going to have a live studio audience. We're going to shoot it in the big studio over here. So even as big as it is, it even then is limited to, I think - John just said we have 28 chairs. But if you want to come to that, November 30th, right after the radio show, so about 2:30 in the afternoon, we would love to have you. But you must email tickets@twit.tv because I know how many fans you have, Steve. There are going to be a lot more people than we can accommodate. So if you're listening to this, right now, tickets@twit.tv, say "I will be there." And you'd better darn well show up because we want to get [crosstalk].

Steve: And, you know, I guess it's a good thing that Petaluma is a little bit out of the way, too. So it's, you know, you've got to...

Leo: Oh, yeah, should mention that, Northern California, yeah.

Steve: Yeah, you've got to take that goat trail out from Marin north in order to get to Petaluma.

Leo: Oh, boy. But we do have a big parking lot, so all of you will get to park your goat.

Steve: Yay. Well, so, yeah. So the Gothenburg presentation was recorded. Anybody who can't wait, if you go to GRC.com/sqrl, I've added it, because it's up on YouTube, I've added it to that page so it's easy to find. But I want the final official one to be done at TWiT, with TWiT, since it's a consequence of the podcast, Leo, that this whole thing happened in the first place.

And as you said, I call it the "SQRL story." I sort of explain how it happened, what it is, and completely explain it. It's not short. It's about two hours. It just always ends up that it takes me two hours of nonstop hand-waving and pointing at diagrams on the screen to explain what it is. But anybody who watches it comes away saying, oh, holy crap, I understand that. So that's really my goal is to just have something that - because nobody wants to read, even though all the documentation is now up and relevant. It just makes sense to have a video presentation to sort of put the seal on it, and so we're going to do that.

Leo: Well, and that was one thing that was really fun is that Bill Cheswick got it immediately. I mean, he asked one question, said, "Oh, yeah." And...

Steve: Yes. Yeah, they asked...

Leo: Said, "Oh, I get it. Sounds good. Like the idea." And I said, "Break it, Bill. Come up with something." And nobody could come up with anything that broke it because obviously you've spent a long time, years now, thinking about all the ways it could break. And I think everybody agreed. And here's the deal, and I'm going to continue to pressure them. The LastPass CIO was there; Gerry, the CISO was there. They were interested. So I would, boy, that's what you need is LastPass to incorporate that in there and have single sign-on and other things.

Steve: Well, and in fact we already had our tickets to head back here the next morning. And he said to me, he said, "Are you leaving tomorrow?" Like if you're going to be around, let's sit down. But unfortunately I just didn't have any chance. But yeah.

Leo: There'll be opportunities.

Steve: Yeah.

Leo: There'll be opportunities, I'm sure. But that's what you need. And that's what Cheswick suggested is that you work with somebody to make a PAM module.

Steve: Actually since then I found out we have one.

Leo: Thought you did, good.

Steve: So you can use it for logging onto your Linux machines.

Leo: And then the next step is to get the Debian maintainers to make it part of the standard distribution so that everybody has SQRL on their Linux distro. Then, man, why wouldn't a website implement it? I mean, it just would be automatic. And I think that's the key. Well, we've got other stuff to talk about. What are we doing today?

Steve: We do. We're going to reveal a miracle mistake that was made by a hacker more than two years ago that saved the world...

Leo: Oh, dear.

Steve: ...from devastating ransomware attack. This podcast, #735 for October 8th, is titled "Makes Ya WannaCry" because we've often talked about how our friend Marcus Hutchins registered a domain name that he found buried in the original WannaCry very potent ransomware worm, which stopped it. Well, it turns out that within two days a variant had been created that was unstoppable, but a mistake was made which prevented it from wiping us off the face of the Earth. So we're going to talk about that after we catch up with some other recent ransomware activities, examine the detailed handoff, which has now been sort of deeply reverse-engineered by security firms, with that GandCrab shutdown and then the not long afterwards Sodinokibi startup. And now it's really looking like they're all one and the same.

We also have a welcome change in Microsoft's Extended Security Update policy for Windows 7. And I have to confess it sort of launched me into a bit of a rant, but that's the nature of how I feel about Windows 10. We have a nasty zero-day remote code execution in vBulletin, and a little nice bit of SQRL news, and a fun Picture of the Week. So I think we're back in the saddle, Leo. We're both back home. And we're going to do another great podcast for our listeners.

Leo: Yay. I know they can't wait. Loved the Sync thing podcast last week.

Steve: Yeah.

Leo: "The Joy of Sync." And I hope you got to listen to that.

Steve: And we have retired our time machine for the time being. We've got a lot of listeners who - we're back to knowing nothing in advance and hopefully remembering what's happened.

Leo: On we go, Steve.

Steve: I've been holding this Picture of the Week for October because of course it is the Halloween month. And I just got a kick out of this. It's meant to look like a bulletin board maybe in an elementary school. So it says "Halloween." And the question asked to these kids is "What scares you the most?"

Leo: And they're little kids. You know, they're like first-graders, yeah.

Steve: Yeah, exactly. Paul says, "Werewolves." And Nina says, "Sharks." And down at the bottom, Catherine says, "Ghosts." But Dylan, who is a little bit, you know, he's following a different path about what scares him most. He says: "The demise of Moore's law and its ramifications for modern computing innovation."

Leo: Ask Little Leo, he might say, "Quantum computing."

Steve: Ah, that's right.

Leo: We talked about - I was stunned. We talked about this on the panel in Boston. I thought, oh, you know, this is decades off. And everybody on the panel said, not only is it coming, and it will break current crypto, but the good news is everybody's already planned for this.

Steve: Yup, the academics have needed something to do for the last five years, so they've got post-quantum crypto already ready to launch.

Leo: We're good. And I love - the best advice I got, practical advice: Double your key size, you're good.

Steve: Yes, exactly. That was - exactly. And it turns out you were at 4096.

Leo: Yeah.

Steve: And you said, "Should I double that to 8192?" And Bill said, "No, you've already doubled it."

Leo: I did. I doubled it.

Steve: Because 2048 is all - you already doubled it to 4096.

Leo: I doubled it years ago from 2048 to 4096. I thought, you know, just in case.

Steve: Yeah. And Leo...

Leo: It doesn't hurt. It's not like modern machines are slowed down by this.

Steve: Leo, we have long said, many people have said you are already post-quantum.

Leo: I'm post-quantum, baby.

Steve: You are Post-Quantum Leo. That's right. So it seems we are unable to get away from ransomware.

Leo: Uh-oh.

Steve: I know. This is the current scourge of our time. The security firm Armor, and we've talked about some of their analysis in the past, they've been tracking ransomware attacks across the U.S. And last week they published an updated report on the state of the chaos. In total, and this was a number that caught me by surprise, they report more than 500 U.S. schools were hit by ransomware so far in 2019 alone. And just in the previous two weeks, 15 U.S. school districts that are responsible for 100 schools were hit, in just the last 14 days.

They tracked ransomware infections at a total of 54 educational organizations, meaning school districts and colleges, which account for this total, the total disruptions at more than 500 schools. And ransomware attacks appear to have picked up further steam, just as I said, in the last two weeks, with 15 school districts, 100 K-12 schools getting hit, apparently deliberately because they're, like, extra critical at the start of their new school year. And of those 15 most recent incidents, attacking 15 school districts, Armor said that five of them were caused by Ryuk. So there has been some identification of the ransomware behind the problem.

Connecticut, the state of Connecticut, was hit by ransomware infections at seven school districts so far during 2019, giving it the dubious honor of being the state whose educational institutions were compromised more than any other this year. And while Connecticut was visited by the greatest number of ransomware infections targeting school districts, it was the state of Louisiana, and we reported this at the time, that handled the attacks best. Governor John Bel Edwards declared a state of emergency for his state in response to the wave of ransomware infections that hit three of their school districts. And as a consequence, they were able to rally multiple state and private incidence response teams together to help their impacted districts just before the start of the year, and they chose not to pay the ransom demand. It cost them dearly, but they just decided to stick by their guns and not do it.

The Armor report doesn't specify which districts paid the ransom demands and which did not, since that information is not widely available. Sometimes they'll say, "Yes, we did." They're public institutions, so to some degree more than private organizations, as we've been talking about, that has to be made public. But we do know that apparently the bad guys are getting more aggressive. We talked in the last couple weeks about some demands that were so large that the districts were unable to pay them, even if they wanted to. It turns out that Crowder College of Neosho, Missouri, reported receiving the highest single demand of all school districts, with the hackers requesting $1.6 million to provide the district with the means to decrypt their systems.

Leo: That's just an incompetent hacker. You know? You've got to know your market.

Steve: It is. Exactly. It's like, how many movies have we seen where the ransom demand from kidnapping is so over the top that, while Mom and Dad, they want Susie back, it's like we can't raise that amount of money. We just - we don't have it.

Leo: Yeah. That's just dumb.

Steve: So there's some uncertainty since this reporting is inconsistent. A different AV company, Emsisoft, reported that it had identified 62 ransomware incidents impacting U.S. schools in 2019. And they said that those 62 incidents took place at school districts and other educational establishments. And their number was also concomitantly higher. They ended up saying it was 1,051 individual schools, colleges, and universities that they had identified, making it more than double that 500 number that was reported by Armor. So, clearly, it's a huge problem.

In fact, I have here in the notes somewhere that the - oh, yeah, here - that in response to this, last week the U.S. Senate passed a bill called the "DHS Cyber Hunt and Incident Response Teams Act" which aims to create incident response teams for helping private and public entities to defend against cyberattacks including ransomware. That bill had already passed through the House, so our two legislative bodies have both said "Yea," and it's expected to be signed into law by our illustrious President probably within the next couple months, as soon as he frees up some time.

So anyway, this all makes very clear that we are in the middle of a serious ransomware, I mean, you would be tempted to call it a "holocaust" because essentially the bad guys have figured out that there is a soft target that has money that cannot afford to be down for long. And in the reporting that we've done it's been clear that, whether or not you pay the ransom, just bringing these systems back online, even if the ransom is paid and the decryption keys are made available, still costs hundreds of thousands of dollars. So, I mean, it really is a mess.

Well, that's the public sector. In the private sector, we talked about that large aluminum producer Norsk Hydro, whose remediation cost in recovering, because they're so large and sprawling, and I guess the stuff really got deep into their network, their remediation cost was originally estimated at $40 million. That's now expected to actually hit 70, once all is said and done. But it turns out that an even more expensive attack hit Demant, which is the world's largest manufacturer of hearing aids, Leo, Demant. I had never encountered them before.

Leo: Huh. I wonder if they use another brand.

Steve: They may, yes, because they have so many different divisions. They've been hit by ransomware network-wide, and they're expected to incur losses of up to $95 million following an infection that hit them just last week. Their troubles started at the beginning of the month, on September 3rd. I guess, no, wait, at the beginning of last month on September 3rd, when they issued a short statement on their website saying that they were shutting down their entire IT infrastructure following what they initially described as a "critical incident," but didn't provide any additional details.

So what happened to the company's network we'll never know for sure, as Demant never revealed anything except that its "IT infrastructure was hit by cybercrime." However, reports in Danish media soon pegged the incident as a ransomware event, and it did bear all the hallmarks of such an event from the outside. From its own statements, the

company's entire infrastructure was severely impacted. And of course we know nothing can do that quite like a prolific ransomware attack. Their enterprise-wide resource planning system, their production and distribution facilities in Poland, their production and service sites in Mexico, cochlear implants production sites in France...

Leo: Oh, wow.

Steve: ...amplifier production site in Denmark, and its entire Asia-Pacific network were all taken down. So anyway, it's clear just from that enumeration that this is a big operation.

Leo: Yeah. The chatroom has found all the brand names they use. And the biggest is Oticon, which is very, very big. But there's also Bernafon, Sonic, Audika, MAICO, Interacoustics, Amplivox, Grason-Stadler, MedRx, and Sennheiser. So they are...

Steve: Sennheiser.

Leo: Well, Sennheiser Communications. I don't know if...

Steve: Oh, okay.

Leo: Maybe they own Sennheiser, or maybe they just make - I bet you they make hearing aids under the Sennheiser brand, yeah.

Steve: Sennheiser, right, right.

Leo: But Oticon is a big hearing aid brand. So that's probably the main one.

Steve: Wow.

Leo: Yeah. Wow is right.

Steve: So they've been out of action for weeks, and in fact they're still recovering assets today, expecting to take an additional two weeks to recover in full. So anyway, of course, all of those systems are important to their ongoing business. And they said that the biggest losses came from the impact of not having access to those systems in the first place, of course. So they have both employee-required networks and then background infrastructure operations stuff. So they're saying that they're going to cash in - they do have a $14.6 million cyber insurance policy which presumably they once upon a time thought was sufficient to cover the cost of their losses, which unfortunately is now looking like it's going to top $95 million.

Leo: Whew.

Steve: Yeah. So in a press release last week, Demant said: "Approximately half of the estimated lost sales relates to our hearing aid wholesale business." They said: "The incident has prevented us from executing our ambitious growth activities in some of the most important months of the year, particularly in the U.S.," which they said is their biggest market. They said: "A little less than half of the estimated lost sales relates to our retail business, where a significant number of clinics have been unable to service end-users in a regular fashion." So basically it killed, even like all the way out to the clinic service endpoints across the U.S.

They said: "We estimate that our retail business will see the biggest impact in Australia, the U.S., and Canada, followed by the U.K. The vast majority of our clinics," they said, "are now fully operational. However, due to the effect of the incident on our ability to generate new appointments during September," I mean, so even, I mean, these guys are fully automated, and it shut down their appointment system, all the way out of the endpoints. They said: "We expect some lost sales in the next one or two months, which is also included in our current estimate."

They said: "Our remaining business activities - Hearing Implants, Diagnostics, and Personal Communication - have also been impacted by the incident, but with a relatively smaller overall group impact due to the nature and size of those businesses." Demant indicated that it expects the incident to have a long-lasting effect on its bottom line. Previous customers may have been driven to a competitor during the Demant outage, and of course they may never return, having been forced to switch.

So it's certainly useful that they were insured. But as I noted before, the insurance payout didn't even begin to cover the whole cost of restoring all services. So this gives us a snapshot into how truly devastating this kind of deep infection that gets into a private enterprise's network can be. And we don't know, because they're private, whether or not they paid, or whether they recovered from backups. We don't know the inside of this.

However, we do have a story that a three-hospital system in Alabama that was hit did decide to pay its attackers after a ransomware attack knocked its systems offline exactly one week ago, last Tuesday, October 1st. Officials at the DCH Health System in Alabama declined to say how much the hospitals paid for the decryption key. But they noted that they have started a methodical process of system restoration.

A notice posted on their website read: "In collaboration with law enforcement and independent IT security experts, we've begun a methodical process of system restoration. We've been using our own DCH backup files to rebuild certain system components, and we have obtained a decryption key from the attacker to restore access to locked systems. We've successfully completed a test decryption of multiple servers, and we are now executing a sequential plan to decrypt, test, and bring systems online one by one. This will be a deliberate progression that will prioritize primary operating systems and essential functions for emergency care. DCH has thousands of computer devices in its network, so this process will take time.

"We cannot provide a specific timetable at this time, but our teams continue to work around the clock to restore normal hospital operations as we incrementally bring system components back online across our medical centers. This will require a time-intensive process to complete, as we will continue testing and confirming secure operations as we go." Wow.

Leo: Wow. It's as bad as it gets, really. Wow.

Steve: It really is. The system consists of the DCH Regional Medical Center, Northport Medical Center, and Fayette Medical Center. DCH administrators said that, in the wake of the attack, medical staff have shifted operations into manual mode and are using paper copies in place of digital records, and that new patients are being turned away. The process will take a while - this is only a week ago that this happened - with the hospitals having a sequential plan in place to decrypt, test, and bring the network systems back online.

DCH officials said: "Although the attack has impacted DCH's ability to accept new patients, we are still able to provide critical medical services to those who need it. Patients who have non-emergency medical needs are encouraged to seek assistance from other providers while DCH works to restore our systems," they said. The hospitals said they are working with law enforcement, outside IT security and forensics experts to address the incident. For their reporting on this, Threatpost asked DCH how the attack was initiated, but DCH elected not to reply.

BleepingComputer's coverage of this included the additional information that the infecting agent was our new friend Ryuk, that DCH was still not stating how much they paid for the decryptor, but they did confirm that they successfully decrypted multiple servers using the key they received from Ryuk's attackers in return for ransom payment.

Leo: Oh, so they paid the ransom. Wow.

Steve: They paid the ransom. But look at it. Thousands of machines, Leo, thousands. I'm just like, yikes. You know, yeah, you may have the key. But they're all down, and you need to then go in and decrypt it and make sure it's working. I mean, this reminds me a little bit, I don't think, I don't know if we mentioned on the podcast that you guys were having to turn the lights out after midnight tonight.

Leo: No, yeah. Anybody listening live, we may be dark tomorrow, we don't know yet, because of fire danger in the area. PG&E, our local power company, has decided that somehow that will magically help prevent forest fires or wildfires. And so starting at 4:00 a.m. they're going to turn off the power. They haven't told us when it will come back on.

Steve: Yeah. So, I mean, and so, you know, you've got cameras all over the place. You've got servers and racks and lots of stuff. And, like, what's the Skypasaurus or something? You still have the Skype...

Leo: Yeah, yeah.

Steve: Yeah. I mean, so it just, you know, this stuff all has to be turned off and then turned back on. And there is some...

Leo: We're turning off everything tonight when we go home. And we're hoping that, when we come in in the morning, we'll be able to turn it back on. But, you know.

Steve: Yeah. And so, for example, when a server comes up, or a system, it wants to have a DHCP server available to receive its request for an IP. And like all of the stuff kind of has to come back up in the right order, too.

Leo: Yeah.

Steve: So, boy, it just, you know, I think what we see is, in an instance like this, with this hospital system, no doubt they started with one hospital, and then another one. And they linked them together, and that was a major project. And then they linked in a third. And over time, you know, everything is computerized. And it's easy to grow what ends up being a huge system, but you just kind of grow it by accretion over time, you know, the way barnacles form on the hull of a ship. And then, boy, if something comes through and wipes all that out, it's tough to recover.

Leo: Well, that's why the Battlestar Galactica was able to stay afloat, because Commander what's-his-name didn't like the modern networking technology; right? Even the phones were just connected by wires. No wireless.

Steve: Yup.

Leo: Haven't we learned anything since Galactica?

Steve: Apparently not, Leo. And that was actually set a long time ago in the past; wasn't it.

Leo: Was it? I know Star Wars was.

Steve: I think it was.

Leo: Oh, well, then there you go. We should have learned something.

Steve: I think that Galactica may have also been. Anyway, on the same day, also last Tuesday, in Australia, seven major hospitals and several smaller health services from Australia's Gippsland and southwest Victoria regions were forced to either completely shut down some of their systems, or go to manual operation mode following a widespread ransomware infection throughout their IT systems.

The advisory issued from Victoria's Department of Premier and Cabinet said: "The cyber incident, which was uncovered on Monday," so eight days ago, they wrote, "has blocked access to several systems by the infiltration of ransomware, including financial management. Hospitals have isolated and disconnected a number of systems" - I love this - "such as the Internet to quarantine the infection, with the isolation leading to the full shutdown of multiple systems, including but not limited to patient records, booking, and management systems." Which pretty much shuts the hospital down. The advisory added: "Where practical, hospitals are reverting to manual systems to maintain their services." And remember we were talking about the police who were having to fill out tickets by hand.

Leo: Shocking, shocking. Savages.

Steve: So as expected in the case of ransomware attacks, although the Victoria police and the Australian Cyber Security Centre are investigating the incident, they found no evidence that personal patient information has been accessed. Well, if you don't count encryption as an access. So seven major hospitals and smaller health services off, I mean, like shut down, off the 'Net, thanks to another cyber incident.

And in our final piece of ransomware news - actually, let's take our second break, and then we're going to wrap this up with...

Leo: At some point, Steve, you've going to have to stop doing ransomware reports because it's just going to take over the whole podcast; right? I mean...

Steve: It is, exactly.

Leo: I mean, just at some point it's going to be shorthand. Well, they got this guy, this guy, this guy, this guy, this guy, and this guy. Because...

Steve: Exactly. And then there was ransomware, and then we'll move on, exactly, rather than...

Leo: All right. I think honestly, in the long run, this is - I think this is going to be the worst threat of 2020. Forget 2019, which has been a terrible year.

Steve: Yes.

Leo: We're just getting started. And, you know, I predicted back in August, when we were talking about the first ransomware attack on a school, I said, you know, I bet there's going to be a rash of them because all these school systems have been off all summer. They're going to turn them on, they're going to, oh, look, I got some email. They're going to click the link. And I was right, boom.

Steve: Yeah. And lots of them are insured, so they do have deep pockets.

Leo: They're good, yeah.

Steve: And, yeah, and they represent soft targets. As you said, somebody comes back from a long summer off and goes, oh, look, a prince in Nairobi really needs some help with his cash management.

Leo: Has some money for me.

Steve: That's right.

Leo: You know, I just knock on wood, we haven't been bit here at TWiT. We've got really good IT people.

Steve: And Leo, I'll just say it is the thing that I worry about more than anything else. And so my backups have backups and backups because it is potentially such a problem.

Leo: We do use G Suite. All our corporate mail is through Gmail. And Gmail, I think Google does - there's one compelling reason to use Gmail. They do a very good job of filtering out malware. And so those malware payloads often just don't get through.

Steve: Oh, Leo, in fact, sometimes I try to use my Gmail account to send something to someone. You can't send anything through there.

Leo: No.

Steve: It doesn't matter, I make the mistake of, like, sending an EXE [buzzer sound]. I zip it up [buzzer sound].

Leo: Good, good, good.

Steve: I mean, you just - you can't...

Leo: Stop it, Steve. You should know better. That's what Dropbox is for. Or, wait a minute, you're using Sync.com.

Steve: And, yeah, I know, I have lots of alternatives, yeah.

Leo: You've got a way to share, yeah, yeah. Yeah, I'm not going to say what else we use, but we have a fairly - I think we have, as with any good security system, layers upon layers of defense. And I don't want to talk about it because I don't want to give anybody any ideas. But knock on wood.

Steve: And as we know, ultimately, backups. Have offline backups is what you need.

Leo: Yup, yup, cold backups.

Steve: And it's not a nice day when you have to restore from backups.

Leo: No.

Steve: But it's sure better than, like, losing anything. Or everything.

Leo: To the ransomware report.

Steve: Of course I can't promise we're never going to talk about ransomware again. I keep trying to promise that, but it just...

Leo: Well, no, it's important. You could see these businesses could fail. I mean, this is huge.

Steve: Yes. In fact, there was an item that I didn't cover where a business did fail. They were hit, and it was going to take them more time and effort to recover than it was worth, and they just shut the doors. They just - they're gone.

Leo: By the way, I love this Ransomware as a Service model. Oh, my god.

Steve: I know.

Leo: Don't skip this story. This is too good. Well, it's up to you.

Steve: No, we have to, yeah.

Leo: Yeah, we've got to do that.

Steve: No, no, no. Yeah, yeah, yeah. So that's the new acronym, RaaS, Ransomware as a Service.

Leo: Oh, my god. Oh, my god.

Steve: So BleepingComputer is reporting that our new friend Sodinokibi, which is also known as REvil, R-E-V-I-L, has successfully assembled what they're describing as an "all star group of affiliate attackers." Sodinokibi ransomware, as we know, we've talked about a couple times as they're making news lately as they target the enterprise, managed service providers, and government entities. Remember it was managed service providers that were the key to gluing together all of those small organizations, the small schools, I don't remember what state it was in now, but a whole bunch of them were hit. It's because they all used a common managed service provider. The bad stuff got in there and then caused trouble.

So anyway, and also, of course, they're attacking government entities using a handpicked team of what they're describing as "all-star affiliates." What's interesting is these affiliates appear to have had a prior history with the GandCrab Ransomware as a Service model which used similar distribution methods. Sodinokibi was first discovered in April exploiting vulnerable WebLogic servers. And it has seen wide success worldwide

through exploit kits; phishing campaigns; remote desktop attacks; and, as we mentioned, large-scale attacks through hacking managed service providers.

In two new reports from McAfee, the Sodinokibi ransomware has been analyzed to provide information about code similarities between this ransomware and its sort of predecessor, GandCrab. The affiliates of both of these RaaS operations have also been analyzed to reveal similarities between the two and how many affiliates probably switched to Sodinokibi as GandCrab began shutting down. Remember we talked about this earlier this year, that GandCrab announced a month ahead of time their plans to roll up the sidewalks. They said: "We've made all the money we need to. We've reinvested our ill-gotten gains in legitimate enterprises and in cryptocurrency and online and offline things, and we've decided we're done." And so they preannounced their shutdown a month ahead of time.

And this was also done to get their affiliates, who were in the process of infecting other people, to make sure the ransomware payments were paid because after a month they were going to shut down their whole payment, the ransomware payment processing infrastructure. So that all happened. And we posed the question at the time, what will fill this vacuum which was created by GandCrab's shutdown? Well, we have the answer now, and it is Sodinokibi.

Okay. So we know how GandCrab was operating. We know that they created an affiliate structure. And to their credit, they gave the affiliates the lion's share of the proceeds. That is, they only took between - the GandCrab operators took between 30 and 40%, which covered their ransomware management, the creation of the ransomware, and they maintained the payment system. So we have a chart of this, a sort of a flowchart diagram that shows how the affiliates would have outbound infections to the victims. But the way the system works, the victims pay the ransomware developers directly, who then provide the decryption keys to the affiliates to then provide to the victims, and then they take a piece of the action.

Leo: Sure.

Steve: Yeah, and then provide 60 to 70% of the proceeds back to the affiliates in order to provide the incentive.

Leo: Money ruins everything. We had this nice little ransomware cottage industry, and now big business is moving in, and their affiliate scheme. Geez.

Steve: That's right. That's right. So what's interesting is that McAfee analyzed everything that was known of GandCrab and looked at the distribution of proceeds from GandCrab. There was one particular affiliate, ID 99, that was at the top of the heap. There were a total of 292 affiliates that were registered with the original GandCrab, although many of those were not highly active. And you have onscreen right now, and I have in the...

Leo: I can't even fit it on the screen.

Steve: I know. It's amazing. So there was an ID and a SubID. And apparently affiliates were - they were assigned an ID from the GandCrab operators, and then the affiliates were able to assign their own SubID for their own internal tracking purposes. And so this chart shows all the SubIDs and which infections were found in the wild of ransomware

flowing from the SubID, all of which were aggregated under the single affiliate's primary ID. So, I mean, it's a big deal.

Leo: Multilevel marketing comes to ransomware.

Steve: Yes.

Leo: You need your down line, man, to really produce here, if you're going to make money on ransomware.

Steve: That's right.

Leo: Geez. Aw, geez.

Steve: Yeah. And these guys, if we believe the report, they made - the GandCrab operators made many, many millions of dollars, funneled back to them through the work of their affiliates.

Leo: Because they made it easy for any script kiddie to do it.

Steve: Exactly. Exactly. So that was GandCrab. That's shut down. So now onto Sodinokibi, the inheritor of that. And here's what's interesting. A month before Sodinokibi became active, McAfee noted that the highest profile affiliates suddenly went missing from GandCrab's final version 5.2 build. And then, shortly afterward, as we know and discussed at the time, a completely new and at the time unnamed RaaS, Ransomware as a Service, started being marketed on online hacker forums such as Exploit.in, where a member named UNKN, you know, unknown, UNKN, was now recruiting affiliates. So what we believe is a selective pre-recruitment process, which only accepted a limited number of highly vetted applicants, had been initiated.

And in fact the cream of GandCrab's crop was offered to move over to the next-generation ransomware. One of the people who replied to the topic in the forum and vouched for the Ransomware as a Service, was a member named Lalartu, who stated that they were previously a GandCrab affiliate. And very soon afterward Sodinokibi exploded with ransomware distribution that was hauntingly similar to the high-profile attacks that had been seen previously with GandCrab. The evidence collected by McAfee strongly suggests that the GandCrab operators privately informed their top affiliates that they would soon be shutting down and either transferred them to Sodinokibi or that the affiliates decided to move to the new RaaS on their own. And really, with GandCrab shutting down, I mean, these guys are making a lot of money. It's more widely distributed than the malware operator, but they're making money.

So check this out. This is when analyzing the Sodinokibi sample code, McAfee found that Sodinokibi used affiliate IDs and SubIDs in exactly the same way as GandCrab, so the same design. But the clincher came when the infection code of the two was broken down and placed side by side. And I have in the show notes a graphic of Sodinokibi on the left, GandCrab on the right, just showing the block level architecture that was automatically, through automation, created.

Leo: Pretty similar.

Steve: Well, is there any doubt in anyone's mind that this is the same architecture? Yes. It's quickly clear that the two code bases were in many places virtually identical. Also, when Sodinokibi connects back to the ransomware's command-and-control server, it does so through a randomized runtime-generated URL. And as previously found by other researchers, McAfee confirmed that the URLs generated between the two ransomware families are nearly identical. So, I mean, it must be that Sodinokibi is the new GandCrab. That is, for whatever reason, maybe it was just time to clean house. They had acquired those 292 affiliates, and a bunch of them were just sort of deadwood. So it's like, okay, we're going to start over.

Despite the preponderance of evidence that suggests it is the same, of course we can't be 100% certain. It is the case that a great deal of malicious code is routinely reused, begged, borrowed, or stolen among the criminal underground. And who knows. Maybe the operators of GandCrab really did shut down and give or maybe privately sell their code to another group who said, hey, wait a minute, we want to continue this. This thing's working for you guys. So let us do it.

So on the "yes, this is the same group" side, we have the strong similarities and the affiliates who were previously part of GandCrab and are using the same distribution tactics with Sodinokibi. But on the "maybe not" side is the observation that the Sodinokibi operators' approach seems to be significantly different now as opposed to previously. With GandCrab, the operators were open and public with their communications. They joked with and poked the research community and generally had a good time running their operation. By comparison, the Sodinokibi operators have been so far much more quiet, secretive, and almost reclusive in how their Ransomware as a Service operates. So it's left people in the security industry sort of puzzled.

BleepingComputer concluded: "While personalities can change, the stark contrast between the two makes BleepingComputer believe that Sodinokibi is being operated by the programmers of GandCrab, while the original operators have since retired or moved on to new things. This would explain the code similarities, yet the different and more secretive nature of the Sodinokibi RaaS as opposed to GandCrab." And so I summed this up in the show notes by just saying, "Huh, what a world." Unbelievable.

Leo: Yeah. Well, where there's money to be made, that's when the entrepreneurs jump in.

Steve: Yeah.

Leo: Lots of innovation and creativity.

Steve: And as we covered in the first 40 minutes of this podcast, there is unfortunately money to be made by causing a great deal of pain to organizations and saying, hey, give us some money, and we'll minimize your subsequent pain.

So in happier news, Microsoft has announced that they will accept more money from more people in return for offering to make their Windows 7 Extended Security Updates, which they have to produce anyway, also available to small and medium-size businesses, thus broadening its availability beyond its previous exclusive access only to their enterprise volume licensing customers. I've heard you talking with Mary Jo about this,

Leo. And the idea is that the so-called ESUs, the Extended Security Updates, would start being available at the beginning of next year, when Windows 7 updates famously end on, what is it, January 14th is the last one. So starting February there will be no update, no security updates for Windows 7.

Microsoft I guess looked at the distribution of Windows 7 in the enterprise. We covered this a couple weeks ago, noting that the only reason that 7 and 10 finally swapped their places as number one and two, which occurred at the beginning of this year, was the combination of end user capitulation and new system purchases; but that in fact enterprise was overwhelmingly still using Windows 7 and Windows Server 2008 R2, which is the server equivalent of Windows 7. So anyway, I'm using Windows 10 on many of my machines.

Leo: Oh.

Steve: It was - oh, yeah. It was the OS on the laptop that I traveled with to Ireland and Sweden. So, you know, all of my loud protestations notwithstanding, I've made a tentative peace with Windows 10. But I do have access to the Long-Term Servicing Channel, that LTSC edition, which blessedly allows me to avoid ever having to see Candy Crush Soda Saga - oh, my lord - and similar Windows 10 consumer atrocities ever appear on the Start Menu.

But for the most part, enterprises - think about this. Enterprises small, medium, and large, they have not budged. And really, why would they? They have an installed fleet of perfectly working Windows 7 machines causing no one any trouble at all. Everything is fine. Work is getting done. But in every quarterly and annual report since mid-2015, Microsoft has reminded its shareholders and customers that its business plan for Windows 10 includes "new post-license monetization opportunities beyond initial license revenues." Hmm.

Leo: What's that mean? What is that?

Steve: Uh-huh. Windows as a Service. And forgive me, but I have to rant about this because yes, indeed. What comes along for the ride in Windows 10? Every time I see this I just - I can't believe it. Candy Crush Soda Saga. Bubble Witch 3 Saga. I'll never know what happened to Bubble Witches 1 and 2, and I don't care. We have March of Empires and Disney's Magic Kingdoms. This is in Windows 10 Professional.

Leo: Some of those, not all of them, are installed. Some of them are stubs that if you click them it'll bring you to the store and install it. I agree, it's dopey.

Steve: There's, like, little download arrows in the beginning?

Leo: Yeah, that's what it is. But some of them are installed, which is really annoying. When I first installed...

Steve: Also Bing, yeah, Bing Weather.

Leo: Well, you might want that.

Steve: Microsoft Solitaire Collection. The Mixed Reality Portal, as if this reality wasn't mixed already enough. Microsoft People, whoever they are.

Leo: You might want that.

Steve: Skype. The Store Purchase App. Well, yeah, but why not download it if you want it or if you need it, rather than it just being...

Leo: I run a script. When I first run Windows, I run a PowerShell script that deletes everything from the apps store except the apps store. And then you have the choice of doing that. The other thing I do is I delete all the tiles. That's a little more manual process. But then you have a traditional Start Menu without any of those silly tabs.

Steve: Yes. There's even Zune crap in there, Leo.

Leo: Yeah, I know.

Steve: Like two Zune things. Let's keep that success alive. Anyway, I can't - so Microsoft is imagining that enterprises - small, medium, or large - would want to jump on this? Oh, my god. So anyway, Microsoft is now saying that they will allow all of those businesses, which long ago already purchased and paid for their Windows 7 licenses, to continue using them, rather than submit to what Microsoft has deliberately created in Windows 10, if those businesses will effectively repurchase Windows 7 licenses every year moving forward. And remember that what we're really purchasing is the privilege of continuing to receive monthly patches for all of the myriad bugs and mistakes which Microsoft already made in the past, and continues to make with every update to their software. I mean, if this isn't the definition of a racket, I've never seen one.

Leo: By the way, every year the amount you have to pay to continue to use Windows 7 doubles.

Steve: Goes up.

Leo: Now, anybody who's studied exponentiation will know that it rapidly becomes untenable. They don't want you to do this for very long. It's just awful.

Steve: So I do imagine - yes, you're right, Leo. And this is where you remind us about Linux. I do imagine that this will be a nice new revenue source for Microsoft. If given a choice, businesses won't move to Windows 10 ever.

Leo: Right.

Steve: They certainly, you know, they certainly are not doing so now. Eventually, hardware will die, yes. And those replacement PCs will come with Windows 10, decked out with all of its myriad "post-license revenue" sources preinstalled. So, you know, I am truly sympathetic to Microsoft's need to stop servicing their older operating systems. I am. But the only option they have given us is to move to a replacement OS that no one wants because of what they have done in this effort to create an ongoing revenue stream for themselves. And to my mind, that's not okay.

Jared Spataro, corporate vice president for Microsoft 365, said: "Today we are announcing that, through January 2023, we will extend the availability of paid Windows 7 Extended Security Updates to businesses of all sizes. Starting on December 1st, 2019, businesses of any size can purchase ESU through the Cloud Solution Provider program. This means that customers can work with their partners to get the security they need" - for a price - "while they make their way to Windows 10." Right.

Leo: Linux. Linux. Linux.

Steve: Linux. Linux, yes.

Leo: I love Linux. In fact, I don't buy a PC anymore unless I first check to make sure that, should I decide to at some point, I can take off Windows 10 and put Linux on it. And most modern PCs it's not a problem. It's just not a problem. I mean, now Dell comes with - you can get them with Ubuntu. But if you want to try Windows 10 for a while and then put Ubuntu on there, no problem because, I mean, they have all the drivers.

Steve: Yeah.

Leo: Linux is really good these days. It's very good.

Steve: Yes. I had an opportunity toward the end of working with SQRL, actually all the way through, I needed to make sure that it would work under Linux with WINE. And so I put Ubuntu, the LTSC, the long-term servicing channel, I think it was - maybe I'm confusing my acronyms.

Leo: There is, you're right, LTS. No C.

Steve: LTS. LTS.

Leo: Yeah.

Steve: Right, 14 point something or other, I think it was.

Leo: No, that's old. No, must have been 1902 is the last one.

Steve: Oh, yeah, yeah, you're right, you're right. And it just came up and recognized all my hardware, and it ran.

Leo: 19.04.

Steve: And it was like, oh, okay.

Leo: That's the thing. I think people from the old days, god, I remember doing Slackware, and you'd have to then run XFree86 and figure out how to configure your video card and...

Steve: X11 stuff and all that.

Leo: Oh, it was a nightmare. Now, truthfully, the PopOS, which is the Ubuntu Spin I use from System76, is a much faster, simpler installer than the Windows installer. You answer, like, four questions, press "go," five minutes later you have a fully installed, running system that works. It's easy now. I mean, I just - I'm sitting in front of PopOS on a Lenovo laptop right now. I love it. And nowadays, because so much is in the cloud, if you're using Firefox, it's the same.

Steve: Yes. Same Firefox. You're able to get email, you know, Thunderbird email, for example. You're browsing the web for most of the things, I mean, this is what you've been telling people for a long time about Chrome is, you know, for your typical purchase, that's all you need. The era of this super heavyweight massive lumbering OS, it's, you know. Maybe this mess with Windows 10 represents the death throes because they're just trying to hold on to what they've got left. I don't know.

Leo: Neal Stephenson wrote a wonderful book, "In the Beginning There Was the Command Line." He wrote it in the late '90s, but it still holds true. Someday I'm going to bring this in and read the section about operating systems. Because essentially the thrust of it is there really are only two. There's the UNIX-based operating systems like Linux, macOS, BSD. Those are all based on UNIX.

Steve: Yeah.

Leo: And then there's Windows. And there's no reason to use Windows. Because operating systems aren't that complex. The problems have been solved for decades. There's only a commercial reason to keep doing new versions of Windows.

Steve: Well, I would say they are complex, but they've been growing for decades. And this is our argument about the idea of China deciding they're going to create their own Chinese OS from scratch. It's like, you can't. It's just not possible.

Leo: No, don't do it. Because you don't need to.

Steve: Exactly.

Leo: You don't need to.

Steve: No one needs to.

Leo: Don't reinvent the wheel. They invented it.

Steve: If you don't - exactly. And China, if you're listening... Oh, wait. Russia, if you're listening... No. China...

Leo: They're all listening. Well, actually China did have a Red Linux for a long time that they used that was a...

Steve: Yes, and that would be the thing to do. Take, I mean, yes, do vet it. But don't try to recreate it from scratch. It just, I mean, you'll go back to the abacus if you try to do that. Doesn't make any sense.

So we do have a nasty new - and this is sad, Leo, I know you're going to empathize with this - a nasty new zero-day remote code execution vulnerability in vBulletin. vBulletin is a very widespread web-based forum discussion, you know, bulletin board. Two weeks ago, back on Monday, September 23rd, a zero-day exploit written in just 18 lines of Python, basically a proof-of-concept demo, gives any remote attacker unrestricted shell access to any system running the very popular vBulletin forum software. It was anonymously published to the full disclosure list, after which attackers wasted no time jumping on and using it to install bots, cryptocurrency miners, and whatever they wished. I have the link here at the very bottom of page 9 of the show notes, the SecLists.org, where it just shows you just this simple little short bit of Python which anyone could easily translate into any other language if they didn't want to use Python.

Tenable Research wrote, they said: "Tenable Research has analyzed and confirmed that this exploit works on default configurations of vBulletin. Based on the public proof of concept, an unauthenticated attacker can send a specially crafted HTTP POST request to any vulnerable vBulletin host" - and, by the way, that's all of them, from v5 that's very old to the state-of-the-art latest one - "and execute commands."

Leo: You shouldn't be able to POST a shell command to a website. That's ridic- talk about sanitizing your inputs.

Steve: Yes, yes.

Leo: The reason this is such a simple thing is all he's doing is using the POST to put echo shell_exec command.

Steve: Yup. Yup. Tenable says: "These commands would be executed with the permissions of the user account that the vBulletin service is utilizing. Depending on the service user's permissions, this could allow complete control of a host."

Defcon's site uses vBulletin; and Defcon's founder, Jeff Moss, told Ars his team took their site down immediately to avoid getting hacked. He said: "We tested it right away, and none of our defenses would have saved us. We checked the logs and saw no attempts to attack us; but after we patched and went back online, there were two attempts in the first 30 minutes. Definitely active attackers," he wrote. And here's what struck me as a bit sad, Leo. We've talked about the questionable ethics of the "We'll buy your bugs at premium prices" company, Zerodium. In what struck me as a somewhat tacky and tasteless tweet, Zerodium CEO and founder Chaouki Bekrar, stated that the vulnerability has been privately circulated for years.

Leo: Oh, yeah. I'm sure, yeah.

Steve: I have the tweet in the show notes. He said: "The recent vBulletin pre-auth RCE zero-day disclosed by a researcher on full disclosure looks like a bug door, a perfect candidate for PwnieAwards in 2020. Easy to spot and exploit. Many researchers" - this is his tweet. "Many researchers were selling this exploit for years. Zerodium customers were aware of it since three years." In other words, for the past three years, any Zerodium customer who wished to could quietly execute any command they wished on the server of anyone running vBulletin, while in the meantime knowingly leaving every vBulletin system in the world wide open and exposed.

I mean, I suppose that's the on-the-ground reality of any service such as Zerodium. But it does somehow feel wrong, the idea that this has been sitting there listed in a catalog that Zerodium customers purchase, which would allow anyone - nation states, large corporations wanting to do their own backdooring, I mean, vBulletin is widely used. And the idea that this thing was sitting there for three years, I mean, again, it's one thing for the problem to exist and not be known. Here it's listed in a catalog of exploits that you get when you subscribe to Zerodium.

Leo: It's probably been there forever. I mean, it's not like all of a sudden you stop sanitizing inputs. It's probably been there since day one.

Steve: Right, right.

Leo: But honestly, vBulletin and phpBB are the most popular PHP-based bulletin board softwares. Just do a google. Exploit after exploit after exploit.

Steve: I know. I know. Well, and it's why even though I'm not using them for SQRL's forums...

Leo: You use XenForo; right?

Steve: Yes, I use XenForo. And I established it on its own physical hardware box with a separate physical firewall between it and all the rest of GRC because I didn't write the code, and I can't vouch for it. And it's PHP, baby. So, I mean, and again, good as the XenForo guys are, you know, it's their second or third iteration of a system from scratch, it's just - I just can't afford letting anything get loose and get into the rest of GRC. So it's physically isolated.

Leo: We run - our forums, our new forums at twit.community are Discourse, which is a Ruby-based system, much more modern. But you're right. We don't run it on our servers. We run it on their servers. So if there's a problem, it's not our problem, you know.

Steve: Right. Well, and that's very much the reason why, even though I could run ownCloud or My Cloud, I chose Sync because it's their servers that are doing the synchronization, and my files are encrypted before they leave and after they return. And so I'm happy to have the cloud knitting things together. But I'd just rather not have that open exposure because, again I didn't write it myself. So I just can't vouch for it.

Leo: Yeah.

Steve: I got a nice note. This was posted in the SQRL forums by Daniel Persson, who's the guy that wrote the Android client for SQRL, the WordPress plugin, and the PAM module for Linux. He translated from - I guess maybe it was posted in Swedish. Somebody said: "Ha. Added SQRL to my WordPress today." And then he said: "@kalaspuffar's" - that's Daniel's Twitter handle - "plugin enabled this in under five minutes." The guy said: "In and reconnect to my admin account and remove email address. Totally strange that this isn't standard for login everywhere." And then a smiley face. And then Daniel...

Leo: Nice. Can I make a request? Oh, go ahead.

Steve: ...said: "This made my day." Yeah.

Leo: Anybody who has - because I would love to add SQRL to our TWiT forums, but it requires somebody who has a working knowledge of Discourse, our software, and SQRL. And so if there's anybody listening who could do that, I'm sure there are a lot of Discourse users. Discourse is very widely used by companies for community forums, including Imager uses it. Oh, I just saw another company that we were talking about uses it. It's very popular. It would be, you know, it'd be another great way to get the word out.

Steve: Good. I will definitely put the word out in the forums and in the newsgroups, Leo. Discourse.

Leo: Ask around. Discourse, Ruby. Discourse, written in Ruby.

Steve: And I'm sure that there is a plugin authentication option for it where...

Leo: You know, it might support PAM. I don't know. I'll have to look into that. If it did that, it'd be pretty easy, huh. Yeah, there's an API. I'm sure there's all sorts of authentication choices. So, yeah.

Steve: Hooks, hooks. Cool.

Leo: It supports OAuth. It supports a lot of the more traditional authentications.

Steve: The standard, yup.

Leo: Yeah, yeah.

Steve: Cool. So more than two years ago, after the event which briefly rocked the world, and which Marcus Hutchins inadvertently but fortuitously stalled this groundbreaking worm, or earthshaking worm, Sophos recently took a look at the state of the WannaCry worm today. We'd like to say that it's gone, but not forgotten; but we can't because it turns out it's not gone. Okay. So what happened? As we know, on May 12th of 2017, organizations across the world were attacked by what was then a new and unknown, very rapidly spreading piece of malware which we now know as WannaCry. It's now considered one of the most widespread and notoriously destructive malware attacks in history, which was halted only when, out of research curiosity, Marcus registered a domain name that he found embedded in the malware, which unexpectedly and happily acted as its kill switch.

But the kill switch didn't completely kill it. And today, more than two years later, WannaCry continues to adversely affect thousands of computers worldwide, although it doesn't get any press attention, and we'll explain why. In fact, it's joined the legions of worms, we know their names - Code Red, Nimda, MSBlast - which continue to contribute to constant Internet packet noise for which I long ago coined the term "Internet background radiation." It's just like, if you put a system on the 'Net, packets start coming in that you didn't ask for. It's just background radiation. It's these things that will never die, that are still running on servers in obscure places. And then the machines haven't rebooted, or the worms are written to permanent storage, and they arrange to restart after reboot, whatever.

But on that fateful day in May 2017, WannaCry stormed across the world. It was, as we know, made extremely prolific by its use of the EternalBlue vulnerability and exploit which was believed to have been stolen from the U.S. NSA, the National Security Agency, by a group of hackers calling themselves the Shadow Brokers. And WannaCry provided another vivid example of the other thing we're often talking about, the so-called "patch gap," which continues to exist today since the Windows flaw, which was exploited by EternalBlue, had already been found, fixed, and patched in March of 2017's Patch Tuesday, a little more than two months before WannaCry's trans-Internet rampage.

If everyone had patched their Windows machines within those following two months, WannaCry would have never gotten a start. Nothing would have happened. It would have knocked, but not been able to get in. It couldn't have propagated laterally across enterprises. It would have just been game over. But as it was, a great many Windows systems were behind on their patching. And believe it or not, they're still not patched today.

So WannaCry entered into a target-rich environment and infected something like, it's estimated, 200,000 victim machines in the blink of an eye. And as I said, not everyone is patched even now, more than two years later. And WannaCry is not only still alive and, for reasons I'll explain in a minute, now ignoring the kill switch that was designed to stop it, but possibly more alive than ever.

Okay. So what's with the original kill switch? Why was it there? Unless the creators of WannaCry themselves explain their motivation, we'll never know for sure. But there are

two prominent hypotheses. Either the attackers wanted to have for some reason a way to stop the attack at their discretion, or the more likely hypothesis is it was a deliberate anti-sandbox evasion technique. Some sandbox environments fake responses from connections to URLs to make the malware that they're examining think that it is still connected and able to access the Internet, when in fact it's being deliberately prevented from doing so, so that it can't do any harm.

Since the domain name was deliberately unregistered, the attackers knew that if a DNS lookup were to succeed, it could only have been because the malware was under analysis in a sandbox designed to make it think that it's on the Internet, thus positively responding to any DNS query. So then the malware would end the attack to hide its true nature. If this was the motivation for the kill switch, this meant that Marcus's actions effectively turned the entire world into a sandbox and shut down the worm's spread globally.

And it's been a long time since we've talked about this, two years. But the domain name looked like the bad guys just pounded on the keyboard. I mean, there's, like - in fact, it literally looks like that. I see ja's occurring, jae, jap. So there's like some recurring letters. It's, you know, iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com is the domain name. So, yeah, bang on the keyboard for a while. We don't have to worry about that being an actual site. Marcus saw that in the code, registered that crazy domain name, shut the worm down. And as we know, if that was not done, WannaCry's payload would execute.

It did execute in 200,000 machines and would encrypt the files of the victim, then post the infamous extortion screen, which we showed at the time. I have it here reproduced in the show notes. And I always got a kick out of it. The headline, it starts off with, "Ooops," as if this was a mistake. "Ooops, your files have been encrypted." Yeah, ooops. And then it's got, remember, the countdown meter over on the left showing that the payment cost will be raised in, and your files will be permanently lost within a week if you don't pay, and they're not even going to bother to keep the encryption key.

And what they were asking for at the time, it's kind of quaint now in today's numbers, was please send us $300 worth of bitcoin to the following address. And there were four addresses in the code that would surface randomly that it would choose from. Anyway, so back then the ransom was $300 to recover your files, presumably on a personal machine. Of course now we know that 1.6 million was recently asked for the decryption of a sizable network. So there are a couple of interesting notes.

Leo: Oh, PG&E is really going crazy now. They're sending out a warning.

Steve: Oh, no kidding?

Leo: Yeah, we're getting an emergency alert. "Caution. Long-term..."

Steve: On your phone?

Leo: Yeah, getting one of those presidential alerts, you know. "Caution. Long-term power outage plus high fire danger."

Steve: Wow.

Leo: Like, come on, dudes. Personally, I think they're blackmailing the California state legislature. What they want to do - I know what's going on. They're being sued for billions of dollars for the last 2017 fires. And I know what they really want is the California state legislature to say, oh, you can't sue PG&E anymore. And then the power will magically come back on. You watch.

Steve: Wow. So it's like, okay, if you're going to hold us responsible, we're going to turn...

Leo: If you're going to sue us, well, we're just going to have to turn off the power. They've never done it before.

Steve: Wow.

Leo: It's a show of strength.

Steve: Well, when the lights go off, people are going to want their lights back on.

Leo: Oh, yeah.

Steve: You know, your electric toothbrush runs for actually quite a while without power.

Leo: Yeah, I'm worried about brushing my teeth.

Steve: Yeah. But, boy...

Leo: Sorry to interrupt. But the state of California just did, or somebody.

Steve: Yeah. You often go into a room and flip the switch, and it's like, wait a minute. Oh, that's right. It's amazing how handy power is.

Leo: Oh, it's amazing when the power...

Steve: Especially for geeks like we.

Leo: What am I going to do? I'm going to have to go out and take a walk.

Steve: Charge up all your batteries, yeah.

Leo: But I don't think I'll have Internet, either.

Steve: Oh, that's true.

Leo: Actually, sadly, our house is - not sadly, happily. Our house is not in the map that TWiT is. The old studio's not. We're just right on the edge of the map. So I don't know what's going to happen.

Steve: Interesting.

Leo: Yeah. I'm sorry to interrupt. Go right ahead.

Steve: Yeah, no problem. That is definitely newsy. There are a couple of interesting notes about how WannaCry was portrayed at the time of its initial outbreak. For example, and our listeners will remember, despite the suggestions that it was unpatched Windows XP computers primarily responsible for WannaCry's rapid spread, this mistake was due to the fact that some of the more high-profile attacks were XP-based. More than 97% of WannaCry detections at the time were actually coming from the newer Windows 7 operating system.

It's also worth noting that, while a computer patched against the EternalBlue exploit is no longer vulnerable to being infected by a remote connection from another WannaCry infected computer, in other words, that was the way things were getting in was over the SMB file and printer sharing connection and port. If that computer, the patched computer was infected before it was patched, it will still be trying to infect other computers. The anti-EternalBlue patch only prevents the vulnerability from being exploited, not from exploiting others. And if nobody had since updated WannaCry, that is, if it was the original WannaCry, that file that started spreading on May 12th of 2017 would be the same as the file seen in the wild today.

But it turns out the reality is very different and much more intriguing. There's a new WannaCry. Sophos's research is based on a signature named CXmal/Wanna-A, which is the detection name that identifies when a computer suddenly finds the WannaCry payload, which was a file named mssecsvc.exe, so Microsoft Security Service, mssecsvc.exe, plopped into the C:\Windows directory. On a Sophos-protected machine, the client applications immediately, meaning the client AV, immediately blocks and removes any such file. Using this detection data, Sophos has been able to see how many computers are being attacked repeatedly by other computers, that is, causing new instances of that file to be dropped into the Windows directory, as well as the file dropped during the attack.

These infected machines could be on the same network as the ones being attacked, or possibly anywhere in the world. All we really know about the infected machines that attempt to spread the infection is that they don't have a working AV on them because certainly by now all AV has been updated to detect WannaCry. Otherwise they would have stopped WannaCry and would not be attempting to infect other machines. In the three-month period from October 1st, 2018 through December 31st, 2018, so the last quarter of last year, Sophos logged - get this - 5,140,172 detections of CXmal/Wanna-A, nearly two years after the original attack. As nearly every machine that can install the EternalBlue patch has already done so, why are there so many detections?

Leo: Yeah, good question.

Steve: As a sanity check, since the data was nearly a year old, Sophos just in August, two months ago, reran their queries, looking at just one month of attack data, August 2019. They discovered that in that month alone, they had recorded more than 4.3 million attacks against their customers' machines. It seems like a significant increase, but those numbers can be misleading because the data is based on customer machine feedback, and the number of customer reports changes over time as the size of their customer base changes, presumably increasing as they're growing. So that can make the problem seem like it's getting worse when in fact it is uniform.

What was important to note is that the proportion of the total number of attacks targeting Sophos customers in specific countries remained consistent in the data from 2018 and now this recent data in 2019, with the machines in the U.S. topping the list of countries most subjected to failed attempts at WannaCry infections. The fact that WannaCry is still going at all raises some interesting questions. Are all these machines really still not patched? Why is the kill switch not preventing the infected computers from trying to attack others, as indeed they are? Why is no one complaining about files being encrypted?

So Sophos knew the answer to the first question already, that is, are all these machines really still not patched. This CXmal/Wanna-A detection is only possible on unpatched machines. To be sure of this, they investigated a random selection of computers to manually verify that they had indeed not been patched against EternalBlue or anything else in the last two years. And that is the case, even though Sophos's AV is on those machines, they are never being updated for more than two years.

To answer question two, why is the kill switch not preventing the infected computers from trying to attack others? Because that's what it's designed to do. They know the computers reporting the detections have Internet access because that's how they obtain their data. Since those machines are most likely being attacked by infected computers on the same network, it seems likely that those attacking machines would also have Internet access. So why isn't the kill switch stopping them?

Analyzing those 5.1 million detections over last year's three-month period, from October 1st through December 31st, they discovered something unexpected. The malicious file being dropped on these computers was not the original WannaCry mssecsvc.exe file. In fact, among the 5.1 million detections, they identified 12,481 unique files. The original true WannaCry file was only seen 40 times, a number so low that it could easily be attributed to testing rather than real attack. 12,005 of the unique files identified were seen fewer than a hundred times each. So also rare. 476 of the unique files accounted for an overwhelming 98.8, almost 99% of the detections, with 10 of those files accounting for 3.4 million of the detections and the top three accounting for 2.6 million.

So they analyzed those top 10 most prevalent files and quickly saw that they had all been altered from the initial released WannaCry code. The alterations in all 10 samples bypass the kill switch entirely. This means that these 10 updated WannaCry variants' ability to spread is no longer restrained by the kill switch. So they examined all of the files they had discovered and found four different techniques which have been used to render the kill switch ineffective. They found one simply removing or changing the kill switch URL. In roughly half the samples, they simply removed the URL completely. The next most common approach was to change the last two letters from "ea" to "ff." So modifying the kill switch domain resulted in these variants of WannaCry again being unable to obtain a DNS resolution, freeing them to attack.

The second method was to change the code to instruct the malware, regardless of the result of the kill switch test, move to the next command. In other words, just change, tweak the code, a byte or two of the code. They also found an instance where the kill switch was nop'd. The actual op codes were just changed to do-nothing codes, so it didn't

even bother doing the test. And the fourth method was a 2-byte jump instruction to jump over the code that checks the result of the kill switch connection, also resulting in just a simple continuation of the attack.

What's really interesting is that all four of these techniques were implemented with hex editors, hex editing the original WannaCry malware executable binary file, not by recompiling from the original source code. Since anyone who obtains a copy of the executable binary file is able to hex edit it, this suggests that many miscreants around the world, or four or five, were attempting to immediately, two days after Marcus stopped it, because that's how old these are, to immediately untether and unleash the original WannaCry malware worm upon a still unsuspecting world.

We know that the original WannaCry kill switch is still crucially important because, in a recent interview of Jamie Hawkins, who actually was working with Marcus on that fateful domain-registering day, Jamie indicated that in June, just a few months ago, of 2019 alone, the kill switch is known to have prevented about 60 million ransomware events. In other words, today, if that domain were not still registered, 60 million systems would be encrypted by WannaCry, a virulent strain that is still potent and still trying to do this. It's performing those DNS lookups. The answer comes back, yeah, we've got an IP, and it just shuts it down.

If that domain name were not still registered, in one month, 60 million systems - well, or 60 million instances. We don't know how many times each system is doing a DNS query, so it's not 60 million systems, it's 60 million queries. Certainly a bunch of systems. That indicates that there are still potentially at least thousands of computers infected with the original WannaCry, and keeping that kill switch domain online is the only thing preventing a second outbreak.

Okay. So if all of those manually edited, with a hex editor, copies of WannaCry have been unleashed by the hex editing, why hasn't a second massive wave broken out? To answer that question, Sophos executed a random - actually ran, they executed a random selection of samples, including the top 10 that were most prevalent on unprotected computers. In each case, no files were encrypted, and no ransom notes were created. Turns out there's one component that spreads the malware to other machines, and then there is a separate component that does the encryption. This second component is contained within a password-protected ZIP archive. The contents of the ZIP archive are extracted to the computer and then used to execute the ransomware phase of the attack.

In all 2,725 samples, that ZIP archive was corrupted. Errors during extraction appeared after only a few of the archive files had been extracted from the contents, and the extraction stopped. That was the discovery they were seeking which made everything else make sense. The large volume of detections were due to the lack of a kill switch. But nobody was complaining about their files being encrypted because, in every single sample seen in the wild, the archive was corrupt and would not decompress, so the system would not decrypt anything. There but for the grace of God.

Sophos researchers were not the only ones to spot this. Back in May of this year, Kevin Beaumont tweeted - and I have his tweet in the show notes. He tweets, as we've often talked about Kevin's work, he's a well-known security researcher, he tweets as @GossiTheDog. He said: "Probably the most interesting WannaCry thing now is it is still spreading. In fact, there's more spreading than when it began. Why don't we hear about it? Somebody broke the ransomware portion of the variants going around. Almost all of them, like 99% plus, don't unpack."

So as it turns out, this broken payload that appeared almost immediately following the original infection was inadvertently duplicated and promulgated by the bad guys. On May 14th, two days after the May 12th original WannaCry event, researchers at Kaspersky

discovered a variant of WannaCry that had been uploaded to VirusTotal earlier that day. They shared the sample with researcher Matt Suiche, and in a blog post that same day he confirmed that the sample did not have a kill switch, and that the archive was corrupt. So that appeared two days after the original infection. It was also noted that, while the sample had been uploaded to VirusTotal, it had not been seen in the wild.

This sample led to Sophos's final discovery. The MD5 hash of the file uploaded to VirusTotal, which doesn't have a kill switch and doesn't encrypt files, is none other than the exact same file they now see causing the highest number of WannaCry detections. It is number one on the unique file variants list shown earlier, causing 29% of all WannaCry detections in their data.

Even more amazing is that the top three files on their list are all variants of this same file. So the bad guys copied the bad one and put it out there. The other two files contain the same corrupt archive. The only difference is in how the kill switch has been removed. And we talked about those variants. In other words, it's really sort of a true miracle that a subtle mistake made just days after the first WannaCry wave prevented another utterly unrestrained and unrestrainable devastation that would have occurred with WannaCry's immediate return. We lucked out.

Leo: But how long can we stay lucky?

Steve: Uh-huh. Yup, yup. Amazing.

Leo: What a world we live in, my friend.

Steve: Fun to describe it, however, to our listeners, who really appreciate our efforts here.

Leo: Yeah, yeah. Yes, thank you to all of you. It was great fun to see you in Boston. We'll look forward to doing more of these events with Steve. And don't forget our SQRL expos. We'll talk about the ins and outs of SQRL next month, November 30th, the Saturday after Thanksgiving, a special event.

Steve: Assuming that the lights are on.

Leo: They will be. The fires are over by then. Fires always. And, you know, a number of people have said, oh, be careful, stay safe. There are no fires right now. They're doing it proactively.

Steve: Preemptive, preemptive, yeah.

Leo: There are no fires right now. I just want to say that, although we had some terrible ones a couple of years ago. Steve does this show, barring fires and trips to Europe, every Tuesday around 1:30 Pacific. That would be 4:30 Eastern time, 20:30 UTC. If you want to watch live, oh, you can. TWiT.tv/live or listen live, too. That's where our shows stream. We make on-demand versions available on our website, TWiT.tv/sn.

Steve has them, too. And he has a couple of unique versions of the show. Of course he's got the regular 64Kb audio, but he also has 16Kb audio for people who want smaller files, and human-transcribed versions which really make it a lot easier to read along while you watch or listen. And that's all at GRC.com. That's Steve's website. While you're there, pick up a copy of SpinRite, the world's best hard drive maintenance and recovery utility.

Steve: Which just for the record I will be getting back to very shortly. I posted a plan to the SQRL groups, telling them that I was going to have to tweak the documentation a little bit to update it to some decisions we made just before I left for the European tour. And then I'm going to make a tiny change to the server. I'm not going to bother to change the client. I've got a list of things to do, but none of them are showstoppers. There's just some little cosmetic-y things. As with the software that I create, there are no bugs in it. So it's fine. But I am not going to delay getting back to SpinRite. I am going to get back to it very quickly.

Leo: Yeah. And Steve and I talked while we were in Boston about the plans, and this is very exciting. So I look forward to that SpinRite 6.1 and then, maybe someday in the distant future, SpinRite 7. But let's not rush things along. GRC.com. You can tweet at him, @SGgrc; or you can send feedback at GRC.com/feedback. That would be a - both of those are good places. We have our new TWiT Community. I mentioned our forums. Steve's got his forums. They're the SQRL forums. We have forums, too, at twit.community. You can leave your thoughts and comments there. All our shows our posted there, and that's a great place for you to get in a conversation with other people who watch the show, as is our chatroom at irc.twit.tv.

Don't forget to subscribe to the show. That's really the best way. That way you'll get every episode the minute it's available. And you'll never miss an episode. Even if, for instance, Windows Weekly gets deferred tomorrow, if you subscribe, you'll get it the minute we've recorded it. Same with This Week in Google and all of our other shows. So subscription is probably the best way. Then you don't have to worry about our schedule. You can get it on your schedule. Thanks, Steve. We'll see you next time on Security Now!.

Steve: Yay. Thanks, Leo.