Urgent/11

Description: This week we close the chapter on the Marcus Hutchins saga. The U.S. Attorney General weighs in on "warrant-proof" data encryption. We look at what's popular with the underground, give an update on the latest four new ransomware attacks, examine three different attacks on exposed network attached storage (NAS) servers, cover a bit of miscellany, then take a close look at the news of the just-released-yesterday vulnerabilities in the two billion-strong VxWorks embedded OS.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-725.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-725-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. Marcus Hutchins gets his sentence, a terrible show on Netflix, and how software running on over two billion devices is vulnerable to hacking. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 725, recorded Tuesday, July 30th, 2019: Urgent/11.

It's time for Security Now! the show where we cover your security - I'm saying it like a baseball announcer. And in left field, with his giant mug o' Joe, Steve Gibson. Hello, Steve.

Steve Gibson: Yo, Leo. It's great to be with you. We are, as I have said, we are closing in on the end of our 14th year.

Leo: Holy moly.

Steve: Next month by this time we'll be into year 15. And boy, are we not running out of things to talk about.

Leo: Things aren't getting any better, are they.

Steve: Oh, my god. So this is Episode 725. I was going to call this, I was all set, everything was like - the show notes were written. The outlines were put together. The title of this was going to be "Your NAS Is Grass."

Leo: I like it.

Steve: And I did, too. Until yesterday's shocking announcement of 11 serious flaws in an embedded OS that no one has even probably ever heard of before called VxWorks. And VxWorks has been sort of like the secret weapon of embedded designers for the last 32 years. There was something, there was Charles River Systems, and then Wind River Systems. Oh, and Ready Systems was the original source.

Leo: Yeah, I remember all those. Yeah, yeah.

Steve: Way back, more than three decades ago. Unfortunately, it's closed source, so it's never been subject to anyone scrutinizing it. And it turns out that it is everywhere. I mean, it's almost laughably everywhere. It's what the Mars Rover runs on.

Leo: Wow.

Steve: So, yeah. And it turns out that, so, like, there's two billion installs. It's what IoT devices are all using. Those that aren't using a little trimmed down Linux kernel are pretty much using VxWorks.

Leo: It's funny because I just don't know that name. Wind River I know absolutely.

Steve: Right.

Leo: So they must have gone by that for a long time.

Steve: Yes, exactly.

Leo: Yeah.

Steve: So anyway, unfortunately, "Your NAS Is Grass" ended up becoming a subtopic of the show rather than our title, which is "URGENT/11," which is the formal title given by Armis, Inc., who reverse engineered, they got old, like, obsolete source to kind of give them a start. And then they had to reverse engineer the binary of installed in-place VxWorks in order to take a look at it. And what they found was horrifying. It turns out that all of these devices that are connected to the Internet - the good news is the Rover is not on the 'Net. But, you know, surprising things are, like SCADA systems that are controlling all of our nuclear reactors.

Leo: Great.

Steve: I mean, that's all VxWorks. And everybody's car has VxWorks in it. So anyway, that took over the podcast, and we will be talking about that in detail. We're going to close the chapter, happily, I mean, a happy ending on Marcus Hutchins, that whole two-

year saga we've been following since he was nabbed when leaving Las Vegas. We have our U.S. Attorney General weighing in on warrant-proof data encryption and how horrible that is. We look at what's popular with the underground, in the underground of the Internet.

We'll update on the latest four new ransomware attacks which have occurred since last week. We'll examine three different attacks on exposed NAS servers that, as I said, were going to be the main topic, but that got supplanted by VxWorks. We'll discuss a little bit of miscellany and then take a close look at this news of these just-released-yesterday vulnerabilities in two billion installs of devices using VxWorks, for example, all - well, not all, but most SonicWall firewalls are using VxWorks. And so, I mean, it's designed to be on the Internet, which unfortunately is not where you want it to be right now. So I think another great podcast for our listeners.

Leo: Sounds fantastic, as always.

Steve: So our Picture of the Week I got a kick out of. Someone tweeted it to me a couple weeks ago, and now we have a slot open for it. It's a cartoon with four frames. First frame shows a guy saying, "Thanks to Windows Subsystem for Linux," second frame, "I can have the workflow of Linux in Windows." Then the third frame shows the blue screen, "Working on updates. 11% complete. Don't turn off your computer." And of course, you know, with the rollercoaster dots spinning around. And the fourth frame has this creature looking at us again saying, "Marvelous." So, yeah. Not quite the entire Linux experience. Thank you, Windows.

Leo: It does make you wonder, why bother? Just put Linux on your machine.

Steve: Oh, my goodness, yes. Why?

Leo: Why do you want to wrap it with Windows? Yeah.

Steve: Yeah. So Marcus Hutchins is free. Free at last. It was two years ago this coming DEF CON. After the annual 2017 DEF CON security conference, as Marcus was - I guess he described himself as still sort of suffering, he was hung over and intoxicated from partying the night before. He was walking through the Las Vegas airport...

Leo: That's when they get you.

Steve: Yeah. You have your guard down.

Leo: Yeah.

Steve: Preparing to return home to the U.K. He was nabbed by law enforcement. And of course he had been for many years a reformed gray or black hat, I guess. I don't think he ever actually participated in malicious hacking, but he did write some, in his youth, as an adolescent, he wrote some malware. Anyway, he was nabbed and held on charges of

computer hacking, fraud, and abuse. It wasn't long before he was released on bail from jail, but I think he had an ankle tracker.

So he was working with attorneys, and we've talked about him several times over the last couple years as his case has moved through the legal system. And he's been working with his defense team and appearing at various legal hearings from time to time. We know that he had outgrown those earlier, you know, his sort of sketchy adolescence where he was doing some things that were not on the up-and-up. And let us not forget that what initially brought Steve Jobs and Steve Wozniak together was their interest in what was known as "blue boxing," which were these little boxes which generated different sets of tones than the normal touchtone tones, which were used to sidestep the long-distance telephone billing that the U.S. telephone system used for making free long-distance phone calls. So, you know, even our contemporary tech heroes were not always on the up-and up.

Anyway, shortly before his arrest, he was studying, that is, Marcus was studying the alarming emergence and rapid propagation of the incredibly prolific and dangerous WannaCry Internet worm. And in his research he serendipitously halted its progress, and we've talked about this many times, by looking inside the code, seeing that there was kind of an odd DNS query that the worm was making. When he looked up what the DNS domain was that it was querying, he found it was unregistered. He thought, okay, that's weird, I wonder what it's doing with that DNS address? So he registered it. And in the process of it no longer being unregistered, just that act halted the worm's propagation. And we never really understood in detail, like we never had a clear understanding of why. It's believed that that was a kill switch, which Marcus, as I said, serendipitously set in order to cause the worm to stop propagating.

And it turns out that this was taken into account. U.S. District Judge Joseph Peter Stadtmueller said that the malware Hutchins helped stop was much more damaging than the two programs he created, and thus sentenced him only to time served, with a year of supervised release. So Marcus is free to return to the U.K. He tweeted on July 26, which was last Friday, he tweeted first: "Heading into court now. No matter what happens, I love y'all." And then a short time later he tweeted: "Sentenced to time served! Incredibly thankful for the understanding and leniency of the judge, the wonderful character letter you all sent, and everyone who helped me through the past two years, both financially and emotionally." That was at 11:25 a.m. last Friday.

So he's free to return to the U.K. U.S. authorities still need to decide whether he's now barred from returning to the U.S. due to his "criminal record." And of course in my opinion barring him would be really dumb. But on the other hand, we did say "U.S. authorities." So, you know, we'll see what happens. So that's good news, a nice outcome. And it would be nice if he were free to return. His presentation at Black Hat or DEF CON was about what he had just done with WannaCry, and so after demonstrating, I mean, he had been doing other white hat hacking things. As he know, his Twitter handle was MalwareTechBlog. And so, you know, he was blogging about how to stop this stuff now. And anyway, so this was the right outcome. And it would be nice if we let him come back to future Black Hat and DEF CON presentations.

And Leo, I have a two-minute YouTube video of U.S. Attorney General William Barr on warrant-proof data encryption.

Leo: Oh, is this the speech he was giving? Oh.

Steve: Yes. This was two minutes. So I thought it would be worthwhile to play this into the podcast since this is the...

Leo: Go ahead. I'm sorry.

Steve: Yeah, no. Let's just go ahead and play it.

Leo: All right.

[YouTube clip]

WILLIAM BARR: The deployment of warrant-proof encryption is already imposing huge costs on society. It seriously degrades the ability of law enforcement to detect and prevent crime before it occurs. And after crimes are committed, it is thwarting law enforcement's ability to identify those responsible or to successfully prosecute the guilty parties. These costs will grow exponentially as deployment of warrant-proof encryption accelerates, and criminals are emboldened by their ability to evade detection. Converting the Internet and communications platforms into a law-free zone, and thus giving criminals the means to operate free of lawful scrutiny, will inevitably propel an expansion of criminal activity. If you remove any possibility that the cops are going to be watching a neighborhood, the criminals already in the neighborhood are going to commit a lot more crimes.

But there has been enough dogmatic pronouncements that lawful access simply cannot be done. It can be, and it must be. We are confident that there are technical solutions that will allow lawful access to encrypted data and communications by law enforcement without materially weakening the security provided by encryption. But I am suggesting that it is well past time for some in the tech community to abandon the posture that a technical solution is not worth exploring and instead turn their considerable talent to developing products that will reconcile good cybersecurity to the imperative of public safety and national security.

[End clip]

Leo: That seems somewhat similar to your point of view. Yes?

Steve: Well, the devil is in the details, of course. And my feeling is that, in some of these ecosystems, it's possible for us to do some of it. For example, as I was just saying recently, right now Apple is managing the encryption keys for iMessage. So it would be possible to have a hidden participant in iMessage conversations that in no way does it weaken the system except that, yes, you are making a conversation available to a third party. But it's still entirely under Apple's control, as it is now.

But of course, if you try to broaden this too far, for example, if the government were to say we need the ability to decrypt any TLS connection, now that's a horse of a different color. That's a whole different problem where they're saying, you know, we need, I mean, that really would then be some form of a backdoor if you said, you know, we need to be able to get into any TLS connection between a web browser and a server. That's a big different problem.

So, I mean, it really is the case, if I were to play devil's advocate to myself, it really is the case that the technology we have developed is secure point-to-point encryption that we've developed this technology, we the industry, over decades, without the assumption that a backdoor is going to be required, and the technology doesn't allow it. So the

reason this is consistent with my position on iMessage is that iMessage is a layer above. It's still supporting encrypted point-to-point, but the points are aggregated, and messages are being reencrypted by Apple in order to send them to other devices.

So it's not at all clear how you would implement the ability - which is what Bill Barr is saying. He's saying that, essentially, they want to be able to decrypt everything; that they don't want the Internet to be a, quote, "law-free zone." So I'm 100% onboard with the position that none of our fundamental encryption algorithms support this today. They don't. I mean, they don't. So if it would be acceptable to encrypt, to somehow make the data available outside of the encrypted connection, which is what iMessage does, and which is what I've been talking about, then we know how to do that. But we don't know how to make all of our current point-to-point encryption accessible to a third party. It isn't currently. It just isn't, fundamentally.

So anyway, I thought this was interesting because, if a compromise can be reached, then I think a compromise is technically feasible. But if something like the government demands to be able to decrypt everything is what they're asking for, that really can't be done. I mean, that really requires going back to the drawing board. I mean, there are really advanced, much different schemes for encryption, sort of like at the next level, things like homomorphic encryption where, I mean, it's a whole 'nother generation of encryption which isn't currently in use and deployed. And, I mean, it really does send us back to the drawing board from where we are today.

Leo: I feel like the real issue, and the thing that they're going to end up going for, look, it's too late to prevent VeraCrypt and other strong encryption technologies from existing. You can't stop that.

Steve: It's out of the bag; right.

Leo: It's out of the bag.

Steve: It's math.

Leo: So they know that. So what this really is, is to get Samsung and Apple and all the other phone manufacturers who ship with encryption to provide backdoors. And they'll be happy with that. And any criminal who wants to use Signal can continue to use Signal because you can't stop Signal. It's done. So you're not going to be able to go to Moxie Marlinspike and say could you please put in a backdoor. He's going to laugh at you.

Steve: Although the API that Signal uses is the OS's API. And so...

Leo: Ah, yes. So that's why I'm saying, if you can get the phone, you're going to get 90% of what you want anyway.

Steve: Right. And you can grab, you can tap the keyboard and the screen before and after Signal does its encryption and its decryption.

Leo: So if you want privacy, you're going to use open source software. You're going to use an open source operating system. You're going to use existing crypto tools, open source. And you can...

Steve: Actually, if you want privacy, you're not going to use a smartphone.

Leo: Just don't use a smartphone. There are coming FOS smartphones. There's a Firefox phone. Librem is making a phone. And I think that's really what they're aiming at is that day in the not-too-distant future when no commercial device will ship with strong encryption, or foolproof encryption.

Steve: Or without the ability to be served a warrant and have its contents available.

Leo: But despite what AG Barr said, we know that, if you put a backdoor in devices like that, you can't - I don't think you can keep it to law enforcement only. A backdoor, any extant backdoor, even if requires a warrant, well, you've talked about ways maybe a company like Apple could have secret keys that they keep in a vault kind of thing.

Steve: Yeah, yeah, I mean, again, it's easy to use Apple as an example because they've built such a sophisticated, controlled environment. So right now Apple goes to great lengths to explain how they do not have the key to the secure enclave, how the device generates it and never sends it. Well, that's their choice. They've chosen that. But if the device, over a secure connection, after generating its secure enclave key, I mean, and again, Apple could do this if they wanted to. If it shared that...

Leo: Or are forced to by law.

Steve: Yes, or are forced to.

Leo: Because I don't think they'll ever want to. But if they're forced to.

Steve: Right, right, right. So, and I meant "want" from a technical standpoint. They could receive that secure enclave key. So the counter argument is that having Apple, some Apple storage of all of the enclave keys for all of their devices is a weakness. And there's no argument to that. Right now they don't have, you know, you can't lose what you don't have. No one can hack what you don't have. So they don't want to have the secure enclave keys. They really, really, really don't. And notice that their security model, their privacy model, their sales model is we don't have those keys.

Leo: Yeah. But can I point out they do have the keys to iCloud, and they do encourage everybody to back up everything to iCloud?

Steve: Yeah, right.

Leo: And they even told the FBI, well, if you'd only let the phone back up to iCloud, we could have given you everything.

Steve: Yup, yup.

Leo: So honestly, Apple, well, I don't know what Apple really thinks. But it seems to me more a marketing strategy than anything else.

Steve: Yeah.

Leo: And you're right. If you wanted to stay private from the government for whatever reason, and by the way I think increasingly it becomes clear it isn't merely because you're unlawful or a bad person, you merely could be a dissident, and you want to keep your stuff private, you won't use a commercial device of any kind, computer or phone. Period. You can't because those companies will be compelled by law, by the law of the country they're in, whether it's the U.S. or China, to provide backdoor access to law enforcement.

Steve: As we've said, if you really, really, really want private communication, you meet with someone naked in the middle of Central Park, throw a blanket over you so that your lips cannot be read, and you very - oh, and you use - I don't know if paper and pencil would be safe either. Maybe just whisper.

Leo: Don't write anything down, that's for sure.

Steve: Right, right.

Leo: And by the way, they now have satellites that can read that pencil and paper over your shoulder. So maybe cover your mouth, too, while you're talking.

Steve: Yeah. I mean, it's just - yeah.

Leo: It's pretty hard to defeat somebody with the resources of a government.

Steve: Yes. And the problem is that this technology is so convenient that it's what gets used. It's like, if you really, really, really want to be secure, you have to be physically in the same location and whisper into somebody else's ear underneath a blanket. Otherwise, as soon as you start wanting convenience, you sacrifice true security. You know, it's easy, easy to have the appearance of security, for everyone to feel happy and, like, oh, yeah, we've got encryption. But it's like, okay, great. You also have malware on your phone that's sending everything that is encrypted, before it gets encrypted, somewhere else. So, yeah.

Leo: I think it's prudent to start preparing ourselves and thinking about what it means to be private, how we would achieve that privacy, how we would know if it wasn't private, what things to look for, all of that.

Steve: Well, and really, as we also said, Leo, does it really matter? Does anyone care?

Leo: It doesn't matter now. I'm not convinced it's not going to matter in the next five years.

Steve: Yeah.

Leo: I'm not completely sanguine about the future of liberty in this world.

Steve: And there are places where we really do want strength, like our voting systems. We would like our voting systems to be immune from the fact that we just learned that Russia was actively trying to not hack just one or two locations, but all 50 states during the 2016 elections.

Leo: Which is why I really question the motivation of our government when they say, "And we want a backdoor." Because they've got to understand that that makes us vulnerable to everyone.

Steve: Yeah. It will be, I mean, again, I can't think of a more interesting issue like for right now where we are. And, boy, I hope this gets resolved by podcast 999 because, you know, otherwise...

Leo: You're going to have to stick around, Steve, I'm sorry. You need to keep going until we get the job done. That's all I'm saying, Steve.

Steve: So what is popular on the Internet underground? The firm Recorded Future did a bunch of really interesting sleuthing. They assembled a beautiful report titled "Bestsellers in the Underground Economy: Measuring Malware Popularity by Forum." And for anyone who wants the details, I'm just going to cover the top layer. But I've got the link both to their posting and also to the detailed PDF that has a whole bunch of interesting graphs.

In summary, they said: "By analyzing over 3.9 million posts from May 2018 to May 2019" - now, first of all, hold on. In one year there were 3.9 million posts? Think about that. That's a lot of posts in a year. They said: "...across all underground forums indexed by the Recorded Future platform. Recorded Future's Insikt [I-N-S-I-K-T] Group identified the top malware variants being referenced on underground forums. The Insikt Group also attempted to find real-world events that correlated with a higher number of malware references on these forums, as well as differences in tools advertised in forums of different languages, to see if any differences existed.

"The Insikt Group discovered that a majority of the top 10 mentions of malware in multiple languages included openly available dual-use tools, open source malware, or cracked malware. Some of these malware families were also over three years old or could be mitigated with basic security precautions. Activity in underground forums that

correlated to growth in malware references included sale of malware in a larger bundle, advertising updates to the malware, advertisements of the malware on a new forum in which the malware was not previously sold, news articles related to malware shared on forums, and community engagement.

"Insikt Group also discovered that underground communities in different languages did indeed focus on different malware, malware categories, and attack vectors." So there was language-based bias. "English- and Chinese-speaking underground communities, for example, focused more on Android malware than other communities. By separating forum advertisements by language, Insikt Group found that forum members occasionally used online translation services to attract business partners and buyers from different language communities."

Then they broke this all down into four key judgments, which I'm going to share. But it's interesting. Reading between the lines is really interesting because it sort of shows what is and what is not happening there. So there are four key judgments. The first was "The top 10 mentions of malware across Recorded Future underground forum collections suggest that underground forum members are discussing and using tools readily available to them more often than paying for or inventing new tools."

Second: "Based on the prevalence and longevity of the malware, Insikt Group assesses with medium confidence that there likely exist enough victims who do not comply with basic security precautions for forum members to successfully infect." Okay, so in other words, the stuff being transacted on these forums is still effective.

Third: "Approximately half of all activity concerning ransomware on underground forums are either requests for any generic ransomware or sales posts for generic ransomware from lower level vendors." They wrote: "We believe this reflects a growing number of low-level actors developing and sharing generic ransomware on underground forums."

And, fourth: "The Insikt Group assesses with medium confidence that, due to the number of underground forum members sharing, deploying, and providing reviews about malware and its functionality, the 10 most popular malware on underground forums hit host computers with higher frequency, but are low to moderate threats compared to other malware due to their age, ineffectiveness without a delivery vehicle or crypter, and existing AV detections."

So what was interesting, and I did read the whole report, so I'm also pulling from there, but this suggests a few things. For example, I scanned the charts and the graphs and the detailed description for, for example, any mention of Ryuk, which is, as we know, the ransomware that is actually doing damage to municipalities. It is nowhere. Why? Because it's high-end, proprietary, upper-crust ransomware.

Leo: Oh, we only use the best ransomware.

Steve: The ransomware, well, it's not been let go of. It's not been released. The ransomware that's for sale in these forums is sort of the equivalent...

Leo: The old crap. WannaCry. Yeah.

Steve: Yes, yes. The second-hand, non-state-of-the-art, hand-me-down ransomware.

Leo: I might make a different distinction, that Ryuk is spearphished, targeted attacks.

Steve: Yeah.

Leo: Whereas WannaCry and others are where they just email a million pieces out and just see what happens.

Steve: They're just spraying it, yes.

Leo: Just spraying it.

Steve: And also those who are capable of writing state-of-the-art ransomware are not selling it in these forums.

Leo: Yeah. They keep it themselves.

Steve: They're not selling it at all, exactly. They are, rather, they are deploying it. And so perhaps in five years Ryuk will be seen changing hands within the underground community, but not today. Today it's earning a reputation that will evolve into mythology. And then that mythology will eventually be driving its aftermarket release. But that will be long after Ryuk's authors have moved on to the next whatever it is software to achieve their ends.

And so that brings us to this week in ransomware. Lawrence Abrams headlined his weekly snapshot ransomware coverage for his BleepingComputer posting, he called it "State of Emergency." And he started off with a declaration that I think is all too true. He wrote: "Now that ransomware developers know that they can earn monstrous payouts from local cities and insurance policies, we see a new government agency, school district, or large company getting hit with a ransomware attack every day." He said: "For example, this week the Governor of Louisiana declared a state of emergency for the wave of attacks targeting school districts in the state."

Anyway, so that's all I'll share from that. But what happened in this past week? Louisiana's Governor John Bel Edwards last Wednesday declared a formal state of emergency after three public school districts were taken over by ransomware. The reason for them making it a declaration of a state of emergency is interesting, and we'll get to that in a second. One of the three school districts, which was the Sabine Parish in Northern Louisiana released the following statement.

They said: "The Sabine Parish School System was hit with an electronic virus Sunday morning. This virus has disabled some of our technology systems and our central office phone system. The district staff reported this electronic viral attack to local law enforcement, state officials, and the FBI. All available resources are being utilized to get the district systems back online. An investigation involving local, state, federal law enforcement is ongoing at this time. The school phone systems were not affected by this attack." But the district systems were, as opposed to the individual schools.

"The central office phone system is being repaired, and service will be restored as soon as possible. According to the Louisiana Department of Education, several other school

districts were attacked by the same virus this week." And apparently that is the case. We don't have any details yet, but does anyone want to bet that it wasn't Ryuk, since that does seem to be what's being used in all of these recent attacks. State officials have not yet released a full list of the affected systems.

Eddie Jones, who is a principal of the Florien High School within the Sabine Parish, told the local news station KSLA that his technology supervisor received an alert on his phone around 4:00 a.m. Sunday morning about a surge in bandwidth usage. So that was probably an automated report. And he said it was particularly unusual given first the time of day, and also the fact that schools are all on summer break. When technical staff investigated, Eddie Jones said they found ransomware on the servers. The principal said that he doesn't believe that any sensitive information was lost. But what was lost was "anything and everything," quoting him, stored on the school district's servers, including 17 years' worth of Jones' personal documents - his speeches, test schedules, master schedules, and more.

What's interesting is that the declaration of a state of emergency means not only that state resources will be made available, and that assistance will be coming from cybersecurity experts from the Louisiana National Guard, Louisiana State Police, and Office of Technology Services and others to assist local governments in responding to the crisis and preventing further data loss, but also the declaration of an emergency includes protection from being price gouged for the cost of extra help and resources, which apparently has been a problem previously.

Leo: Oh, interesting. Ah.

Steve: Yes, uh-huh. The language concerning that protection from a Louisiana proclamation about states of emergency reads: "During a declared state of emergency, the prices charged or value received for goods and services received within the designated emergency area may not exceed the prices ordinarily charged for comparable goods and services in the same market area at or immediately before the time of the state of emergency..."

Leo: C'mon. That's just surge pricing. C'mon.

Steve: "...unless the price by the seller is attributable to fluctuations in applicable commodity markets."

Leo: It's a fluctuation. That's what's going on.

Steve: Yeah, uh-huh. It's a fluctuation, "...fluctuations in applicable regional or national market trends, or reasonable expenses and charges and attendant business risk incurred in procuring or selling the goods or services during the state of emergency."

So what's interesting is this is the first time that Louisiana has activated its emergency cybersecurity powers, which were created for just this type of cyberattack. There response is being handled by the states' newly formed Cyber Security Commission, which was established two years ago, in 2017. It brings together the state's key stakeholders, subject matter experts, and cybersecurity professionals from Louisiana's public sector, private industry, academia, and law enforcement. So anyway, three districts in Louisiana, Northern Louisiana, were all hit. So it's interesting that the timing was coincident for

those three. It's probably the case that there was some network connectivity among them that allowed a successful penetration to get into those districts. So they were likely linked in some fashion.

Leo: Well, but remember the school calendar, too, Steve. Because these districts are closed for the summer. Administrators come back right about now. Teachers come back in, getting ready. They open their email. They click those links.

Steve: Yes, yes. And I was thinking that it might...

Leo: Get ready, because there's going to be a whole bunch of them soon; right?

Steve: Yes. I was thinking it was likely that there would be less pressure on them to get their systems up. But following up on all of this, it turns out that they're, like, a week away from needing to get themselves up and going. So you're exactly right.

Leo: Yeah, there's no coincidence, yeah.

Steve: You're exactly right, Leo. Probably it was email that was, like, waiting for them. And then just yesterday we learned of a fourth Louisiana school district. And I can't even begin to pronounce this: T-A-N-G-I-P-A-H-O-A, Tangipahoa.

Leo: Laissez les bons temps rouler. Tangipahoa. I think you're right, Tangipahoa, yeah.

Steve: Tangipahoa. Anyway, they're down, too. The Advocate in Baton Rouge had an article that stated just yesterday a fourth Louisiana school district was attacked. In local reporting of that attack, the comment was made that the timing was especially troublesome since school was scheduled to resume in about a week. So I guess they are all under significant pressure to get themselves back up. And I guess we will find out.

Leo: I guess we're going to see a lot more of this in the next month, is what I guess.

Steve: Oh, boy. Yeah.

Leo: Yeah. Wow.

Steve: Deep pockets and insurance companies and very effective ransomware.

Leo: Well, and also administrators and teachers coming back a couple weeks before the kids do.

Steve: Yup, and saying, gee, well, and kind of being in a hurry to catch up on all of the mail that they got in their inbox and maybe being a little less cautious. So yikes.

As I said, until the Urgent/11 announcement, this podcast was going to be titled "Your NAS Is Grass." One by one, as we have been seeing, service by service, we have been seeing attackers targeting anything that's exposed and is either deliberately or inadvertently offering services to the Internet. Last week's podcast was titled "Hide Your RDP Now" because, as we saw, even non-BlueKeep-vulnerable RDP services and servers were under attack to a sobering degree with password guessing. So now we're looking at NAS, Network Attached Storage, because it turns out those are often, by nature, I mean, certainly some NAS is inside the organization. It's providing Intranet services. But it's often the case, unfortunately, that these things have a public exposure, as well.

Earlier this month a campaign targeting the NAS devices produced by the Taiwanese company QNAP Systems, Inc. was uncovered by researchers at Anomali Labs. They found that QNAP's devices were being compromised, both by brute-forcing weak credentials and exploiting known vulnerabilities. And, once infected, a malicious payload was then encrypting specific file extensions on the NAS - thus we're talking ransomware - using AES encryption and then appending the .encrypt extension to the encrypted files.

After that was done, the following ransom note was left behind. It reads: "All your data has been locked (crypted). How to unclock," actually it says in a typo "(decrypt) instruction located in this Tor website." So then it pointed people to a .onion Tor site with a bitcoin address and with the instructions, "Use Tor browser for access .onion websites." And then it gives you a DuckDuckGo URL with the link to search for "tor browser how to" in order to instruct the person how to use Tor in order to go to the onion address.

Leo: I like that they're using DuckDuckGo, though. I think that's good. They really care about our privacy, yeah.

Steve: Wasn't that a nice touch, Leo? Yes, exactly. Then they say: "Do not remove this file and not remove last line in this file," which contains the cryptographic key, Base64 encoded, which is necessary to be provided to them in order to decrypt the NAS. So basically we have brute forcing of either, well, not only QNAP, but probably any. But in the case of QNAP they're able to get in, install malware, encrypt all of your files. And presumably, if it's a NAS, it's got a lot of storage and a lot of stuff that you care about.

Leo: A lot of stuff, yeah. You're backing everything up there, yeah.

Steve: And so it's ransomware. They reverse engineered the ransomware, discovered that it had been written in the Go programming language; that it was very straightforward, not very complex; consisted of fewer than 400 lines of code. Upon execution, the malware first reaches out to its command-and-control server, listening on IP 192.99.206.61 on some high-numbered port, I don't remember which. That notifies it that the encryption process has started. The malware then walks the file system hierarchy, looking for files that have not yet been encrypted, meaning don't have the .encrypt extension already, and encrypts them, then appends .encrypt to the end. Once it's done, it again contacts the command-and-control server, notifies it of completion, and produces the ransom note, which it leaves behind.

And in the coverage of this I thought that they made a good point, which is that NAS devices are not normally running any form of AV software since they tend to be turnkey embedded systems, often without a screen or keyboard. They're just, you know, mount

them in the rack or put them somewhere, plug them in, and they go. Even so, at the time of its discovery, VirusTotal reported that only two or three out of, what, like 70-some AV systems that VirusTotal queries were detecting this malware as being malicious. So it had not been seen widely before and had not been submitted for analysis before such that it was largely unknown by VirusTotal.

And in their conclusion the researchers recommended that external access to QNAP NAS devices be restricted. Ensure that the device's firmware is current, up to date. Use strong credentials. And, I mean, that's super important for any devices that are exposed to the Internet. As we saw last week, there is a real upsurge in Internet-connected things. We talked about RDP brute forcing. Now we're looking at NAS device brute forcing.

Leo: I think a lot of these NASes are unsophisticated people [crosstalk].

Steve: Yes.

Leo: And they really are vulnerable. And they're using monkey123. I mean, on my Synology I have two-factor enabled. I've turned off all services. I don't have FTP turned on. If you turn on SSH, don't use passwords, use SSH keys. I mean, there are just ways to secure any server that are sensible. And I do see, every time I look at my log, I see Chinese IP addresses and others trying to brute force the password. It's every day. And Synology has - I'm sure QNAP does, too, because it's very good - a feature where you say, if somebody tries to log in five times from a single IP address and fails, block that IP address forever. And I do that, too.

Steve: Yes. Good.

Leo: So, I mean, honestly, I think it's not terribly difficult to secure your NAS. But I think a lot of these are just people plugging them in.

Steve: Yeah. Well, and speaking of Synology, that's story number two here. Last week Synology issued an urgent warning titled "Synology Urges All Users to Take Immediate Action to Protect Data from Ransomware Attack." And this was July 23rd. They said: "Synology recently found that several users were under a ransomware attack, where admins' credentials were stolen by brute-force login attacks, and their data was encrypted as a result. We investigated and found that the causes of these attacks were due to dictionary attacks instead of specific system vulnerabilities."

Leo: Yeah. Yeah.

Steve: So props to Synology, exactly as you were saying, Leo.

Leo: And they offer two-factor, which would also be a good thing to do in this case.

Steve: Yes, yes. And I'm wondering if here, blah blah blah blah blah. Ken Lee, Manager of Security Incident Response Team at Synology said: "We believe this is an organized attack. After an intensive investigation into this matter" - oh, because several of their

users did have ransomware attacks - "we found that the attacker used botnet addresses to hide the real source IP after collecting admin account passwords with brute-force attacks. Since this attack was not related to system security vulnerabilities, it's recommended that Synology users utilize built-in network and account management settings to enhance system security level, preventing malicious attacks from the Internet."

So this is just like a general, you know, please protect yourself because if these boxes are publicly exposed, they are going to be brute-force attacked. And so the end of their announcement said, exactly as you said, LEO: Use a complex and strong password and apply password strength rules to all users. Create a new account in the administrator group and disable the default "admin" account. Enable - and here's the nice feature - Auto Block in the control panel to block IP addresses with too many failed login attempts. And then run the Security Advisor to make sure there are no weak passwords in the system. So, you know, Synology is a beautiful piece of equipment. It doesn't have a problem. But if you expose it publicly, and you use a weak password, you're going to get yourself taken over.

Leo: Put your server on the Internet.

Steve: Yes, yes, yes. Deliberately.

Leo: Yeah.

Steve: And so third and last, and this is unfortunately not a strong use case, as Synology is, Lenovo-EMC and Iomega have a significant flaw. And when I saw Iomega, it's like, what? Iomega? They're still around? Well, it turns out that 11 years ago, in 2008, EMC bought up the assets of Iomega. Then five years ago a Lenovo-EMC joint venture relaunched Iomega as LenovoEMC. So today we have an Iomega/LenovoEMC vulnerability announcement.

Our story begins with an intrepid employee with the infosecurity firm Vertical Structure, based in Northern Ireland. He first discovered files apparently being publicly exposed on the Internet via Shodan.io last year. After a bit of additional sleuthing, Vertical Structure confirmed that documents, a great many documents actually, were being publicly exposed to the Internet, without any password or authentication checks, through an unauthenticated API.

So here we have a situation where people were putting these NAS devices on the Internet. And unfortunately, they not only offered the standard file access API, but a different API elsewhere, that is, running on other ports with no authentication. Clearly, I mean, assuming that the designers of this weren't completely out of their mind, they assumed that this NAS would not be publicly exposed, or that it would be behind a firewall of some kind so that all of the ports of the NAS's IP were not public. But that didn't happen.

The exposed API was eventually tracked down to belonging to an older set of Iomega NAS boxes that were - thanks to this widely exposed and unauthenticated API - now, today, leaving many millions of files, more than three million as it turns out, totaling 36TB of information, exposed on the Internet. Simon Whittaker, a director at Vertical Structure, the group that found this, said there were a significant number of files containing sensitive financial information, including credit card numbers and financial records.

Vertical Structure was able to track down the common source, a legacy Iomega storage product acquired by EMC and co-branded LenovoEMC as a result of their joint venture. Within those three million files, Whittaker said there were 405,000 images, 20,055 documents, 13,677 spreadsheets, 13,972 text documents, and then lots of other stuff to bring the total above three million. After realizing the extent of the exposure, Vertical Structure called in the firm WhiteHat in Silicon Valley, who ran their own independent investigation of the leak and confirmed that public-facing Iomega-LenovoEMC devices were indeed spewing all of their data onto the Internet via an unauthenticated API.

The two companies alerted Lenovo to the problem, and the vendor responded, Lenovo responded by bringing the software essentially out of retirement to address the bug. There is now a LenovoEMC NAS vulnerability disclosure. There's a patch available. I've got a link to it in the show notes. So if anybody listening has an older Iomega NAS, you want to make sure that it is not among those that are vulnerable. I can't remember the name. There was a bunch of them that were just a bunch of cryptic, weird-looking names. But something "Stor" something, S-T-O-R - I ought to just click on this link, if I've got it right here in front of me, and bring up the announcement. StorCenter. So the bulk of them, one, two, three, four, five different StorCenter NAS Cloud Servers and others.

So anyway, if you have an older NAS device, you want to make sure that you bring this thing current. So as it would you, Leo, it makes me shake my head that even consumer NAT routers provide more security to us than we're seeing in a commercial NAS like this. The idea that this thing could apparently, by default, be publishing an unauthenticated API on its public-facing interface is just crazy. As I said, it must be that the designers intended this to be behind a firewall so that somebody would only be mapping the NAS normal interface through from the public, rather than putting it out publicly.

And that's just, as a word of advice for all of our listeners, don't put a NAS on - don't give it its own public IP. Put it behind a NAT router. Map the ports that you need through to it. Put it behind a firewall. Only map through to it what you need. There's just no safe way to make a device like that, to give it its own IP and say to the Internet, here, scan this device and attack anything that says hello when you connect to it because that's what Shodan did. And Shodan found all of these things, incredibly.

Okay. Time for a little fun, Leo.

Leo: Well, or not.

Steve: Or not. I did mention the show on the podcast. I don't remember if it was with you two weeks ago.

Leo: Yeah, two weeks ago. You liked the publicity stills of Katee Sackhoff in her skivvies.

Steve: Ah, right. I did, indeed.

Leo: That should have told us something, by the way.

Steve: Yeah. She's better known to us as Starbuck...

Leo: Starbuck, yeah.

Steve: ...from "Battlestar Galactica," which is a much-appreciated sci-fi series.

Leo: Great show, yeah.

Steve: So I did have - I had high hopes for the Netflix series "Another Life," which dropped in its entirety last Friday. I tweeted immediately after: "The best thing about Netflix's much-anticipated, incredibly, unbelievably awful and disappointing science fiction series 'Another Life' are the reviews on IMDB."

Leo: Which are universally terrible.

Steve: Oh, my god, Leo.

Leo: But I figured it out after watching 10 minutes of this. I knew exactly. This is very Hollywood. Somebody said, "We want to give Katee a show." "Well, she's got to be in her underwear," somebody else said. Then somebody said, "You know what's hot? You know what the kids like these days? They like those reality shows like 'Big Brother' or 'Real Life,' where you take a bunch of young people, you put them in a house, and you let them fight it out. What if we did 'Big Brother in Space'?"

Steve: That's exactly what happened.

Leo: And that's what it is. It's awful.

Steve: Yes. Yes. It is un- well, I mean, it just - it isn't for us. It isn't for our listeners.

Leo: I don't know who it's for.

Steve: It isn't actually science fiction. I mean, it's just unbelievably bad.

Leo: The first 10 minutes are all exposition. I mean, I hate it when you put words in people's mouths like, "Well, and then the alien artifact arrived on Earth, and everybody wanted to know where it was going," I mean, they were explaining the whole thing. But the best line, my favorite line was once they get on the ship, and it's completely out of nowhere, it's not in response to anything, Katee says, "Well, 10 years ago they said we didn't have to wear uniforms in space." And it's clear that they did that so that people could be dressed in high heels and leather pants and skivvies.

Steve: Yes, I mean, there was somebody in high heels, Leo.

Leo: Which is of course very practical for space.

Steve: That's right, yes. And, I mean, oh, I won't go any further. It was just...

Leo: It was awful.

Steve: It was unbelievably bad.

Leo: Yeah. But not so bad - not like "good" bad. It's bad bad.

Steve: Well, and I have to say, if you are a Netflix subscriber...

Leo: It's pretty.

Steve: It's really almost worth 30 minutes. Lorrie and I got 30 minutes in.

Leo: You got further than I did. I couldn't.

Steve: I know. Because I just didn't - I had hope. I wanted to think - and, I mean, you know, we know how to do really good special effects. Although, Leo, when you're slingshotting around a star, why are you subject to sudden jolts that is causing the lighting panels above you to fall loose and swing from their wires?

Leo: The science wasn't exactly well thought out in this, I don't think.

Steve: It's really, really, really, really, really, really...

Leo: It's kind of - I don't understand how it got produced. I really don't.

Steve: I don't. I agree. Somebody spent some money on this thing. Anyway, it's, yeah, it's really bad.

Leo: So bad.

Steve: So I have two pieces of better news.

Leo: Okay.

Steve: The first is, also released Friday, "The Great Hack." It's a just-released Netflix original documentary, primarily about Cambridge Analytica and, somewhat secondarily,

about its role in the 2016 U.S. Presidential Election. It is not very technical. It's got some beautiful graphics. It's predominantly kind of a human interest piece, and it obtains a look inside Cambridge Analytica and several related organizations through the eyes of a young woman who got swept up a bit in the power and, as a consequence, was very much on the inside. I mean, she was there and later saw what this thing had become.

The sense I got was that we have her story because she's still the only one talking. The main guy, whose name I forgot, isn't talking. There's doubtless more to be told, and presumably more will come out over time. But it was a two-hour documentary. Anyone watching it, I think - Lorrie and I really enjoyed it - will very much come away with a deeper appreciation of the truly influential power that big data mining and its use to drive targeted advertising has over us. So it was compelling from that sense. And I thought it was a worthwhile two hours on Netflix.

You know, when you think about it, in today's world we are direct eyewitnesses to only a tiny portion of all that we believe that we know to be an accurate depiction of reality. Everything else we receive is relayed through a channel that has some purpose for doing so. Anyway, it's called "The Great Hack," available since last Friday. And so I would, if you think you would be interested in learning more...

Leo: I will watch that, yeah.

Steve: ...about the effect of big data, yeah. And I'll ask you what you thought of it next week, Leo, because I think it was worthwhile.

Leo: We did have Alexander Nix, who was the initial whistleblower for that, on Tech News Weekly this past week.

Steve: Oh, cool.

Leo: Or I think it was Tech News Weekly. So worth watching that, as well.

Steve: And for those who like Tarantino.

Leo: Christopher Wylie, that's his name.

Steve: Ah, Christopher Wylie. For those who like Quentin Tarantino's work - are you a Tarantino fan, Leo?

Leo: Love him. Love him. And I'm dying to see this new movie. Did you like it?

Steve: It's fantastic.

Leo: Oh, I can't wait.

Steve: In fact, my biggest problem was that Lorrie and I were, I guess, screaming out loud, laughing. I was so self-conscious of the rest of the - the fact that we weren't alone in the theater. I was trying to mute myself, but it was - okay. So first of all, I read a whole bunch of the reviews on IMDB. It's at nine point plus. It's north of nine. So, I mean, it is - they're all tens. There were a couple people who gave it a seven or a six. And I have to say, as I was watching it, DiCaprio and Brad Pitt are two major names, although Michael Madsen is there, Bruce Dern is there. Again, anybody who, you know, Quentin says, "Hey, would you want to be in my new movie," they're going to say yeah, you know, yeah, please.

So it was - I want to say it was plotless. And it was almost plotless. And about maybe two hours in - it was two hours and 45 minutes. So it's a long - it's one of Quentin's typical long movies. It was enjoyable. Great performances. But you're just sort of - I remember thinking, well, maybe I'm going to be kind of disappointed by this. Maybe, like, this is going to be like a movie about nothing, where it was nice, but nothing really happened. Leo, it's all a setup. It is all just Quentin playing with us for almost probably two and a half hours, until the whole thing comes crashing into a crescendo that is just unbelievably wonderful. So, I mean, I will...

Leo: Good. I will go see it.

Steve: ...absolutely see it again. And, I mean, I can't quite sit through the entire two hours and 45 minutes just to experience the [crosstalk]...

Leo: A long setup. That is a long setup.

Steve: It was a long setup, but OMG.

Leo: I can't wait.

Steve: Oh, my god, it was fun. And I completely get it that some people are like, who want a plot, people who want [crosstalk] movies...

Leo: I like this kind of movie. I like this kind of movie, the Hollywood insider movie. I like "The Player," and I like that kind of movie.

Steve: Yes.

Leo: Yeah, yeah.

Steve: Yes. It is absolutely that. And DiCaprio does some of his best acting of his career. Brad Pitt is fabulous. It's just, I mean, it just is, it was a great piece of work.

Leo: I'm surprised, though. You did not have the one story of the week I really thought you would be talking about. "The Expanse" is coming back for Season 4. And I know you love this show.

Steve: I am glad, yes. I read the books.

Leo: And they could go on for years, really, couldn't they.

Steve: It was a fabulously rendered series. I mean, that was it. I've talked about "The Expanse" on the show. It had some of the best realistic combat I have ever seen put on film.

Leo: Yeah, yeah. Well, they're bringing it back.

Steve: Yeah, I'm going to have to get Lorrie to sit through it. It was a little, I mean, there was a lot of, like, the Belter-Mars politics...

Leo: Oh, at the beginning, the first episode there's a lot to get into, yeah.

Steve: Yeah.

Leo: I've actually watched the first episode four times and not got past it. So I will now. And how many "Expanse" books are there? There are quite a few; right?

Steve: Yeah. They kept going. So there were, I think, three in the original, and then there was a fourth, and maybe a fifth. So, but, yeah.

Leo: There's a lot of material.

Steve: Yeah. Really, really hard, hard sci-fi. It is a little, I mean, it's a little challenging because time is spent with the politics of Earth, Mars, and the Belt, and the fact that they have different needs that drive different politics. And that creates tension. But, boy, it was good.

Leo: Yeah, yeah. There's nine total. I guess eight of them have been published. So there's...

Steve: Wow.

Leo: There'll be many, many years if Amazon Prime wants to continue producing the show.

Steve: And if they continue it, if they maintain the production quality, then it would be worth...

Leo: You've got all the CGI templates, you might as well; right?

Steve: Yeah.

Leo: All the work's been done.

Steve: Okay. So the news that has taken the industry's breath away is that, as I said at the top of the show, the number one most used embedded operating system on the planet, which is closed and has never been scrutinized, was painstakingly reverse engineered. We were just recently talking in the context of the idea of China rolling their own Internet operating system, how ridiculously improbable that really is. And remember I used the example of the huge amount of trouble our entire industry had just getting the TCP/IP stacks in our operating systems running solidly and correctly due to the extreme complexity and all edge cases of the evolving TCP/IP spec over time. So that's where the problems are.

The entire industry has now been bitten by a set of 11 vulnerabilities, six of them critical remote code execution vulnerabilities, found to affect VxWorks' TCP/IP stack. That's where the problems are. Which has been quietly embedded into more than two billion devices.

Leo: Whoa. Wow.

Steve: Billion with a "b." Two billion. And Leo, if you jump ahead and scroll through the show notes, I couldn't resist listing them by class. I'll get to that in a second. But okay. Since VxWorks is not a common household name, we need to step back for a moment to understand what VxWorks is and why it matters.

I've talked about so-called "embedded operating systems" in the past. A microwave oven will have an embedded operating system. The good news is it probably won't have an Internet connection. All modern automobiles have at least one, and probably several. The Amazon Kindle is based upon an embedded Linux kernel that's been stripped down for embedding. All of our consumer NAT routers have one, as will commercial firewall devices. Certainly all modern printers are written on top of an embedded OS. And somewhat more worrisomely, virtually all sophisticated IoT devices, you know, Internet of Things, the "I" is the Internet, which means connectivity.

Leo: Wait a minute. Even Grandma is running, even Grandma is running on this.

Steve: I know, I saw that. That was a kick. So IoT devices will have an embedded OS at their heart. The number one most popular, most widely used OS with a 20, sorry, with a 32-year history is Wind River Systems' VxWorks. Wikipedia has the following to say about VxWorks. They say: "VxWorks is a real-time operating system (RTOS) developed as proprietary software by Wind River Systems, a wholly owned subsidiary of TPG Capital. First released in '87, VxWorks is designed for use in embedded systems requiring real-time, deterministic performance and, in many cases, safety and security certification, for industries such as aerospace and defense, medical devices, industrial equipment, robotics, energy, transportation, network infrastructure, automotive, and consumer electronics."

They say: "VxWorks supports Intel architecture, PowerPC architecture, and ARM. The RTOS can be used in multicore asymmetric multiprocessing, symmetric multiprocessing, and mixed modes and multi-OS, for example, Type 1 hypervisor designs, on 32- and 64-bit processors." So it's very capable. "VxWorks comes with the kernel, middleware, board support packages, Wind River Workbench development suite, and complementary third-party software and hardware technologies. In its latest release, VxWorks 7, the RTOS has been re-engineered for modularity and upgradeability so the OS kernel is separate from middleware, applications, and other packages. Scalability, security, safety, connectivity, and graphics have been improved to address Internet of Things (IoT) needs."

So then, under Notable Uses, Wikipedia enumerates a few, which is worth sharing to get a better sense for the popularity and broad sweep of this OS. Yes, VxWorks will be in the Mars 2020 rover scheduled for launch next year. It is currently in the Mars Reconnaissance Orbiter. It's in the Mars Science Laboratory, also known as the Curiosity rover. It's in also the rovers Spirit, Opportunity, and Sojourner. It's in the Deep Space Program Science Experiment, the Phoenix Mars lander, the Deep Impact space probe, the Mars Pathfinder mission, the SpaceX Dragon, and NASA's Juno space probe sent to Jupiter. In other words, it's what NASA uses, and JPL uses, as the core OS for all their stuff.

Fortunately, those things don't have IP addresses, so we're probably okay. Although we did actually recently hear about an exploit that was getting into the communications link to something going on with NASA. I forgot what it was. I talked about it just recently. So that may be a concern. We also have it in the AgustaWestland Project Zero aircraft, whatever that is. Northrop Grumman's X-47B Unmanned Combat Air System uses VxWorks, as does the Airbus A400M Airlifter. BAE Systems Tornado Advanced Radar Display Information System, that's TARDIS, used in the Tornado GR4 aircraft for the U.K.'s Royal Air Force, and Lockheed Martin's RQ-170 Sentinel UAV. So it's also in drones.

And this list goes on and on and on. Toshiba uses it in automotive for their image recognition advanced driver assistance systems. Bosch Motor has it in their race car telemetry. Hyundai Mobis's IVI system. It's inside BMW's iDrive system since 2008. Siemens uses it in their automotive navigation system. Renault trucks. The Volkswagen RNS 510 navigation systems. It is the OS in the Apple Airport Extreme. The Drobo uses it. I really thought Drobo was Linux-based, but apparently it's VxWorks. Even the cute Honda Asimo robot is VxWorks based. It's also in Linksys's WRT54G wireless router, unless you apparently reflash it with the Linux-based firmware. I mean, ReplayTV uses it as its embedded OS in their DVR.

And, I mean, there's industrial robotics, test and measurement, transportation, all kinds of SCADA controllers, external RAID controllers. As you said, GrandMA full-scale - GrandMA is Grand M-A, full-size and light console by MA Lighting, whatever that is. Medical systems, Varian, and on and on and on and on. And then, unfortunately, the longest list is networking and communications infrastructure, which are probably on the Internet. Certainly, and there were some notable ones, Cisco's CSS platform and their ONS platforms. Dell PowerConnect switches are VxWorks based, as are SonicWall firewalls. And that may be the most obvious, biggest problem because there's lots of SonicWall firewalls deployed in enterprise environments all over the Internet.

And unfortunately this problem, this is an exploit in the IP networking for VxWorks that these devices are going to have. So it's almost easier to ask what doesn't use VxWorks. And probably in the embedded world, the only thing that doesn't are things that do use embedded versions of Linux, you know, stripped-down Linux for their applications. So today, or actually yesterday, after a 32-year, relatively blemish-free track record, we now have 11 very serious vulnerabilities, six of which are remote code execution capable, that we know of in VxWorks.

Armis, Inc. found and responsibly reported and disclosed these findings to VxWorks, which has of course fixed them all and released patches. The problem is, well, okay. We can't patch - maybe NASA could patch the Mars rover if it were concerned about it, but they probably aren't. But unfortunately, many of these devices are hooked up to the Internet. And those that are in IoT may not be firmware rewriteable. They just may be fixed. So they could be in trouble.

Armis explains what they found. Urgent/11, as they called it, is a set of 11 vulnerabilities found to affect VxWorks' TCP/IP stack, which is a module which you can include in VxWorks known as IPnet, that is, the IP networking module. It's used by versions, many versions of VxWorks. Six of the vulnerabilities, six of the 11, are classified as critical and enable remote code execution. The remaining vulnerabilities are classified as denial of service, information leaks, or logical flaws. As each vulnerability affects a different part of the network stack, it impacts a different set of VxWorks versions.

However, as a group, Urgent/11 affects the VxWorks versions described with at least one remote code execution vulnerability for each version. A wide range of affected versions spanning over the last 13 years, they write, is a rare occurrence in the cyber arena and is the result of VxWorks' relative obscurity in the research community. This time span might be even longer, as according to Wind River three of the vulnerabilities were already existent in IPnet when it acquired the stack from Interpeak back in 2006.

Urgent/11 are the most severe vulnerabilities found in VxWorks to date, which, they write, has suffered from only 13 public CVEs in its entire 32-year history. Urgent/11 is a unique group of vulnerabilities that allow hackers to circumvent NAT and firewalls. And this is important. These pass through NAT and firewalls and, they write, take control of devices remotely via the TCP/IP stack undetected, with no user interaction required. This is due to the vulnerabilities' low-level position inside the TCP/IP stack, which enables attacks to be viewed as legitimate network activity.

Such vulnerabilities do not require any adaptations for the various devices using the network stack, making them exceptionally easy to spread. In most operating systems, such fundamental vulnerabilities in the crucial networking stacks have become extinct after years of scrutiny unraveled and mitigated such flaws, just as I've been saying of our public OS stacks.

They said: "Urgent/11 is comprised of 11 vulnerabilities, separated into two classes of severity. There are six critical vulnerabilities allowing remote code execution, and five vulnerabilities leading to denial of service." So to give our listeners a sense for what these are, there's a stack overflow in the parsing of the IPv4 options. They said: "This vulnerability can be triggered by a specially crafted IP packet sent to the target device, even as a broadcast or multicast packet. It does not require any specific application or configuration to be running on the device," again, because it hits too low, down in the low level stack. They said: "...and it affects any device running VxWorks v6.9.4 or above with a network connection." And that's, because VxWorks evolves very slowly, this is very widespread the past 13 years.

"The vulnerability causes a stack overflow in the handling of IP options in the IPv4 header, making it easy to reach remote code execution through it." They said: "There are four memory corruption vulnerabilities stemming from erroneous handling of TCP's Urgent Pointer field. The four vulnerabilities all stem from erroneous handling of TCP/IP's Urgent Pointer. The Urgent Pointer is an esoteric TCP field that is rarely used in modern applications. An attacker can trigger the erroneous handling of this field by either directly connecting to an open TCP port on the target device, or by hijacking an outbound TCP connection originating from the target device.

"Once triggered, these vulnerabilities will cause the application on the target device to receive more bytes than expected from the system's receive function, leading to a memory corruption of either the stack, the heap, or a global data section, depending on which buffer was passed to the receive function. This means an attacker can probe the various TCP connections of the target device and attack the application that is the easiest to exploit."

And then they go on through additional details, breaking down each of these four different Urgent Pointer attacks. Then they also discuss a heap buffer overflow in this. And the disclosure goes on. They have complete details, and the fact of this was made public yesterday because VxWorks fixed this a month ago, and they will be detailing this in greater depth during their Black Hat presentation next week on August 8th in Las Vegas.

Trying to sound like this wasn't really their fault, a Wind River spokesperson told ZDNet: "These vulnerabilities are not unique to Wind River software. The IPnet stack was acquired by Wind River through its acquisition of Interpeak in 2006. Prior to the acquisition, the stack was broadly licensed to and deployed by a number of other RTOS vendors." Uh-huh. So if you have a SonicWall, Dell PowerConnect switches, a Linksys WRT54G wireless router v5 or later, or a Drobo exposed to the Internet, you really need to pay attention. Make absolutely sure that you have patches, not only current, but that they are within the last month or so, so that you know that the patch vendor will have received the RTOS update from their source and will have updated because this is bad.

The technical press expects essentially that this problem is going to be with us, that is, VxWorks-related problems, hacks, and exploits are probably going to be with us, essentially forever. It will be until the vulnerable devices are retired. We know that some of them are going to get updated. But, you know, look at Windows that has a fully mature patching system in place, where you have to just not prevent it from updating, and it does. And even there, months after fixes are available, they're not fixed. Well, we know that light bulbs that have embedded OSes in them, and our household thermostats, who knows, you know, what's in the higher end IoT devices is very likely a copy of VxWorks is the embedded OS in these things.

So anyway, this is, I mean, unfortunately on a per-device basis there's nothing end users can do except follow the advice of keeping your stuff patched. And I know that, once this podcast is done, I've got a bunch of stuff I'm going to be checking up on.

Leo: Wow.

Steve: Wow. Two billion devices. And really, you know, the takeaway moral of this is that the reason this happened is they were using an unaudited networking software for 13 years.

Leo: Yeah.

Steve: Yes, this guy says, "Hey, it's not our fault. We bought this from somebody else." Uh-huh, 13 years ago in '06 you bought it. And you never let anybody see the source. You kept it closed. And as a consequence, this happened.

Leo: Yup. Well, let's hope the people fix it and that the Mars rover isn't hacked. Although that'd be an epic hack.

Steve: Oh. Yup.

Leo: We do this show every Tuesday about 1:30 Pacific, 4:30 Eastern, 20:30 UTC. It's a fun one to tune in and listen to live, if you can, at TWiT.tv/live. On the other hand, if you wait until the transcript comes out and download the audio, you can read along, and that might make it a little more comprehensible. Sometimes you need those aids to understand everything that goes on in this show. This was a pretty straightforward show, I think. You'll find all of those at Steve's site, GRC.com, the Gibson Research Corporation, GRC.com.

He also has, of course, SpinRite, the world's best hard drive maintenance and recovery utility, available for purchase there. Lots of other stuff, all of it free, including the latest about SQRL, and his Perfect Paper Passwords. ShieldsUP!, I think the single most-used network utility in the history of mankind. It's got to be up there, anyway. All of that at GRC.com. Steve's on the Twitter at @SGgrc. You can DM him there if you've got a question, or go to GRC.com/feedback.

We also have audio and video of the show, if for some reason you want to watch it, at our website, TWiT.tv/sn for Security Now!. You could subscribe, too, in your favorite podcast application. Every single one will have Security Now!. And if you subscribe, the advantage of that is you'll get it automatically. Even if you forget, oh, it's Tuesday, it'll automatically appear on your phone or device. And that way you can listen on Wednesday. Steve, thank you. And we'll see you next time on Security Now!.

Steve: Thanks, buddy. Bye.