The MV720

Description: This week we start off by updating our follow-up to this month's Patch Tuesday. Things were more interesting than they originally seemed. Then we keep up with the evolving state of Microsoft Office's VBA macro foreign document execution. We also have a fabulous bit of news about some default security policy changes for Windows 11 announced by Microsoft. Then, with August rapidly approaching, we have a few calendar notes to mention; I have a welcome and long-awaited bit of SpinRite news to share; we have a bit of miscellany and some brief bits of listener feedback to cover. Then we take a deep dive into the poor-by-design security of a very popular and frightening widely used aftermarket GPS tracking device. You don't want one of these anywhere near you or your enterprise. Yet 1.5 million are.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-881.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-881-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here with an update on the update on last week's Microsoft Patch Tuesday. Maybe not as good as we thought, including the weirdest printer solution and problem you've ever heard of. We'll then talk about the on and off again VBA macro solution from Microsoft. This time Microsoft says no, no, this is definite. And finally, he calls it the Demon Box, a GPS tracker that is so woefully insecure that if you have it on your car, and you may not even know, you must remove it immediately. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 881, recorded Tuesday, July 26th, 2022: The MV720.

It's time for Security Now!, the show where we protect you, your loved ones, your privacy online with this guy right here, Steve Gibson. And by the way, Steve, at least half a dozen people came up to me and said - because I had mentioned when I was going on the cruise two weeks ago, oh, everybody's going to say hi to Steve. They came up and said, "Tell Steve we said hi." So everybody...

Steve Gibson: Mission accomplished.

Leo: Mission accomplished. I said we begged Steve to go on it. Maybe next time Steve will go. If you...

Steve: Well, and now we know why we didn't.

Leo: You were smart. You were smart. Because, yes, Lisa and I did contract COVID, and a couple of other of the TWiT group did that I know of. But most of them emerged unscathed, had a great time. Thank you all for joining us. We really appreciate it. And I promise I am going to strong-arm Mr. Gibson. Maybe when COVID's over we could do it; okay? Or you pick the trip you want. You want to go to Ireland? Whatever you want to do.

Steve: Sounds good.

Leo: All right. What's going on in the world, Steve?

Steve: Well, this is Security Now! 881, our final episode for July. We're going to start off by updating, actually updating our follow-up to this month's Patch Tuesday, which we did last week. Thank you, Jason, for filling in for Leo.

Leo: Yes, thank you, Jason.

Steve: Things turned out to be more interesting than they seemed at the time. Then we keep up with the evolving state of Microsoft Office's VBA macro foreign document...

Leo: Wait a minute, there's more?

Steve: Oh, my god. And we've got drama now also.

Leo: Oh, boy.

Steve: So we're going to add that. We also have a fabulous bit of news about some default security policy changes for Windows 11, announced by Microsoft. And we also see that those are not easy for them to make. Then, with August rapidly approaching, we've got a few calendar notes to mention. I have a welcome and long-awaited bit of SpinRite news to share. We have a bit of miscellany and some brief bits of listener feedback to cover. Then we're going to take a deep dive into - and this is why the podcast's title is "The MV720." It's a poor-by-design security of a very popular and frighteningly widely used aftermarket GPS tracking device. Yes, $26 from Amazon.

Leo: Ooh, wow.

Steve: You don't want one of these little puppies.

Leo: Oh, okay.

Steve: Anywhere near you or your enterprise, yet 1.5 million of this particular model are out there. And you're not going to believe, like just the lack of care. And it's another perfect example of the weird place we're in now where such high-end technology is

available so inexpensively that there's almost no budget for security, or no apparent concern whatsoever. And people are buying these things because, hey, 26 bucks, I want one, click. And then, you know, it phones home to China and everybody else. So anyway. Oh, and Leo, we've got - this is one of the best Pictures of the Week in a long time.

Leo: Cool. I haven't peeked.

Steve: So I think another great podcast.

Leo: I haven't peeked at it.

Steve: You should be on mic when you first see it.

Leo: Oh, good, all right.

Steve: Because it's, you know, so the audience can capture your reaction.

Leo: I will. I have not looked.

Steve: All right.

Leo: I've been very good. I look forward to this, so I like to save it for myself.

Steve: It's one of those that takes some visual parsing. But when it hits you, it hits you hard.

Leo: I love those. I love those because you go [gasp]. I'm going to pull it up right now, and we will look at it together, all of us. All right? It says "Love this. Computer Security Career Paths, Path 1, Path 2." Path 1 is a long one, 20 years: forensic analyst, forensic lab director, chief security official. Or go the hacker, criminal, convict two years, and you can be a high-paid security consultant in 14 months with good behavior. I love it. It's unfortunately kind of true; isn't it.

Steve: That's part of what makes this thing work so well. So it starts off with a computer security expert, and you have two choices of path you want to take.

Leo: A fork in the road, yes.

Steve: You can become the forensic analyst and then get promoted to be a forensic lab director, eventually get to be the chief security official, and then become finally, after 20 years, the highly paid security consultant. That's the traditional path. Or you can, knowing your way around computers...

Leo: It's the shortcut, yeah.

Steve: You start, you do some hacking.

Leo: You get caught.

Steve: You get caught, yeah, you get caught, and you're a criminal. So you get convicted. And it shows two years later, or 14 months with good behavior, you're out, and now you're a highly paid security consultant taking the shortcut route. Now, it has been noted that you will end up with a felony on your record, which may...

Leo: Yeah.

Steve: On the other hand, you might just, you know, depending upon who's hiring you, they might just figure, hey, that's just, you know, that's the way we saved 18 years in hiring this kid. That's the price of entry.

Leo: I love it.

Steve: Okay. So last week, which was the week following July's Patch Tuesday, I congratulated Microsoft for their having patched some 84 known flaws without simultaneously crippling Windows. But since then it has come to light that I may have been somewhat premature in my praise. Published under "Issue details for July 2022" is the topic - this is Microsoft's publication - "Printing to USB-connected printers might fail," with the status of "Confirmed" in their little table. So the affected, or I should say afflicted, platforms include both client versions of Windows 10 - this is Windows 10 only - 20H2, 21H1, and 21H2, and the server version 20H2.

Microsoft explains: "Microsoft has received reports of issues affecting some printing devices following installation of Windows updates released June 28th and later. Symptoms observed may include: Windows might show duplicate copies of printers installed on a device, commonly with a similar name and the suffix 'Copy1.' Applications that refer to the printer by a specific name cannot print. Normal printer usage might be interrupted for either scenario, resulting in a failure of printing operations."

Okay. So as we know, Windows printing, like Windows LAN Manager networking, has pretty much always been a mess. As we know, last year's Windows Printer Spooling security debacle dogged Microsoft for more than half a year. Some of Windows' architecture has not aged well through the decades. And it's understandably difficult to ever make that decision to scrap something that mostly works, in favor of a major redesign which, while fixing the problem, the underlying problems, is certain also to break a large number of things that are currently working, especially when there's so much hidden dependency upon the existing system just being left the way it is.

So it really is the case that at this point Microsoft can barely change anything without breaking everything. I think that probably when a future history is written of this era of Microsoft and Windows, it will show that they painted themselves into a corner from which there was no escape. And while it's easy for us to say, oh, look, they broke it again, because of the way how creaky it's all become, it's like, yeah, but when were they supposed to stop and, like, break it badly in order to fix it? Actually, it's what I did with

SpinRite; right? I said, okay, no more. Anyway, we'll talk about that later. But it could not be any more clear that Windows is at this point not actually getting any better; right? I mean, like nobody wants any of what they're doing because it's not better. It's now clearly getting worse. Anyway, but that doesn't work with or isn't aligned with, I guess you we should say, with Microsoft's need to appear to always be moving forward, even though no one wants them to.

Anyway, if by some chance your printing to USB stopped working earlier this month, and you have not yet decided to tackle that problem, hoping maybe that August's patches would bring it back to life again, the trouble appears to surround the spontaneous creation of a duplicate printer instance where it, the duplicate, somehow obtains the proper configuration while upsetting the configuration of the original instance. They have like this section of workarounds.

Microsoft says: "Open the Settings app, navigate to Bluetooth and Devices, and select Printers and Scanners." They said, "If there appears to be a duplicate installation of an existing printer, such as with suffix 'Copy1,' confirm if printing works for this printer." They said: "This printer should operate as expected. If there's a need to use the original printer installation and not the duplicate" - the one which now works - "right-click the duplicate printer, select Printer Properties, and select the Ports tab. Observe the port in use. Now open Printer Properties on the original printer. Select the Ports tab. From the list displayed, select the port option in use by the duplicate printer." Can you believe this, Leo?

Leo: Observe the port in use.

Steve: Yeah. So, okay. So apparently, reading between the lines of this workaround, it sounds as though whatever it was Microsoft was attempting to so intended to create a new instance of a USB printer, copy the original instance's settings into the new instance, then presumably remove the original instance, and give the new instance the name of the original.

Leo: Why?

Steve: I know. Because Windows. So it sounds like for some users...

Leo: Such a kludge.

Steve: It's a disaster.

Leo: Oh, my god.

Steve: And this is what Microsoft is saying. If you really to print - like, oh. You want to print in Windows? Well, here's how.

Leo: Oh, my god.

Steve: So it sounds like the process got part of the way along and then died. And it did not back itself out and revert to the original configuration, which was working before all of this began. Right? Like everything was fine. USB printers were going. And then you got a Copy1 which works. The original one stopped working. And they said if your application addresses printers by name, like oh, okay. Well, the name it has broke. Like we broke it. So...

Leo: So copy the name to a new printer.

Steve: Oh.

Leo: Oh, my god. This is why I do not answer printer questions on the radio show. Right there in a nutshell.

Steve: Right. In fact, Lorrie, I think it was early last week, she said, "Nothing's printing."

Leo: Oh.

Steve: And I said, oh. Because, I mean, and I had - I was right in the middle of like this really cool work on SpinRite. And I just - or maybe it was after dinner, and I was ready to go back to it.

Leo: Oh, it's the worst, yeah.

Steve: I had my evening planned. Well, there went my evening.

Leo: There goes your evening. You're a good husband. You're a good husband.

Steve: And she said, "Honey," like when it was all working again, she said, "How can anybody else do what you just did?" And I said, well, you open the printer dialog.

Leo: Observe it working.

Steve: And you observe the working printer.

Leo: Oh, that's, in a nutshell, that's exactly what Lisa says. It's what everybody I know says. Probably what everybody who knows the people who listen to this show say, which is how does anybody use this crap? Unless you've got somebody, an expert, a local expert.

Steve: There are people who go buy a new one, Leo.

Leo: Yeah. Most people.

Steve: They just go, okay.

Leo: Most people.

Steve: Yeah. It's like, well, you know, things began falling off, and finally I just decided to go to Best Buy. You know? Just, you know, they're not that expensive anymore. I got one that's smaller and lighter and faster.

Leo: Of course, and it's exacerbated by terrible printer drivers, I mean, multiple versions of Windows that don't...

Steve: Oh, Leo, yes. In fact, I was going to talk about that. I went to HP's site just to remind myself how many hundreds of megabytes.

Leo: Yes, yes.

Steve: It's a quarter gig of printer driver.

Leo: Yes, and you'd better get the right one because you - oh, god, it's a mess.

Steve: Yeah. And the time before this last time when Lorrie needed me to fix her printer, I realized...

Leo: You mean you've done this more than once?

Steve: Oh, yeah. We got about six months out of the last round. So that's pretty good. So I realized you just need like ungodly patience. It's like something is spinning, and just leave it alone.

Leo: Don't touch it.

Steve: I'm so tempted to think, oh, it hung, or it's not going anywhere. It's been 15 minutes. No. It needs hours. And I don't know why. But I just, I like, finally I just said, I just gritted my teeth, and I go, I'm just going to wait. I'm going to just wait. And then like after a couple hours, something changed. It was like, oh. Look. And then when I just let it really take - and this is - we're running on a state-of-the-art NUC with like NVMe memory. This stuff is fast. Hers is the fastest machine in the house because of course I work on stuff you have to wind.

Leo: No. Lisa has the fastest machine in the house, too. That's, again, we're good husbands. We're good husbands, yes. That's all I can say.

Steve: Oh, lord. Anyway, this is, yeah, this is Windows. And yeah, it is.

Leo: It's life. It's life as a tech guy. This morning before I came to work I spent an hour and a half trying to get the Sonos stuff to talk to each other. And literally the last thing I did before I came in to work was order a Vizio sound bar and say screw it. No more Sonos. All right.

Steve: Yeah, yeah. And I've told the story about my wonderful realtor friend Judy, who went from what she called her "modem," which was actually a TI Silent 700. She was a realtor, and so she would dial the phone and then take that olive green handset and stick it into the acoustic coupler cups on top of the thermal printer, and then she would like...

Leo: Get the listings, yeah.

Steve: Yeah, get her scroll-y, that stinky thermal paper...

Leo: It curls up, yeah.

Steve: ...roll that curls up, yeah. And she would take that off and to a client. Anyway, so we moved her, I was there when we moved her to Windows. And, oh, it was just - she called, she didn't realize that the Internet was not Google, so she thought it was the same. And she used to say to me, like when I would right-click, I'd say, oh, no, Judy, you've got to right-click. What? I said, you see how your mouse has two little ears up there, a left and a right ear? You push the right one in order to get that little menu.

Leo: So, what, those are called ears?

Steve: Well, I had to help her along. Because if I said button, she'd say, nope, there's no button.

Leo: There's no button. No, no.

Steve: Oh, and that used to happen, too, oh, with her husband Jan. I'd say, Jan - because I'd give up talking to Judy. I said, "Judy, put Jan on the phone." And I'd say, "Okay, now, do you see that button?" And he'd go, "What?" And finally I realized we were both looking at the same thing, but he saw a rectangle with a shadow, and I was calling it a button.

Leo: Yeah, that's right, a button.

Steve: And he said - I said, "No, okay, Jan, it's that rectangle where - see how it's shadowed to kind of look like it's 3D."

Leo: Kinda looks like a button.

Steve: Oh. "And what should I do with that?"

Leo: We have all been there.

Steve: Oh, boy.

Leo: We have - everyone who's listening is immediately identifying with this, when you start to describe stuff. It's just hysterical.

Steve: Yeah.

Leo: There's an old video, John Mayer, the folk singer, talking to his dad outside a concert. And he's on the street talking to his dad, and he's going, "No, Dad, the start, the start button. It's in the lower left." And when you see that, you go, yup. It's universal.

Steve: Well, and I remember saying to someone, I don't remember now who, but when I was trying to describe something by voice over the phone, I finally said, okay. Here's the problem. We do not share a vocabulary. Like I cannot describe to you what has to happen here.

Leo: Oh, it's not just a vocabulary. It's a worldview.

Steve: Because I have to use terms...

Leo: No, no, it's an entire different vision of the world and how it works. It's we're in different planets. I think there might even be a gene. There's something. It's just - and I'm not making a value judgment. It's not good or bad.

Steve: No, no.

Leo: But it's different, maybe it's different dimensions of, you know.

Steve: Well, and Judy finally asked me, she said, "How..."

Leo: How is a very big question.

Steve: "...will people ever get this?" And I said, "No, Judy. You will die. I mean, it's like the dinosaurs. They're gone. You will die. Your inability to navigate with a mouse will go with you."

Leo: And everybody will know.

Steve: The world will be full of people who do. They've always had mice.

Leo: Who knew, though? Who knew? The mouse is now going away. It's all touch, baby.

Steve: Yeah.

Leo: That's probably why. Nobody could figure them out.

Steve: I've actually made the mistake, after using a machine with touch for a while, you start touching the screen of things that don't.

Leo: Touch the screen. Nothing happens. Yeah.

Steve: And it's like you get a weird little ripple that kind of moves away from where you touch because you disturb the liquid crystal underneath. But it's like, okay.

Leo: We have a - Evanescence Photo has provided us with new album art. Steve, I think you'll enjoy it. Disaster Now!, ladies and gentlemen. That's the name of the show. Disaster Now!.

Steve: Oh, that's a...

Leo: New album art. All right. I'll stop interrupting. Go ahead.

Steve: Okay. So the continuing saga of Windows VBA macros. As yet another example of one of Microsoft's very poor early design decisions not aging well, and their refusal for many years not to simply do the right thing, we have the continuing saga and drama of Windows VBA macros. Last Wednesday night...

Leo: Okay. Now wait a minute. Now, when I left, this was all resolved.

Steve: No.

Leo: No. Okay.

Steve: No.

Leo: All right.

Steve: Last Wednesday night they confirmed, Microsoft confirmed that it was resuming the rollout of their plan which they first announced earlier this year, back in February, which is when we threw the party. But then that announcement back then was greeted with great relief by everyone who understood what it would mean for the security of Microsoft's much-abused Office documents. After years of head-in-the-sand policy, Microsoft would finally be blocking the execution of remotely received VBA macros by default across most Office apps.

Predictably, this would break some things. Which of course explains Microsoft's reticence to do the right thing sooner. We've never really talked about the pushback against this change, but I came across some interesting bits which address that. Even though Microsoft declined to provide information about why the effort had been paused, several experts said customers complained about this new, well, this change. It's not really a new feature. It's a change.

Michael Tal, the technical director for Votiro, which is a company specializing in malicious content filtering in the cloud, he told The Record that he works closely with partners in the banking and financial sectors and explained that macros play "an integral part of our clients' business workflows." He said that the initial block caused a "massive hindrance on business productivity." Basically, the recession that we're heading into was caused by Microsoft's decision - no. Okay. What happened was that something changed. Just as Microsoft warned everyone it was going to back in February, when they said to get prepared. They told everybody in February we're going to do this, so everybody should, like, do what you need to because macros are going to stop running by default the way they have been. Well, guess what? It turns out Microsoft wasn't kidding.

Michael Tal explained, he said: "Macros are a powerful tool in the financial sector, as they are used to create robust financial modeling, calculate loan interest, automate repetitive, labor-intensive tasks. They're recorded sets of actions which can be run to save time and labor. It's also used to simplify budget forecasting and makes a difference in a day-to-day workload of any entity who's using it as it speeds up the process to generate a task after finalizing the creation of the macro and setting the variables." Yeah. Right. And you're going to have to now press a button to make that happen rather than not.

Anyway, he added that while he understood Microsoft's desire to combat malware like Emotet, Trickbot, Qbot, and Dridex, they should have come up with a more creative approach - so he's complaining, right, about increased security - a more creative approach to deal with legitimate business use cases for macros and allow for continuity without compromising security.

Okay. So it's not as if macros have been stripped out of Office tools and are gone.

Leo: No. No, no, no. Just a property now.

Steve: Yes. They simply no longer run without provocation. You just need to click a button to explicitly permit their use. And, you know, as we've seen, you showed two weeks ago, Leo, that flowchart. I have it in the show notes here again. We've seen that crazy flowchart that enterprise-wide group policy settings can be made to cause it to, like, no behavior change. Decision box 4a in the flowchart is "Cloud policy to block?" You set it to "no." Then decision box 4b gets control, which is titled "ADMX or Group policy to block?" That could be used to enable macros at that point so behavior doesn't change.

Leo: It's just really a question whether you want to fail secure or fail insecure. Right?

Steve: Right.

Leo: What the default is.

Steve: Exactly. And so basically everybody's having a conniption because they want the insecurity of allowing unsolicited, unsigned, documents of unknown provenance to be received by email or clicked on on a web page and just have everything work. At the same time, they want Microsoft to somehow magically not allow malware to do the same thing. Well, folks, sorry about that. You know? I mean, all the enterprises would have to do if they wanted that was to sign the document. Signing them is another way of immediately...

Leo: There's all sorts of things, yeah.

Steve: Yes. This is a decision tree where most of the outputs of the tree are macros enabled. There's only one red box that has them blocked by policy. And Microsoft added one at the end. If you get through step after step after step after step after step, there are five steps, and you still haven't reached a decision, it used to just be okay, fine, let's go. Now it's okay, wait a minute. Let's make sure this is what you want. Are you absolutely sure? And that was too much to ask.

Leo: So often security takes a back seat to the stupidest user. Right? And unfortunately...

Steve: Yes, the lowest common denominator.

Leo: ...that's the guy in the corner office. And because he signs the checks, he's the guy who gets to say to the IT guys, "I like this behavior, Simmons."

Steve: You know? So how can any moron think that it's a good idea to allow macros to run unbidden in a document received through email?

Leo: Well, you have to press the Allow button. Come on, it's not completely unbidden. You have to say its name three times.

Steve: Oh, Leo. Again, it's just, I mean, so I get it that Microsoft doesn't want to offend or upset or ruffle any features. These people should just be ignored. I mean, Microsoft warned the industry, the world, in February, this was coming. It finally happened, and so oh, my god, it's the end of life as we've known it because our macros don't run themselves.

Leo: So what's the current status? Because it's been back and forth and back and forth.

Steve: The current status is, quote, this is what they said: "We're resuming the rollout of this change in Current Channel."

Leo: Good.

Steve: "Based on our review of customer feedback, we've made updates to both our end-user and our IT admin documentation to make clearer what options you have for different scenarios."

Leo: Good. So get off your butts, set the Group Policy if you want it to be different. But we're going to default secure.

Steve: Yes, exactly. If you insist on allowing all the malware, you know, Follina used Office macros in May to infect a whole bunch of people. And if you want to be admissive of all of this malware, by all means. Just set your document policies. Set Group Policy. But the rest of us have decided, okay, it's an inconvenience. We're going to have to actually act a little more securely. Fine.

Leo: Good. I actually think signing the macros is a great idea.

Steve: Yes. That's a win. Just somebody is building these documents and has all this financial, tricky financial stuff in it. Just give him a certificate.

Leo: Yeah.

Steve: Have him sign it. And it'll just - it moves like grease through a goose. Not a problem. Speaking of which, let's take a break.

Leo: I have some grease for your goose. I've been waiting for you to ask for it.

Steve: And in another bit of happy news, I mean, I don't want to draw any great conclusions here and suggest that maybe Microsoft is actually finally getting a clue, but Windows 11 now blocks RDP brute force attacks by default.

Leo: Wow.

Steve: Which is astonishing. Last Thursday Microsoft's VP for Enterprise and OS Security, Dave Weston, he tweeted from @windowsinsider, he said: "Windows 11 builds now have a DEFAULT" - and he, I mean, he understands. It's all caps in his tweet - "DEFAULT account lockout policy to mitigate RDP and other brute force password vectors. This technique," he says, "is very commonly used in Human Operated Ransomware and other

attacks." He says: "This control will make brute forcing much harder, which is awesome." Now, everyone listening to this podcast is acutely aware of the importance of default settings. There may as well not even be any settings since the default is almost universally what is left to apply.

"The other thing everyone listening to this podcast knows is that the inherent insecurity created by Microsoft's remote desktop protocol being placed out onto the public Internet without any sort of brute force credential-stuffing protection in place for years has been insane. It's been responsible for untold numbers of remote network intrusion, pain, and loss to Microsoft's users. In fact, the FBI said RDP is responsible for roughly 70 to 80% of all network breaches."

Leo: What? Oh, my god.

Steve: 70 to 80% come through Remote Desktop Protocol.

Leo: That's incredible.

Steve: Because there's no...

Leo: There's no protection.

Steve: They're unmonitored.

Leo: Yeah.

Steve: Right? Yeah. So, David's news was incredibly welcome. But my jubilation was somewhat tempered when I saw the Local Group Policy Editor settings that he was announcing and celebrating. It is true. Windows 11 now has its failed login attempts account lockout triggering after 10 invalid logon attempts. But the lockout duration is only 10 minutes.

Leo: Oh, come on.

Steve: I know. And the failed attempts counter also resets every 10 minutes.

Leo: I guess that could be enough for the random brute force guy. But not for targeted attacks.

Steve: Right. Could someone explain to me how any legitimate user of remote desktop protocol - whose RDP client has probably memorized and stored their logon authentication for them anyway, which makes it automatic for the user, they don't even have to do anything - how any legitimate user is going to be inconvenienced by a lockout which doesn't engage until they have somehow failed to properly authenticate themselves 10 times?

Since, as we've seen, Microsoft clearly goes to great lengths to never inconvenience any user in the name of security, they must believe, as I do, that no one but an attacker would ever trip the "10 strikes before you're out" rule. So why, then, give an attacker a clean slate 10 minutes after those 10 failed attempts? So, okay, I get it. I guess baby steps; right? So let's just hope and pray that the error message returned by the RDP endpoint is the same for a failed logon attempt as for a block by policy.

Just, please, Microsoft, just say your authentication failed. Don't tell them that a policy has been switched on, which is why authentication has been blocked. Because of course that would allow them to probe the endpoint to figure out what the timeout is and what the number of failed attempts counter is and so forth. Just tell them nothing. Let the bad guy believe that every single one of their attempts is still hitting a wall. And so that they're not able then to throttle themselves and slow down.

Anyway, at least now we have the concept in place of default mitigation against brute forcing unmonitored authentication endpoints. That's some progress. And really that's the problem, right, is that almost nobody knows that their security is being pounded on by a credential stuffing attack 24/7. You know, everyone just sort of goes, oh, that's just, you know, Internet noise; right? Well, in fact I coined the term "Internet background radiation," just these packets flying around, just like doing stuff. It's like, yeah, yeah, we just ignore that. It's like, well, except that it's pounding at you, trying to get into your network. And as the FBI said, 70 to 80% of ways in is that. So worth taking note.

As I mentioned at the top of the podcast, this is our final podcast for July as we're going to be heading into August. August traditionally contains a few interesting security events. We have the two traditional major hacking conferences, Black Hat and DEF CON. This year, running from the 6th through the 11th, is the 25th Black Hat USA. It'll be holding, as a consequence of the changes that COVID has wrought, a hybrid conference allowing the cybersecurity community to choose how they wish to participate. The conference's first four days will be virtual trainings conducted in real-time online, with all instructors accessible throughout each class. So virtual online real-time and interactive. Then the final two-day main conference will occur both virtually online and live in-person in Las Vegas at the Mandalay Bay Hotel and Casino.

Then, as always immediately following Black Hat, is DEF CON, August 11th through the 14th. And I had to smile and just sort of shake my head as I was checking in on DEF CON's description of itself and its planned proceedings. Since I think everyone will get a kick out of what they wrote, I'll share what they had to say. They said: "Started in 1992 by the Dark Tangent, DEF CON is the world's longest running and largest underground hacking conference. Hackers, corporate IT professionals, and three-letter government agencies all converge on Las Vegas every summer to absorb cutting-edge hacking research from the most brilliant minds in the world and test their skills in contests of hacking might.

"DEF CON comes right after Black Hat, a conference and trade show for cybersecurity professionals. While Black Hat feels more like a traditional Vegas trade show, DEF CON is anything but. How is it different from other conventions? Well, first, DEF CON is run by volunteers, and it has no corporate sponsorship. Secondly, there is no online registration, so even the organizers really don't know who is attending. When you arrive, everything is paid for with cash. They don't take credit cards. Most of these people attending really don't want a record of them being there. Everyone from your average everyday hacker to criminals and agents from government agencies like the FBI, CIA, and NSA will attend. When you enter, you pay $280 cash, and they hand you a generic badge. No ID is required for admittance." So those two conferences begin...

Leo: But then you may be subject to Spot the Fed. Right? That's part of the game; isn't it?

Steve: Exactly.

Leo: So grow that crew cut out.

Steve: And we are also celebrating Security Now's 17th birthday, Leo.

Leo: Today?

Steve: No.

Leo: Oh.

Steve: On August 19th...

Leo: Oh, good. I have time to bake a cake. Good, okay.

Steve: We have some time. You have time to fully recover. August 19th, the anniversary of the first episode of this podcast. This coming August 19th we'll be finishing out our 17th year, and we begin into year 18.

Leo: Wow.

Steve: So Leo.

Leo: You're an adult.

Steve: It is almost at adulthood.

Leo: You can drink.

Steve: You've almost reached maturity.

Leo: No, you can't drink. But you can join the army and shoot a gun.

Steve: I do like my cabernet.

Leo: I think you have to wait till 21.

Steve: I think so.

Leo: In most states, yes.

Steve: Yes. I remember Mom, after her divorce, was dating someone. And when she was going out she'd set us up with a frozen pizza which she'd quickly bake.

Leo: Of course, yes.

Steve: And glasses of red wine that were 2:1 watered down. I got my start early.

Leo: That'll keep them - that'll get them to sleep.

Steve: And the point is I remember the guy that she was seeing coming over and looking at the kitchen counter, and here were two eight and six year olds...

Leo: With wine glasses.

Steve: ...with red wine. Yeah. We're liking this dinner a lot. Have a nice time.

Leo: Have a good time, Mom.

Steve: That's right.

Leo: My mom didn't do that, but she did give us TV dinners. And I still have a taste for the weird cardboard-flavored corn.

Steve: I do, yes. It was a weird - they were sectioned off.

Leo: Yeah, they were sectioned off. But the flavors combined somehow.

Steve: Yes.

Leo: Everything tasted the same, yeah, yeah.

Steve: The peas sort of had a, what was that...

Leo: Apple pie mixed in with them. And there was the fried chicken.

Steve: Salisbury steak.

Leo: Salisbury steak, oh, the gravy would spill over, yeah.

Steve: Yeah, the gravy and the Salisbury steak, that's right.

Leo: Oh, god.

Steve: And we used the term "steak" very lightly in this context.

Leo: They don't still sell TV - does Swanson still sell TV dinners?

Steve: Why would they have stopped?

Leo: Good guess. I don't know. I don't know.

Steve: Microsoft still has printing problems.

Leo: Yeah.

Steve: So I think Swanson's probably still selling TV dinners.

Last Friday afternoon I posted to the grc.spinrite.dev newsgroup under the subject "It's Alive!" As we know, I essentially had to take SpinRite completely offline and down to perform the degree of surgery that was needed, not only to completely strip out all of SpinRite's traditional dependence upon the BIOS, but to also, as I've explained during this journey, to completely re-architect SpinRite around a data-recovery-centric, device-independent mass storage device abstraction so that not only can SATA and IDE drives connected with AHCI and PCI bus mastering adapters now be communicated with at their lowest possible hardware level, but also so that the next step in SpinRite's evolution, which will add similar direct access for USB and NVMe devices, and whatever else might show up in the future, will be able to support plug-in drivers essentially, without needing, any, again, any similar reworking. I've done all of that work upfront.

I'm mentioning this because I can finally report that SpinRite is beginning to come back to life. Humpty Dumpty is getting its pieces reassembled.

Leo: Woohoo.

Steve: It is starting to run again.

Leo: Yeah.

Steve: It is by no means ready yet. I don't want to give anyone that mis-impression. I still have lots of work left to do because the surgery that SpinRite needed broke virtually every assumption that it was originally built upon, assumptions which were made back in 1987 when we had 4.77 MHz Intel 8088 processors with a maximum of 640 Kbytes of RAM, and a 20MB hard drive was a luxury. Actually, Leo, in the show notes I snipped out the first three lines of the sr.asm file. I wasn't sure whether it was '86 or '87. Anyway, the header of the file says file:sr.asm by Steven M. Gibson, created 03/30/87.

Leo: That's history right there. That's great.

Steve: That's the creation of the first SpinRite dot ASM file.

Leo: Wow. Did you have a macro to do the +---+? Or did you type that by hand?

Steve: No, no, no.

Leo: I figured you'd have a macro.

Steve: That was Brief. I don't - oh, back then?

Leo: Oh, of course, yeah.

Steve: Actually that was before I hired - Steve Rank was my first non-security or my first techie employee. I hired Sue. And Sue's been with me for I think, like, 36 years or something. Steve was employee number two. And one of the first things I had him do just to sort of get his feet wet was to write this massive macro package for Brief. And, I mean, it did everything I could ever ask it to do. And so I was able to like snap text boxes with a beautiful line drawing characters around. And so this is actually an ASCII-ized version of that. Because I later wrote a conversion of the beautiful line drawing characters back into ASCII when I - actually it was recently, it was a couple years ago because I needed to be working, I had to give up Brief because it was 16-bit code, and I would have had to run in a VM, and it was just not worth the hassle. So now I'm doing everything...

Leo: You used Brief for almost as long as I knew you, though. I mean, I remember you were the Brief guy.

Steve: Yes.

Leo: By the way, I looked more through that listing, that assembly language listing from 1987. And buried deep within it I found this, which I thought was kind of surprising. There is a Salisbury steak.

Steve: Oh, it is, Salisbury steak.

Leo: Now, I don't know if you got the free safety-colored rain poncho.

Steve: It looks like a brownie in the middle, there, Leo.

Leo: It's gingerbread or some - and then remember those mashed potatoes that were stiff, and they were crusty, and oh, yeah.

Steve: We were, Leo, we were hungry.

Leo: We were. We'd eat anything. That glass of wine didn't hurt, though, you know, with the appetite.

Steve: Yeah, that helped to wash it down, that's for sure.

Leo: It's so great that you - so you posted that source code, or no? Is that private, that source code? The original assembly language?

Steve: I will ultimately release it to the world.

Leo: Oh, nice.

Steve: Because the world ought to have it. And I will do that at a point when I am no longer maintaining SpinRite.

Leo: Somebody can fork it, then, which would be cool.

Steve: Yeah, exactly. At some point I'm just going to say, okay, I'm...

Leo: It's yours.

Steve: Hopefully it'll be at a point around where we said goodbye to Jerry Pournelle, somewhere at that level.

Leo: Yes. I can't wait to have Steve Gibson come on the show and talk about the good old days.

Steve: How those things used to spin. They actually spun.

Leo: They spun.

Steve: Why would you spin something like that?

Leo: Thank you, Steven "Tiberius" Gibson, for joining us for Episode 20,000. Anyway.

Steve: So anyway, everything since then has changed. None of those assumptions, they no longer hold, but they had been allowed to remain in place, even through SpinRite 6, though like with all things Microsoft they were becoming quite old and creaky. So as everyone knows, 6.1 is not a patch to SpinRite 6. Even though it's a minor version bump and therefore a free upgrade for everyone who owns 6, I am making this multiyear investment in SpinRite's future today because I've seen the future. And to my utter amazement, SpinRite is still in it.

Leo: Right on.

Steve: You know? So mostly I'm looking forward to writing the code beyond 6.1. But we have to have 6.1 first to create the platform for that. So the point is it's alive. I'm sort of astonished. I mean, like I actually have it running. And now I'm going through and like finding weird little bits because among other things, it used to be 16-bit code, which means that I'm having to write within segments which are 64K. And SpinRite used to fit all in one segment. That is, all of its data and all of its code was in 64K. But with maybe SpinRite 5 I think is where it would no longer fit. I needed to add things, and there was nowhere for it to go. So I created a second segment. But it's a pain to cross segment boundaries, for lots of reasons.

Anyway, so one of the things that I've been doing is I've been moving chunks of SpinRite over into this secondary segment, just so make some elbow room for the future. So anyway, it's coming back to life. I'm finding, the reason I mention that, is that there were like weird little side effects of code running in a different segment that thinks its data is in the same segment as it is because that's always been true. But it's no longer true. And so there are side effects of that. So I have a ways to go. But we're getting there. And I'm asking questions in the newsgroup like should the log files still use the line drawing characters, or should when we log, should I translate everything into ASCII? And everyone agrees it should all be moved over to ASCII because no one's viewing the log files in DOS anymore. They're viewing them in their own operating systems. So maybe UTF-8. We'll see. But anyway, progress on that front.

Leo: Woohoo.

Steve: Also pfSense and Tailscale. Everyone knows that pfSense is my preferred Internet firewall router solution. It's open source, has a fully capable free community-supported release. It's rock solid, runs on most hardware, inducing little fanless consumer routers like my little favorite, that Netgate SG-1100. And it has a very comfortable web-based UI for configuring it. And it'll do anything you could want.

As I mentioned, I use it to glue my various locations together over permanent links to essentially run a single, what we would now call an "overlay network." But I did it like the

old-fashioned way before we had easy-to-use overlay networks. Which brings me to Tailscale. Among pfSense's many features is a modular package management system which makes managing the router what I would call "manpage-free" pleasure. You don't need that. You know, you just point and click, and things go.

Leo: Everything should have a package manager. That's just the best, yeah.

Steve: Yes, yes. It's just it makes life possible. So the news I wanted to share is that pfSense will soon, with its forthcoming v22.05, which is now the dev release, when it goes into the main channel it will be receiving built-in drop-menu selectable support for the Tailscale VPN mesh overlay network.

Leo: Nice.

Steve: That's the way to do this. You missed somebody last week, Leo, commenting that - we were talking, remember, the week before we were talking about using a VPN in a caf or somewhere. Someone mentioned just bring a little box that has a Raspberry Pi on it running Tailscale. And essentially you can simply plug into that and be on your home network, wherever you are, thanks to an overlay network, which works very much the way Hamachi did back in the day. Hamachi was the first overlay network to become really popular.

Leo: So that's kind of cool. So like Hamachi you'd be appearing to yourself to be on your home network.

Steve: Yes.

Leo: Would all the other home network features be available, as well?

Steve: Yes.

Leo: Oh, that's nice.

Steve: It'd be like you were plugged into your router at home.

Leo: That's very cool. I like that.

Steve: And Tailscale is built on WireGuard, so it uses that state-of-the-art minimal next-generation VPN, which is the improvement over OpenVPN, which very much like OpenSSL has just gotten too long in the tooth. It's got so much crap in it now that's no longer needed. So WireGuard is a clean rewrite. Tailscale runs on top of it. It's all free. It does automatic key rotation, NAT traversal, single sign-on with two-factor authentication. These guys have it nailed. And shortly you'll be able to do a point-and-click in order to install it under pfSense. So I wanted to give everyone a heads-up about that.

And lastly, two little bits of Closing the Loop. Someone whose Twitter handle or his Twitter name is "Dangerously Close to Hijinks" - apparently you can use long names in Twitter. He said: "Thanks for all you do. Would you share the software solution you use for grc.sc? Do you recommend it?" And then before I could reply, he sent me another follow-up. He said: "Thanks to you and Elaine, I found the reference for URL shortener YOURLS in Episode 858."

So yes, yourls, Y-O-U-R-L-S, dot org, is short for "your own URL link shortener," yourls.org. And I love it. It's what I use. It is a tiny little PHP library so you can bring it up on any system that has an SQL server. He likes MYSQL 5 or later. PHP 7.4 or above. You need mod_rewrite enabled if you want to mess around with the API. It runs on pretty much any, you know, certainly Apache, Nginx, Cherokee. I run it on IIS. It does need HTTPS support. Anyway, it's a very - all it is is what it does. There's an admin panel. You're able to drop in a long URL, tell it what you want the short one to be. It saves it to the SQL database. And then when someone comes in with that short URL, it just issues a 302 redirect to the long one. And for a while I was using bit.ly, but I was using episode numbers as a convenience to people. And of course, naturally, somebody began...

Leo: Somebody stole it.

Steve: ...grabbing the episode numbers in advance of my use of them.

Leo: There's always one - this is why we can't have nice things.

Steve: This is why we can't have nice things.

Leo: So is it going to be - you can do your custom domain, too; right? So it'll be grc.com/?

Steve: Actually, since I had sc for shortcut, it's grc.sc.

Leo: Oh, that's nice, slash whatever. And you can...

Steve: Slash whatever.

Leo: That's great. And no one else can do it because - yeah. Good.

Steve: Because it's just mine, yeah.

Leo: It's yours, yeah. I used bit.ly the other day to create our shared photo library for the cruise. And I was thinking, why am I not running my own URL shortener? So now you've pointed me in the right direction.

Steve: Yes. And twit.sc, if it's not already gone.

Leo: Yeah, yeah.

Steve: In fact, [crosstalk] I just said that.

Leo: We have TWiT dot - no, no. We own TWiT.to, so...

Steve: Perfect.

Leo: Yeah, that's a good one, yeah.

Steve: Nice, nice. Yeah, because it wants to be short, too. And I just love this little bit of humor from @biswbmatt. He said: "In regards to Episode 880," he said, "IPv6 is the technology of the future. And it always will be."

Leo: That is a great line.

Steve: Isn't that great? I love that.

Leo: Wow. That's good.

Steve: Something came up, we were talking about - oh, I know what it was. It was, Leo, the price of an IPv4 IP address is, I've forgotten now what it was. It doubled in a year. I think that's what it was. It's now 25 to $30 per IP because, again, no one wants IPv6. They'll pay whatever the going price is for IPv4, even if it's seeing crazy, it was like exponential price increase over the past few years. So again, IPv6 is the technology of the future, now and forever.

Leo: I'm ready for the topic of the moment.

Steve: I probably should have titled this podcast "The Demon Cube."

Leo: Oy.

Steve: So the MV720 is a tiny cube measuring about an inch by an inch by an inch. I've got a picture of it in the show notes at the top of this topic. And if someone were to tuck it under your car's hood without your knowledge, plugging it into your car's wiring harness, you would be hard pressed to know that anything was out of place. In fact, if your car's authorized service people were working under the hood, they, too, would likely pass it off as just some "supposed to be there" relay.

Leo: It's just a little plastic box that sits in between the connector and the plug.

Steve: Yup. And this innocuousness would be by design since the manufacturer of this sneaky little cellular radio-equipped GPS satellite monitoring and vehicle control overriding demon boasts at the top of its web page, below the title "Easy to Hide," it says that "MV720 looks like a relay, but is actually a locator." So the question is, who put it there, and why? Since this thing only costs - now, in my notes I wrote 20 bucks, but later I looked on Amazon, and I found it for $26. So it could be anyone who put it there who has reason, legal or otherwise, to want to monitor and track a vehicle's location and speed while having the option - get this - to remotely shut down the motor's flow of oil and gas, causing the vehicle to gradually slow down to a point where the engine can be shut off and disabled.

Leo: Ow.

Steve: All remotely.

Leo: What?

Steve: And now, wait till you hear how insecure this is. I mean, it's one thing for your light switches and plugs to, like, have crappy security. This thing probably takes the cake.

Leo: So it's really, it's not a tracker, it's a cutoff valve.

Steve: Yes. That, too.

Leo: It's a kill switch and a tracker.

Steve: Yes. Yes. Yes.

Leo: And it's only $26.

Steve: And, yes, a single click on Amazon.

Leo: Holy cow.

Steve: So again, the question is, who put it there and why? These things exist. And while I'd be happy...

Leo: Well, you know, I mean, there's a legitimate use like sometimes now when you buy a car, if you don't make your payments, they've got a kill switch in the car so they don't have to send the dog after you, bounty hunter to get you.

Steve: Instead of the repo man.

Leo: Yeah.

Steve: Right, right.

Leo: You just kill the car. And then they have the GPS to know where it is. So I imagine that's the market they thought they were going after, anyway.

Steve: Right. Well, and unfortunately they're getting more than they bargained for. These things exist. While I'd be happy to be talking about them if only for the sake of noting their existence, as you and I just have been, Leo, they wouldn't normally rise to the level of being a headline topic for this podcast. So our long-term listeners can probably see where this is headed.

What do we know about this thing's manufacturer? Okay? MiCODUS (M-I-C-O-D-U-S) is a Shenzhen, China-based manufacturer and supplier of automotive electronics and accessories. The company's main products are asset, personal, and vehicle GPS trackers. MiCODUS devices are available for purchase via Amazon, AliExpress, eBay, Alibaba, and other major online retailers. And as I said, I found one on Amazon for $26. If you just put in "MV720" into Amazon, up it comes. There's some other reseller is the one that Amazon lists, but it's the same device. You can just tell by looking at it, and all the features are identical.

So in addition to GPS devices, the company provides a cloud-based platform via web, iOS, and Android apps for remote management, fleet and asset tracking, as you were suggesting, in fleet mode and vehicle-specific applications. MiCODUS states it provides "a secure, open and scalable platform that plays an essential role in the optimization of resource utilization by enabling visibility and simplifying management." And of course everyone assumes. They said it's secure. Oh. Okay. Then we don't have anything to worry about.

The security vulnerability research firm BitSight took a look at this little device's security. BitSight chose the MiCODUS MV720 because it's the company's least expensive model with fuel cut-off capability. As we'll see in a minute, it's a cellular-enabled GPS tracker which uses a SIM card to transmit status and location updates to supporting servers and to receive SMS commands from its user. And, unfortunately, also from pretty much anyone else. As I'm sure no one is going to be surprised learning by what they found.

They found six vulnerabilities of a severity up to, two of them, CVSS of 9.8. If there were only a couple of these little one-inch cubes wandering around the planet somewhere, hopefully mainly in China, that would not represent a clear and present danger. But 1.5 million of just these particular models, these little demons, are currently present in vehicles located throughout 169 countries. Later down in the show notes I have a heat map showing where they are. They're present in the vehicles used by several Fortune 50 firms in the U.S., also by European governments, and by state government agencies in the U.S. There's a South American military agency that is employing them, as well as a nuclear plant operator. Given the tracking power...

Leo: Oh, well, what could possibly go wrong there?

Steve: Uh-huh, and the ability to remotely cut off a vehicle's fuel supply, multiple security vulnerabilities become worrisome. Okay, now...

Leo: There's a lot of them in China. That's really where they mostly are; right?

Steve: Yes. They are largely, fortunately, in China. So, good. Unfortunately, not all of them.

Leo: Yeah.

Steve: We know that mistakes happen, right, and that anyone can make a mistake. That's my mantra on the podcast. It's like, it's okay. It's how you deal with the mistakes, how you own up to them and fix them that matters. And this is where things go from worrisome to worse.

On September 9th of last year, 2021, BitSight initiated contact via the only email available on the MiCODUS website, sales@micodus.com. MiCODUS replied, asking for additional information to pass on to the MiCODUS sales department. BitSight requested a security or engineering contact. MiCODUS never responded to that request. So they waited until October 1st, again contacted MiCODUS using the only email address they had, and again requesting to speak with a security or engineering contact. This request was refused. Then MiCODUS contacted BitSight.

Leo: I'm sorry. It's Russia.

Steve: It's Russia.

Leo: Oh, oh, thank you for the correction. You're right.

Steve: Yeah. You're right.

Leo: Wojo said that's Russia, baby. It's actually green in China.

Steve: Yeah.

Leo: The Russians love them. Is great.

Steve: We love them, Demon Cubes.

Leo: We put this everywhere. We put them everywhere. Is great. KGB love Demon Cube.

Steve: So after nine days, BitSight did get email from MiCODUS. This was on October 10th, and I love this, claiming to be "working on the issues," despite the fact that BitSight had not yet shared any technical information with MiCODUS about what the problems were. So don't worry.

Leo: They don't know. They don't know. Nobody does.

Steve: We got it. We're working on it.

Leo: Yeah, it's a mystery.

Steve: We're going to, like, fix the security that you apparently are trying to tell us about, even though we haven't yet - we haven't let you do so yet.

Leo: I knew that. I knew that. What makes you think I didn't know that? I knew that.

Steve: So a month goes by. That was October 10th. Now on October 23rd BitSight made another attempt to contact the vendor. MiCODUS did not respond.

So now, that was November, and toward the end of November. They let December go by, and most of January. Mid-January, on the 14th, BitSight shared its research - and you'll see why in a minute because, I mean, this is worrisome - shared its research and findings with CISA to further its efforts, thinking, okay, maybe the U.S. government security agency can get a response from these clowns. BitSight requested CISA engage with the vendor and share the information. No luck.

On May 1st of this year, CISA again attempted to contact the vendor to share information. CISA established a connection with the vendor and shared the original research and findings. However, CISA has not heard from the vendor since it shared the research. So that was on May Day. Nothing. May goes by. June goes by. First half of July goes by. Nothing. On July 19th, after reasonably exhausting all options to reach MiCODUS, and given the lack of engagement from the vendor, BitSight and CISA collectively determine that these vulnerabilities warrant public disclosure. So CISA and BitSight decided to publish the research. That's what happened on the 19th, exposing all 1.5 million of these little demon boxes, the Demon Cubes, to immediate compromise because none of these problems have been fixed.

So what do we and now the entire rest of the world know about these 1.5 million insecure Chinese vehicle tracking devices operating throughout 169 different countries, mostly in Russia? Gee, I wonder if somebody could take advantage of that? Hello, Ukraine. Anyway.

Leo: Oh. Maybe there's a bright side to all this. Oh, interesting.

Steve: "BitSight discovered six severe vulnerabilities in the MiCODUS MV720 GPS tracker" - this is them writing - "a popular automotive tracking device designed for vehicle fleet management and theft protection for consumers and organizations. The MV720 is a hardwired GPS tracker allowing for external physical control of the device," device meaning vehicle. "In addition to GPS tracking, the MV720 offers anti-theft, fuel cut-off, remote control, and geofencing capabilities." You drive too far, your car stops. "The exploitation of these vulnerabilities" - I wonder if you have to, like, then push it back within, you know, inside the geofence.

Leo: Just a few feet.

Steve: And you can then use reverse in order to get back inside the working area. "The exploitation of these vulnerabilities," they wrote, "could have disastrous and even life-threatening implications. For example, an attacker could exploit some of the vulnerabilities to cut fuel to an entire fleet of commercial or emergency vehicles."

Leo: Oh my god. Oh my god.

Steve: "Or the attacker could leverage GPS information to monitor and abruptly stop vehicles on dangerous highways. Attackers could choose to surreptitiously track individuals or demand ransom payments to return disabled vehicles to working condition."

Leo: Yup.

Steve: "There are many possible scenarios which could result in loss of life, property damage, privacy intrusions, and threaten national security." And wait till you hear, Leo, where there's a non-password protected command that allows, believe it or not, allows you to tell the Demon Cube that its command-and-control server's IP has changed to something else. So now it won't ever try to actually even...

Leo: Oh.

Steve: I know.

Leo: That's devious.

Steve: You could permanently tell it that now you're in control of it.

Leo: Hijack it.

Steve: Yes.

Leo: Oh, my gosh. Holy moly.

Steve: So they wrote: "BitSight's research was conducted with the sole purpose" - just to put everyone's mind at rest, and unfortunately now it's all public, right, because they had no choice - "the sole purpose of assessing the security of the MV720 GPS tracker and to determine whether an attacker could access a user's GPS position." Oh, boy, can they. "Although the results surpassed the proposed initial goal, this report does not represent a full security audit" - I mean, like they just thought, okay, we've done enough - "of the MiCODUS ecosystem. However," they wrote, "we believe other models may be vulnerable

due to security flaws in the MiCODUS architecture. MiCODUS states there are 1.5 million of their GPS tracking devices in use today by individual consumers and organizations.

"Organizations and individuals using MV720 devices in their vehicles are at risk. Leveraging our proprietary data sets, BitSight discovered MiCODUS devices used in 169 countries by organizations including government agencies, military, law enforcement, as well as businesses spanning a variety of sectors and industries including aerospace, energy, engineering, manufacturing, shipping, and more. Given the impact and severity of the vulnerabilities found, it is highly recommended that users immediately stop using or disable any MiCODUS MV720 GPS trackers until a fix is made available." And once again, children, $26 on Amazon. You can have one of your own.

Leo: So Eric Duckman in our chatroom has analyzed the wiring diagram. He says it is a relay, so you have to put it in between your power supply and your oil pump or your gas pump. You have to put it somewhere where it would have that cutoff capability; right.

Steve: Right, right.

Leo: So that's what to look for, kids, if you just wanted to check. You might want to.

Steve: See if you have a Demon Cube in your car. Okay. So they said: "Through packet and traffic analysis observed between the website, the Android application, GPS trackers, and servers, BitSight determined that the MiCODUS architecture is organized as follows: All services appear to be hosted by a single server, www.micodus.net, which is at IP address 47.254.77.28. It provides a website via HTTPS, therefore port 443." So that. That's the website portal.

"Also an unencrypted API server to support the mobile apps via HTTP port 80" - that's at app.micodus.net, same IP - "and a GPS tracker custom protocol server running on port 7700, that's d.micodus.net, same IP. Although the website that's used to access MiCODUS GPS trackers via a browser uses HTTPS, the mobile app," as I mentioned, "uses unencrypted and unauthenticated plain HTTP. GPS trackers communicate with the backend server via a custom protocol on TCP port 7700. The protocol does not appear to be encrypted. Users can directly control and access the GPS tracker via standard SMS text messages." So you can just text these little Demon Cubes directly.

The full command list for model MV720 is - and I have a link in the show notes. And Leo, I couldn't embed it in the show notes because it needs a full screen in order to see it. But it's a little bracing what you can do with the commands. Without any logon or authentication, you can send the tracker the simple SMS command "where," and it will reply with a Google Maps link centered on the vehicle's present location. So, you know, you just send it an SMS "where," and you get back a Google Maps link that allows you to view where the vehicle is located. Or also with no password, sending a "555" turns off the vehicle's fuel, and sending a "666" resumes the fuel. Actually, it's too bad those weren't reversed.

Leo: Oh.

Steve: It'd be better if 666 were to be the shutoff.

Leo: Wow.

Steve: BitSight managed a couple of classic attacks which are enabled by the vulnerabilities they discovered. There's the Man-in-the-Middle Attack. An attacker performs a man-in-the-middle attack intercepting and changing requests between the mobile application and supporting servers, taking advantage of the unencrypted HTTPS communications between them. This would give the threat actor complete control of the GPS tracker; access to location information, routes, geofences, and tracking in real-time; as well as the ability to cut off fuel, disarm the vehicle alarms, and more. And note that by being a man in the middle, you can change what the GPS tracker reports. So after obtaining that status, you wait for the vehicle to go somewhere, you report its location somewhere else, and it can no longer be found by GPS because the man in the middle is in real-time changing the GPS tracker's reports back to the mothership.

Second attack: Authentication Bypass. And I'll detail this in a second. But a flawed authentication mechanism in the mobile application could allow an attacker to access any device via a hardcoded key. Using the key, and by that they mean a password, an attacker could send messages to the GPS tracker as if they were coming via the SMS channel, so you don't even need to use SMS, which should only accept commands from the GPS owner's mobile number. Again, this would give an attacker complete control of the device; access to location information, routes, geofences, and tracking in real-time; and the ability to cut off fuel, disarm alarms, and more.

And finally, the Persistent Invisible Monitoring Attack. It is possible to remotely reprogram the GPS tracker - oh, here they're talking about what I already mentioned - to use a custom IP address as its API server. This would give an attacker the ability to monitor and control all communications to and from the GPS tracker. The attacker could completely control the GPS tracker, with all the implications listed above, including the reporting of incorrect locations to the GPS server.

The ability to remotely reprogram these devices to use a persistent custom Internet IP as its API server strikes me as one of those "wouldn't that be cool" or "we can do this so we should" sorts of things that engineers toss in just because they can, without there ever being any possible need or justification for the feature, and at a significant and serious cost in security. So it's just so dumb for that feature to be in there, and so prone to exploit.

Okay. So what are these six vulnerabilities that BitSight found and that CISA agreed were worthy of CVS designation and in two cases a CVSS of 9.8? Okay. The first 9.8 one. Get this. The API server uses a single - I can hardly even say this, Leo - a single master global password for all devices.

Leo: Is it 123456?

Steve: No. It is 7DU2DJFDR8321.

Leo: Oh, well, no one's going to guess that.

Steve: They're not going to guess it, but now everyone knows it. And it's global. That's all you need.

Leo: Oh. And you can't disable it or anything.

Steve: No. Cannot be disabled. They can't ever change it because there's no provision in there for changing it.

Leo: They don't do firmware updates. What, are you crazy?

Steve: Unh-unh. No.

Leo: That would be insecure.

Steve: On the Demon Cube? No. We just let the demon go off on its own. This is the password used by the user's mobile apps to query and perform actions and execute all remote commands. This allows an attacker to log into the API web server. And notice, everyone now knows the IP. Everyone now knows the password. And in a minute, everyone's going to know the protocol. And then all 1.5 million of these things are vulnerable because their device IDs are also knowable. This is just unbelievably bad, Leo.

Okay. This allows an attacker to log into the API web server, impersonate any user, and directly send SMS commands to their GPS tracker as if they were coming from the GPS owner's mobile number. Using the master API password, a remote, unauthenticated attacker can gain complete control of any GPS tracker; access location information, routes, geofences, tracking locations in real-time; cut off fuel to vehicles; and/or disarm alarms and other features. So it's impossible, I would argue, to label this as a mistake or oversight.

The developers, the people who coded this, must be well aware that this is not per account API authentication. All authentication is shared globally. And what's worse, it's not even necessary to reverse engineer one of their API endpoint apps or rig up some fancy sort of DNS spoofing and TLS intercepting man-in-the-middle proxy with a fraudulent cert or certificate authority. Since the app's API endpoint is HTTP unencrypted to port 80, any passive web sniffer can be used to capture the application's interaction with the MiCODUS API endpoint server.

Leo: Wow.

Steve: So it's not surprising that CISA gave this a CVSS of 9.8. And as I said, the master password, which is stored in all apps and which works universally, when using the protocol you can sniff with a sniffer on the API, I mean, okay. It occurs to me - this hadn't occurred to me before, Leo. For $26 every one of our listeners can buy one of these. You can then download the app. You can sniff your Internet connection while this thing phones home, look at the protocol, and play.

Leo: Oh, man. Sure.

Steve: This is a perfect toolkit for anyone who wants to play around with what is hacking like. Because there's never been a more readymade opportunity to do this. It's just amazing.

Leo: Yeah.

Steve: The password, once again, which all apps use, which works universally for logging into the API endpoint at the IP that I gave earlier, and port 8 over HTTP, meaning standard, you know, in the text query and reply, is 7DU2DJFDR8321.

Leo: Would you stop saying that out loud? Holy moly.

Steve: Vulnerability number two. The second major problem, also a CVSS of 9.8, is broken authentication. These guys write: "The API server provides a way to directly send SMS commands to the GPS tracking device as if those commands were coming from the administrator's mobile device. 123456 is the default GPS tracker password, which should be changed. However, some commands work even without a password." Notably 555 to kill the vehicle's fuel. You don't need a password for that. Go figure.

"The web interface and mobile app also require a password when directly contacting the tracker via SMS. However, it shares the same default password issues as the GPS tracker. Even if the user changes the password, the device is not secure. Some SMS-like command messages sent directly from the API server do not need the device password to function, leaving the device exposed to hackers.

"One potential attack can be perpetrated by abusing the adminip command" - this is the feature that I noted earlier that should never have been included in the API in the first place - "which defines the API endpoint of the GPS tracker." Meaning where the GPS tracker, the little tracking demon, connects to, the IP of the server, you can change it. "This enables an attacker to achieve a persistent man-in-the-middle position, controlling all traffic between the GPS tracker and the original server, and gaining total control over the GPS tracker."

In their full disclosure, they provide a working proof of concept. I didn't put it in the show notes again. There's a link in the show notes to their full disclosure. You had brought it up earlier in the video, Leo, where they show screenshots of all of this being done, redirecting the API through their own server to the original server so that they are able to install their own man in the middle.

Vulnerability 3. Okay. This one came - this was an 8.1, only because probably they just got tired of issuing 9.8s. We always have the popular default password of 123456. They said: "As noted above, all devices ship preconfigured with the default password 123456 [yup] as does the mobile interface." I'll just jump to a different place in the show notes because I happen to have remembered. They did a test of 1,000, they randomly chose 1,000 devices. And again, how do you do that? The device IDs are not hard to guess.

Leo: Can you go to Shodan? No, because it's port 80 traffic.

Steve: Right. Yeah, they actually, because the API is unencrypted, and all you need is the password which we now know, you can then guess the device ID. They guessed 1,000 device IDs, found them. 945 of the thousand had not changed the password.

Leo: Of course not. Of course not.

Steve: From 123456.

Leo: Of course not. Of course not. By the way, there's a simple command to change the password. But no, of course not.

Steve: Uh-huh. So the device ID follow the pattern 720, which of course is the model number, right, MV720 is the title of the podcast. 72011, followed by six digits. And they said: "With the value represented by the X's occurring in sequential order. So you start at zero."

Leo: This is so pathetic.

Steve: It is unbelievable.

Leo: Everything they could do wrong, they did.

Steve: Yes. That sums it up. That should be the title of the podcast. Everything they could do wrong, they did. So, you know, a big problem is that the need for security, the things that security is securing, are more often than not a complete mystery to a device's new user. If someone explained to them what the consequences would be of not changing the password, they would almost certainly happily change it. But 945 out of a thousand users didn't bother. So anyway, this is just a - I think one of the problems, Leo, is that we have devices that sell for $26. And so they're just not expensive enough to take them seriously.

Leo: Right.

Steve: Yet when you plug them in, and they drive off, they're now enumeratable. Every hacker in the world can now know where the vehicle is that is carrying this Demon Cube. And if you happen to wire it into the fuel supply, they can stop it wherever they want to. It's just unbelievable.

Leo: A lot of government agencies are using these.

Steve: Yup.

Leo: That's scary. Jiminy. Okay.

Steve: The takeaway lesson for us here is that, to take this as a valuable case study, we need to recognize that when we're using anything such as this, which connects to a remote Internet service of unknown repute, we truly are placing a huge amount of trust into entities whose trust has not been earned and may not be deserved. It's bad enough to have one's light switches and plugs connected back to potentially hostile foreign soil. But giving remote, and in this case clearly irresponsible, entities real-time knowledge of

vehicle location and movement and even over the vehicle's real-time fuel flow seems reckless at best.

Leo: Yeah.

Steve: And yet it's inexpensive, so it's done.

Leo: Unbelievable. Does this qualify as an IoT device?

Steve: I would say it is.

Leo: Yeah.

Steve: It's an IoT.

Leo: It's in your car and not your house, but it's - yeah. It's out there, and it's on the Internet. Does it use standard cell networks? How does it...

Steve: Yeah. It won't do the latest.

Leo: 5G or LTE.

Steve: 5G. I think it's actually limited to 2G, as I recall, because I read the specs on it.

Leo: Well, the good news is there are not a lot of 2G networks left. That's probably why it's so big in Russia and Mexico.

Steve: Yeah. So it's like 900 and 1800, and I remember seeing the various old-school cellular frequencies.

Leo: So the new version, I think they're going to update it, the new password will be 1234567.

Steve: Ah.

Leo: Just a little tip.

Steve: Whoa, Leo. Nobody will get in.

Leo: We're going to address that security flaw right there.

Steve: It'll just go silent.

Leo: Wow. Yeah, so this must be an older device if it's 2G. Unless it's for fleets that might have their own 2G cell communications or something like that. The U.S., 2G's been turned off pretty much everywhere.

Steve: That's interesting. So there is a red X on one of their web pages in their specs, which says not for use in United States. So it may just be that it just doesn't work there, thank goodness.

Leo: The last 2G network in the U.S. goes down at the end of the year, but most of them have already been turned off.

Steve: But, boy, Ukraine. Hello, Ukraine.

Leo: Yes, yeah. You see where it is, developing nations. Well, you know who uses it? Ukraine also uses it. But you could really go after Russia with this.

Steve: Oh. It's a hot tamale on that map.

Leo: Wow, wow. Unbelievable. What a story. If you want all the details, there are lots of links in the show notes. And if you're looking to hack one of these, everything you need to know is right there.

Steve: I would. It's not illegal if you own it; right? It's your own device? Hack it. I mean, it's a perfect introduction to hacking.

Leo: Yeah. Yeah. And you could - it's a certain kind of relay, though. You need the right pinout. So I'm thinking maybe you could use it for an irrigation sensor or something. Ping your Rain Bird or something. I don't know. It just seems like there could be some uses.

Steve: Or stick it on your Segway, and you'll know where it went.

Leo: Stick it on your Segway, yeah. Well, that's the good news. None of my electric vehicles have either a gas pump or an oil pump. So I think...

Steve: That's good.

Leo: I don't know what they'd attach it to. I think we're all right.

Steve: They attach it to the battery and disconnect that.

Leo: Gone. Gone. It's an NC relay, so you have to have an NC device.

Steve: That just means normally closed.

Leo: Oh, oh, thank you. Chat room, of course, always on top of this. There is good news. If you go to AliExpress, there is now an updated 4G-compatible device.

Steve: Ah.

Leo: It's a little more expensive. But it's the same fine company, MiCODUS.

Steve: Ah, nice.

Leo: It's the 4G ML500G, and this one's waterproof.

Steve: So you can, yes, you can know where your submersible sub went.

Leo: Yes. Yeah. So there you go. And I bet you it's just as insecure. But it'd be worth...

Steve: Leo, it's all based on the same infrastructure. It has to be.

Leo: Right, has to be.

Steve: Just as insecure.

Leo: Yeah. Because it's the server that's insecure, not the device.

Steve: Yup. It is the protocol and the server which is not encrypted.

Leo: This one has a device temperature and voice monitor, as well.

Steve: Oh, that's great.

Leo: Think of what you could do.

Steve: Oh, my god, it's a spybot.

Leo: It supports the latest 4G LTE CAT 1 network on multiple bands for operation globally.

Steve: There's a map with little happy smiley faces all over the globe.

Leo: Everywhere. All over the globe. And of course still support for 2G, in case you want to - oh, look. This one can be magnetically attached under the chassis.

Steve: Oh.

Leo: So this isn't a cutoff, I think. This is just a cheap tracker.

Steve: Oh, god. My stomach hurts from laughing.

Leo: Yeah. Oh.

Steve: Oh, lord.

Leo: Remotely voice monitor. Look, here's a good use. They've got an eight-year-old girl with her backpack, voice monitoring her. And who's this creep listening in? Geez, Louise.

Steve: Oh, my god.

Leo: This is not good. This is not good.

Steve: Oh. Oh.

Leo: Okay. Thank you, Steve, as always. This is the show that gives you the screaming meemies at night. But if you don't listen, just imagine how scary the things you don't know about are. Right? Every Tuesday we gather together, 1:30 Pacific, 4:30 Eastern, 20:30 UTC to learn the latest from this guy right here, Steven M. Gibson, I now know. Steven M. Gibson. If you want to get the show from him, you can. It's at GRC.com. That's his website, the Gibson Research Corporation. You can leave feedback for Steve there, too, GRC.com/feedback.

Steve has 16Kb versions. He's got 64Kb full bandwidth audio. He's also got transcriptions. GRC.com. While you're there, check out check out SpinRite, the world's best hard drive or mass storage, really, any kind of mass storage, even SSDs, maintenance and recovery utility. Currently 6.0, soon to be 6.1. We are inching close. And if you get 6.0 now, you'll get the free upgrade, so this is a good time to get your copy of SpinRite. Everybody, if you've got mass storage, you need SpinRite. Lots of other stuff there, free stuff that Steve does pro bono.

We have copies of the show at our website, ad supported, at TWiT.tv/sn. YouTube has a channel dedicated to Security Now!. You could join the club, get the ads out. There's a couple of ways to get the ads out. You can either go to TWiT.tv/clubtwit, join the club for 7 bucks a month, then get all the shows ad free, plus the Discord, plus the special TWiT+ feed. Or just get Security Now! by itself for $2.99 a month, if you're a cheapskate. Spend the 7 bucks. Get it all, plus the Discord, which is a great place to hang. But again, we always have free versions available at the website. If you want to chat with us while you're watching the show, irc.twit.tv, as well as the Discord channel for club members.

And best way to get it, honestly, subscribe. Subscribe to the audio or the video feed. Each format has its own feed. And you'll get it automatically on a Tuesday evening, right after we chop it up and mince it and put it into fine delicious squares. I guess that's what the editors do. I don't really - I don't understand how that stuff works. Get your favorite podcast client and subscribe to Security Now!.

You watching any good sci-fi, Steve?

Steve: Actually, we just started "The Dropout."

Leo: Love that show.

Steve: Yeah.

Leo: And if you want more dystopian startup stuff, "WeCrashed" on Apple TV is all about WeWork and is fantastic, as well. Those two shows together.

Steve: Ooh, good, good, good.

Leo: If you like "The Dropout," you'll love "WeCrashed."

Steve: Fun. And we also finished the final season of...

Leo: "The Expanse"?

Steve: "Ozark."

Leo: "Ozark." Yeah, it's over.

Steve: I know. That was great.

Leo: When I go home tonight, last episode of "Better Call Saul." If you have not watched - did you watch "Breaking Bad"?

Steve: Oh, of course. And we watched all of "Better Call Saul." Was there more?

Leo: Oh, you haven't seen it all. He had a heart attack, literally, Bob Odenkirk, and they stopped. And there are four final episodes which have been coming out.

Steve: I thought it was as good if not better.

Leo: I agree.

Steve: I mean, it was well - it was at the top of its game.

Leo: Dude?

Steve: Cool.

Leo: It had a cliffhanger. Didn't you notice there was a big cliffhanger? I don't want to say anything. Go back and check your listings.

Steve: Okay. Cool.

Leo: Oh, it's so good. And everybody's probably already seen the final episode because it came out.