The Kaseya Saga

Description: The so-called Windows "PrintNightmare" remote code execution flaw, as bad as it is, was overshadowed by the Sodinokibi malware which the REvil ransomware gang managed to infiltrate into Kaseya, a popular provider of remote network management solutions for managed service providers. Since those MSPs all, in turn, have their own customers, the result was a multiplicative explosion in simultaneous ransomware attacks. Since those attacks reportedly numbered in excess of 1,000, this makes it the worst ransomware event in history. So, while we'll definitely be covering the PrintNightmare and other events of the week, our topic will be the reconstruction of the timeline and details of the Kaseya Saga.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-826.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-826-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here with an update on Microsoft's PrintNightmare. Apparently, they didn't fix it completely. Another patch just came out. Steve explains all. We'll also talk about a BMW with SpinRite running, plus the Kaseya nightmare. How bad is it going to get? Steve has details, all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 826, recorded Tuesday, July 6th, 2021: The Kaseya Saga.

It's time for Security Now!. Get ready. Fasten your seatbelts. We're going to talk about keeping yourself and your loved ones safe, private, and secure online with this guy right here, Steve Gibson of GRC.com. Hi, Steve.

Steve Gibson: Leo, great to be with you again. And I actually do use the phrase "buckle up" later on in the podcast.

Leo: Yeah.

Steve: So, yeah. Be good to have those seatbelts buckled. I tripped over the spelling of this randomly spelled company for the name of the podcast. So I'll be fixing these show notes, if any of you find the spelling somewhat confusing.

Leo: I think you got it right in the show notes.

Steve: I got it right several places. But the download, I think, is K-A-Y-S-E-A, and that's not it. It's K-A-S-E-Y-A. The Kaseya Saga is today's topic. The so-called Windows PrintNightmare, which was both a local privilege elevation or escalation and, it turns out, also a remote code execution flaw, as bad as it is, was overshadowed by the Sodinokibi malware which the REvil ransomware gang managed to infiltrate into Kaseya servers. They're a popular provider of remote management solutions for managed service providers. We were just talking last week about managed service providers being an interesting infection vector because they inherently are in the networks of all of their clients. So if you go up the food chain one level to the purveyor of a server used by MSPs, then if you can get in there, you get everything. So, boy. What was the count you just heard, upwards of 1,500?

Leo: 1,500. It's sad because it's all small businesses.

Steve: Yes.

Leo: Like ours. We use a managed service provider. Russell's an MSP.

Steve: Yes, who would be outsourcing some function of your system.

Leo: You can't afford a full-time IT department, you're going to have the contract IT guy, an MSP, and they're - very frequently they use this software. I don't think Russell does, thank goodness. But 1,500. And that's, I think, going to be a small number compared to the total eventually. Lots of companies.

Steve: So what we have is at least now the worst ransomware event in history. And what's fun is, a lot is known about it, like the fact that they actually knew about the problem before the attack.

Leo: Oh. That's annoying. Oh.

Steve: Oh, that one's got to hurt. So anyway, Episode 826 for this first podcast of July, making next Tuesday a much-anticipated Patch Tuesday. Hopefully Microsoft will have had time to try again to fix the PrintNightmare. Well, we'll be talking about it. But they actually fumbled the first fix last month, which is part of the problem. And we have a really interesting and wacky Picture of the Week. So I think we've got another great podcast for our listeners.

Leo: Yeah. But just to be clear, the Kaseya problem is not related to the Microsoft problem. These are two unrelated...

Steve: Oh, yeah, sorry, correct.

Leo: No, no, I just wanted to [crosstalk].

Steve: Just a lot going on. A lot going on.

Leo: Yeah, no kidding. Steve, shall we do the picture?

Steve: Now, you know, remember that picture we had quite a while ago, a couple years ago, Leo, that had the ground wire going into the bucket full of dirt?

Leo: Yeah. That's ground, yeah.

Steve: I looked at that for a while, and I thought, what is going on here? Well, this picture is not that. It's quite a bit more sophisticated. But when I understood what was happening, I gasped because - okay. Well, for several reasons. First of all, okay, this was tweeted to me from @lifeattv, which is Life at Terminal Velocity is the person's name on Twitter. And it shows a high-end car, a BMW, whose center console he has just completely disassembled. Which, again, that's not where normal people go. It's factory assembled, and it's impossible to get into. I mean, countless YouTube videos are committed to, like, how do I take my radio out of my car?

So we have two pictures in our Picture of the Week. For those who cannot see what's happening on the screen - okay. So what he tweeted, the textual content is "SpinRite saves the day again. My BMW is having fits, has a mechanical hard disk drive." Okay, now, I didn't know this. You knew this, Leo. Stop right there. You have a car with a mechanical hard disk drive in it? Okay, apparently that...

Leo: Seems like a bad idea on the face of it.

Steve: Seems like a really, I think, almost...

Leo: I don't think any modern cars do, but 10 years ago it wasn't uncommon, yeah.

Steve: Leo, as bad as a hard disk drive in a laptop. Who would ever put a hard disk drive in a laptop? Yet, oh my god, everybody did. And in fact we probably recovered - SpinRite was probably used more to recover laptop hard disk drives because there the heads were literally bouncing on the surfaces as someone would, like, toss their drive across the room to their spouse with it, like, on. Anyway, he said: "Dealership wants $1,500 in parts and $1,000 in labor." So that's $2,500.

Leo: Whoa.

Steve: Yeah. Well, look at what it takes. I would charge somebody $1,000 to open all this up. My god. And I'd just walk away without trying to put it back together again because apparently the stories my parents tell me is what I used to do is just take stuff apart to see how it worked, and then I wasn't really that interested in reassembling it.

Leo: I took apart many a pocket watch and other clock devices and never could figure out how to get all those little pieces back in there.

Steve: Yeah. I know. You end up with some spare little springy things.

Leo: Yeah, things go flying across the room, you don't know what the hell they are.

Steve: Do we really need that? I don't think so. So anyway, he said, so $2,500 "to maybe fix the problem." So he said: "This is the second pass," which is the first picture, showing SpinRite running. He says: "This is the second pass. First pass fixed some issues. Radio now boots."

So anyway, this was on June 29th he tweeted this. The first picture shows, again, this is like - so he's got a desktop PC sitting in the passenger seat with the red SATA cable coming out of it, probably plugged into the motherboard, coming out of it to a SATA extension, which you can see in the second picture, which then plugs into a Toshiba 3.5" spinning, you know, I think I have a few of those around here. I think for some reason it was a 1.5TB drive. I don't know, maybe I just zoomed in and I saw that, or I'm not sure why I think that; but, you know. And he's got all of his tools on the driver's seat. And then there's like this cast steel center console thing which is kind of half out. Anyway, I don't know how his car is ever going to go again. But at least the radio boots. So good luck.

Leo: This is hysterical.

Steve: Oh, wow.

Leo: I guess he couldn't - because I would have taken the Toshiba out and brought it into the house. But I guess he couldn't for some reason.

Steve: No, he can. It's got two plugs on it. I mean, it's not...

Leo: Yeah, but I think he needs the power, I'm guessing he needs the power from the car or something. I don't understand exactly why it's done this way. But anyway. Or maybe he just likes the idea of doing it in the car.

Steve: Well, whoever you are, Life at Terminal Velocity, I believe that you are well named because you are definitely running your life at terminal velocity. Whoa.

Leo: Actually, terminal velocity is not that fast. I just want to point out it depends on the air you've got.

Steve: That's true. It's gravity and air pressure and density and the amount of resistance.

Leo: Yeah, I think it's like 95 miles an hour. It sounds dangerous; doesn't it? Terminal velocity.

Steve: It does.

Leo: But it's just the fastest you can go in the air based on the gravity.

Steve: Right.

Leo: 32 meters per second squared, as I remember.

Steve: So our first story is PrintNightmare is not CVE-2021-1675. Probably the biggest nightmare about PrintNightmare, aside from the fact that it's being exploited in the wild right now, I mean, today, okay, after Microsoft thought it was fixed, is the incredible amount of confusion surrounding multiple stumbles that both Microsoft and some well-meaning security researchers have made. This has just been a mess. There are two related but separate and independent issues at play which affect all current and all previous versions of the Windows Print Spooler service, which Windows starts up and runs by default across the board. And being a print spooler, a trusted component, it's of course running with full system kernel privileges.

Now, Windows Print Spooler has historically been a source of many serious vulnerabilities. And we'll all remember, Leo, you were sitting with me when 10 years ago it was the exploitation of it, it provided the exploitation which was leveraged by Stuxnet to take over, spin up, and damage the centrifuges being used by Iran's nuclear enrichment program at the time. And it's been, again, I mean, it's a constant source of problems. And there are things, you know, there's the concept of a lemon, right, where you buy a car, and it's just got one thing wrong after another. And in fact there's a law, I think, right, the lemon law...

Leo: Yeah.

Steve: ...that at some point you're just allowed to say, hey, take this back.

Leo: Is this the lemon flaw? Is that what you're talking...

Steve: Well, no. I'm kind of put in mind of Adobe Flash.

Leo: Oh, yeah. Yeah, that was a lemon, yeah.

Steve: Which was originally, well, and think about it. It was originally written before security was an issue. So was the print spooler. I'm sure there's still code in there from Windows 95, when they thought, oh, we need to pool our sprinting. Wait, spool our printing.

Leo: Or pool our sprinting. Either one, yeah.

Steve: And so we're still - we've still got that code which probably some summer intern - because, I mean, okay. That's a perfect thing for Microsoft to have given a summer intern. Oh, give it to Harry. Because it doesn't matter. It's the print spooler. It's going to work or not. We're still running Harry's code now, and domain controllers are being taken over as a consequence. Anyway, here we are, 10 years later, with thanks to Harry's summer internship, a local privilege escalation vulnerability and also a separate remote code execution vulnerability.

And get this. During last month's June 8th Patch Tuesday, Microsoft believed that they had patched and closed the vulnerability. They only thought there was one. That was the local privilege escalation. They identified it as 2021-1675. But as Will Dormann, the vulnerability analyst at the CERT coordination center, tweeted: "I've published a vulnerability note on this. I suspect that Microsoft will need to issue a new CVE to capture what PrintNightmare exploits, as it sure isn't what Microsoft patched as CVE-2021-1675." In other words, okay, now, that would lead you to believe they patched the wrong thing. But it turns out no.

A Chinese researcher with NSFOCUS, who reported the original actual vulnerability to Microsoft, explained last Thursday in a tweet: "CVE-2021-1675 is meant to fix PrintNightmare, but it seems that they just test with the test case in my report, which is more elegant and also more restricted. So the patch is incomplete." And then he has a little frowny face in his tweet.

Okay. So understanding what he just said, this is not the behavior of a Microsoft whose OS the world can depend upon as much as it currently does. The NSFOCUS tweet suggests that rather than carefully examining the researcher's provided proof of concept and using it to reveal and understand the whole problem that it was intended to reveal, someone at Microsoft, maybe late for lunch, apparently quickly applied a patch to shut down the example code, but without resolving the underlying actual problem. Which you could still work around after the patch had been applied to Windows.

Okay. So then when this researcher saw what was not done last month, he attempted to reach out again to @msftsecresponse. Failing to get satisfaction, he tweeted: "My case of #PrintNightmare is closed. And I can't log into MSRC portal because there is no Microsoft account option which I used." He says: "Then how can I report that you not fix CVE-2021-1675 properly?" And he says: "Another call is kept vulnerable." He says: "That is your cooperation?" And then he adds the @msftsecresponse so that Microsoft security response would receive the tweet.

And then the situation gets even worse, when just before the end of June, another Chinese security vendor, Qi An Xin, announced that they found a way to exploit the vulnerability to achieve both local privilege escalation and remote code execution, and published a demo video while deliberately refraining from sharing additional technical details in the interest of responsible disclosure. But the Hong Kong-based cybersecurity company Sangfor, seeing that, thought okay, well, apparently we're talking about this now. They published an independent deep dive of the same vulnerability to GitHub, which included fully working proof-of-concept code. So they apparently mistakenly believed that Microsoft had fixed it.

Leo: Well, it's been fixed.

Steve: When Microsoft hadn't, like because the guy didn't really give it the time it needed.

Leo: That's so bad.

Steve: Right. So they included in their publication on GitHub fully working proof-of-concept code. The proof of concept remained publicly accessible for several hours before they -someone I'm sure told them, hey, you realize you just published a proof of concept for a problem that Microsoft didn't fix...

Leo: It works.

Steve: ...on the 8th of June. Yeah, it's not a proof of concept, it's a proof of exploit. So they pulled it down, but it had been forked by that time. So the proof of concept remains available. I've got links to them in the show notes.

Leo: Oh, god.

Steve: And so they posted, the principal security researcher at Sangfor posted: "We deleted the proof of concept of PrintNightmare. To mitigate this vulnerability, please update Windows to the latest version" - which, eh, doesn't work - "or disable the spooler service." Which is really the only thing you can do to completely shut this thing down. Unfortunately, as I said, updating Windows won't help. Hopefully updating Windows next Tuesday will. Meanwhile, this is in the wild. Right? I mean, this is being actively exploited.

Leo: So do they need access to your machine? How can they get to the print spooler?

Steve: Yes. It is a local - well, okay. That's complicated, too. One of the things that's been happening among security researchers, like during this drama, is that they've all been publishing - they've been trying to publish flow charts to show what you turn on and what you turn off and where you go. Okay? So, and you're showing it on the screen. I've got it in the show notes here. This is the current flow chart which was produced by the CERT guy, Will Dormann, after his post-patch attempt to get a handle on this.

And so the short version is just, if you don't actually know that you need print spooler - for example, a domain controller probably doesn't have a printer on it; right? It's not - you don't have users dropping print jobs onto a domain controller. That's not what they're for. Print spoolers are typically on your local machine. I mean, you don't even have to use it; right? You can turn it off, and your machine can still print. It just ties up the app while it's printing instead of dumping it into the spool queue so that it can say, yeah, okay, we're doing that in the background.

Leo: But it needs RPC. You need remote access to use this.

Steve: True.

Leo: At least to remotely exploit it. I guess you can do it locally.

Steve: Exactly. The remote exploitation. The biggest problem is that it is a local privilege escalation, and that is in the toolkit now of the bad guys. As we've often said, it sounds like a remote code execution is really bad, and it is. But there's lots of uses, malicious uses for local privilege escalation, where, for example, many times you can do something, for example, like you can log onto an FTP server as an anonymous, very unprivileged user. But if that FTP server where you're logged in unprivileged, and even if it was running in an unprivileged account, right, to be really safe, well, if it's got a flaw that allows you to use an escalation of privilege, now you're root. Now you're system privileged, and you can do whatever you want.

Leo: It's not at all - these days I would expect it's almost universally the case that you don't - it's a chain of exploits. It's rarely just a single exploit. You get this chain that slowly gets you closer and closer to your goal.

Steve: Only when you purchase logon credentials for an RDP server from the dark web. And it's like, oh.

Leo: That works.

Steve: Still works. How nice. Yeah. What do I want to do today?

Leo: Oh, lord.

Steve: So this PrintNightmare was well named. It is a nightmare. It is, I mean, it should be an embarrassment to everybody who dipped their oar in the water of this thing and paddled in the wrong direction.

Leo: I can't believe that the patch was written to the published code as opposed to understanding the problem and fixing it.

Steve: Yes.

Leo: That's like, oh, I got all the questions to the test. What do I need to learn anything for?

Steve: Exactly.

Leo: It's so dumb.

Steve: Exactly. Whoever it was just thought, okay, maybe they're in a hurry. Like I said, maybe they were late for lunch. I don't know.

Leo: We don't know.

Steve: Yeah. But we're still with the problem, unfortunately.

Leo: "Hey, Joey. All the guys are going out for Chinese. Come on. Hurry up." "I've just got to write this patch. I'll be right there."

Steve: Yeah, yeah, because it's got to get out on June 8th. And so, oh, wow. So what about the vulnerability itself? It boils down to the ability of any non-privileged user to bypass the authentication barrier which prevents unprivileged users from installing whatever possibly malicious print drivers they choose. Specifically, any attacker who can bypass the authentication which protects the RpcAddPrinterDriver API can install a malicious print driver. Microsoft's documentation claims that the client needs to hold, that is, the client, the user who's calling the AddPrinterDriver API must have the SeLoadDriverPrivilege, which makes sense, for the AddPrinterDriver call to succeed. When you make a call to AddPrinterDriver, your security privileges are checked to see whether you are holding the LoadPrinterDriver privilege.

It turns out Microsoft's documentation is wrong. You don't need to have the LoadPrinterDriver. A call to the ValidateObject Access is being made. And it turns out that due to a mistake in the code that sets up the call's parameters, the user has control over the validation check and is able to skip it. Which despite the fact that the people who disclosed this confidentially to Microsoft said this, Microsoft said, okay, how do we - you know, like I'm late for Chinese. How do I fix this so this isn't true any longer? And they made a patch that fixed so that the proof of concept would no longer succeed, but the problem wasn't solved. Wow.

So if the target is a Windows domain controller, a normal domain user, an unprivileged user can connect to the spooler service, which, okay, should not be running in a domain controller. Hello. I mean, one of the things that we all used to do, those of us, remember Leo, in the old days, is we'd go through this exhausting and exhaustive list of services that Windows XP was running and just shut off a whole bunch of crap that Microsoft had running, taking up cycles, slowing down our boots, consuming RAM, you know, stuff like whatever synchronized folder link transport or something was. There's like, well, okay, I'm not - there's no one for me to synchronize to. What's this doing running?

Anyway, they just turn it all on because they'd rather that than have you call support if something you try to do doesn't work. But anyway, as a consequence, apparently Windows domain controllers the world over are running print spoolers which they don't need to run, which are vulnerable, and which allow an unprivileged user to install their own malicious driver, take over the Windows domain controller, and then these days spread ransomware throughout the domain. Oh. And before signing off, the researcher noted: "There are more hidden bombs in spooler which are not publicly known."

Leo: Oh, good.

Steve: "We will share more RCE and LPE vulnerabilities in Windows Spooler."

Leo: Thanks so much.

Steve: Yeah. "Please stay tuned and await our Black Hat talk, 'Diving Into Spooler: Discovering LPE and RCE Vulnerabilities in Windows Printer.'" So that ought to be next month. Yeah.

The 0patch guys have quickly produced one of their cool micropatches for this, if you need to keep your print spooler online for the next week and believe that you might become a victim of this before, hopefully, next Tuesday's Patch Tuesday. Either the guy came back from lunch and realized he'd made a mistake, or they kicked him out of his seat and put somebody who actually knows how to patch problems. Whoa. So with any luck this will finally be fixed permanently, and we can put the PrintNightmare behind us.

Leo: Yeah. So I'm just trying to remember. You don't have to use a print spooler. You could still print without a print spooler. Or no?

Steve: Right. If you turn it off, everything still works just fine. You shut the service down.

Leo: Okay. Just the machine may be tied up while you're printing.

Steve: Correct.

Leo: But printers are so fast now.

Steve: And actually not even the machine, just the app. It'll just, like, show printing, and it'll stay up instead of disappearing. And then, I mean, and it's almost annoying because, if you do have a problem with your printer, it goes to the spooler and then dies there.

Leo: And you think it's done, yeah.

Steve: Yes.

Leo: The spooler has always been a bag of hurt. That has never - I can - problem since Windows 95 with the print spooler. Constant.

Steve: Yeah, it's because of that summer intern, Harry.

Leo: The intern, man, he didn't know what he was doing.

Steve: He was there for a couple months. He said, "Yeah, here's your print spooler."

Leo: How hard could it be? It's not rocket science.

Steve: No. Okay. So I titled this one "The Authentication Dilemma." An eight-page PDF was jointly published by the U.S.'s NSA, CISA, and FBI, and the U.K.'s GCHQ-based National Cyber Security Centre, outlining an ongoing brute-force credential-stuffing attack being waged against the West by Russia's GRU, their General Staff Main Intelligence Directorate.

The executive summary on this eight-page detailed report says: "Since at least mid-2019 through early 2021, Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS), military unit 26165" - in other words, we know exactly who. I mean, we probably have the size of their underwear. But we know where they are. This thing says: "...used a Kubernetes cluster to conduct widespread, distributed, and anonymized brute-force access attempts against hundreds of government and private sector targets worldwide." And Leo, I heard you mentioning this on what would normally be the Sunday TWiT, but you recorded it on Saturday because of the Fourth of July.

"GTsSS malicious cyber activity has previously been attributed by the private sector using the names Fancy Bear, APT28, Strontium, and a variety of other identifiers." And we've bemoaned the fact that it's known by, like, 10 different names, so it sounds like 10 different people. But no. Or groups. Nope, just one. The 85th GTsSS directed a significant amount of this activity at organizations using Microsoft Office 365 cloud services; however, they also targeted other service providers and on-premises email servers using a variety of different protocols. These efforts are almost certainly still ongoing. And it's not here in this little executive summary. But like HTTP, HTTPS, SMTP, POP3, and so forth. You know, the standard TCP old-school TCP services.

They said: "This brute-force capability allows the 85th GTsSS actors to access protected data, including email, and identify valid account credentials. Those credentials may then be used for a variety of purposes, including initial access, persistence, privilege escalation, and defense evasion. The actors have used identified account credentials in conjunction with exploiting publicly known vulnerabilities, such as exploiting Microsoft Exchange servers using CVE-2020-0688 and CVE-2020-17144" - in other words, the ProxyLogon problems - "for remote code execution and further access to target networks. After gaining remote access, many well-known tactics, techniques, and procedures" - which we now refer to as TTPs - "are combined to move laterally, evade defenses, and collect additional information within target networks."

And then they finish: "Network managers should adopt and expand usage of multifactor authentication to help counter the effectiveness of this capability. Additional mitigations to ensure strong access controls include time-out and lock-out features, the mandatory use of strong passwords, implementation of a zero trust security model that uses additional attributes when determining access, and analytics to detect anomalous accesses. Additionally, organizations can consider denying all inbound activity from known anonymization services, such as commercial virtual private networks" - and I should mention that in the expanded pages of this they note that they're seeing the use of commercial VPNs to create more of a spray of source IPs to prevent easy lockout. So they're saying block known anonymization services such as commercial VPNs "and The Onion Router, where such access is not associated with typical use. Meaning that some, you know, you can pretty much determine whether typical users would be coming in through those means."

So I absolutely agree with the idea of filtering and blocking any knowable atypical access IPs. As I've often noted, anywhere a relatively static originating IP is knowable - for example, Leo, for you, between your work IP block and your home IP - it should absolutely be used, that is, a known block of allowed IPs as part of a connection qualification filter. Network connections that do not need to inherently be accepted from everywhere should never be accepted from everywhere.

We also know that strong security is not provided by simple obscurity. But when you think about it, that's what a password is. It may be very obscure; but many passwords, even today, contain many fewer than 128 bits of true entropy. So they are less obscure than a strong cryptographic key. In a world where the weakest link determines the effective strength of an entire chain, user-chosen passwords remain a problem.

From time to time, upon account creation - it's happened to me a few times - a web service will pre-assign a super-strong password to me rather than asking me to choose my own. I think that's brilliant. If I don't already have some means of accepting, securely recording, storing, and regurgitating on demand an arbitrary high-entropy string of characters, then I've already lost the game. I'm sure that everyone listening to this podcast has such a facility. We were just talking about one of our sponsors that offers that. But even today, we know that not everyone does.

And this brings me to my takeaway conclusion from this news from our law enforcement and intelligence services that the Internet's background radiation has inevitably evolved from randomly probing packets to deliberately focused and targeted connections which are attempting to brute force their way in. Bad guys are logging into other people's RDP servers using something that someone knows. We really do need to get completely away from the terminally weak "something you know" form of username and password identity authentication. And the sooner the better.

Whatever that solution will be, it needs to be free and easy to use so that everyone will be able to use it. And it doesn't even need to be perfect. It just needs to be a lot better than the decades-old mess we're still all using today. I sincerely hope that the right people somewhere, are giving this the attention it needs. As we all know, I invested seven years of my life creating one complete free solution to this need and problem. FIDO and WebAuthn are useful steps in the right direction, but they both fall short of offering a complete solution. The world doesn't need to use SQRL, but it sure needs to do something. And I hope it does.

Western Digital has stepped up. As we covered last week, many users of Western Digital's My Book Live and My Book Live Duo, whose last firmware update was in 2015, and who were consequently unable to patch even if they wanted to after a vulnerability was discovered three years later, in 2018, which was three years ago, they found themselves to be victims of a recent Internet-wide malicious data wiping campaign. Although direct evidence is not decisive, security industry observers believe that this may be the result of a war between rival botnet groups. We're bringing this up again with the news that Western Digital has, as I said, stepped up. And I'm very impressed.

Last Wednesday, on June 30th, WD updated their coverage of what has been a true disaster for many of their users. They posted: "Western Digital has determined that Internet-connected My Book Live and My Book Live Duo devices are under attack by exploitation of multiple vulnerabilities present in the device. In some cases, the attackers have triggered a factory reset that appears to erase all data on the device." And "appears" is of course the key word here. "To help customers who have lost data as a result of these attacks, Western Digital will provide data recovery services, which will be available beginning in July. My Book Live customers will be offered a trade-in program to upgrade to a supported My Cloud device."

And although it doesn't say it here, I read elsewhere, or someone talked to Western Digital and came away with the information that it would be no charge, no charge data recovery. They said in their note, and actually in their update: "The My Book Live firmware is vulnerable to a remotely exploitable command injection vulnerability when the device has remote access enabled. This vulnerability may be exploited to run arbitrary commands with root privileges. Additionally, the My Book Live is vulnerable to an unauthenticated factory reset operation which allows an attacker to factory reset the device without authentication." Thus unauthenticated. "The unauthenticated factory reset vulnerability," they said, "has been assigned CVE-2021-35941."

They said: "We have heard concerns about the nature of this vulnerability." And actually we voiced them loudly last week. Why did you comment out the test for the password? That seems like a bad thing. Anyway, they said: "We have heard concerns about the

nature of this vulnerability and are sharing technical details to address these questions." And indeed they did.

They said: "We have determined that the unauthenticated factory reset vulnerability was introduced to the My Book Live in April of 2011 as part of a refactor of authentication logic in the device's firmware. The refactor centralized the authentication logic into a single file, which is present on the device as includes/component_config.php, and contains the authentication type required by each endpoint. In this refactor, the authentication logic in system_factory_restore.php was correctly disabled" - that's the commenting that we all saw - "but the appropriate authentication type of ADMIN_AUTH_LAN_ALL was not added to component_config.php, resulting in the vulnerability. The same refactor removed authentication logic from other files and correctly added the appropriate authentication type to the component_config.php file."

They said: "We have reviewed log files which we've received from affected customers to understand and characterize the attack. The log files we reviewed show that the attackers directly connected to the affected My Book Live devices from a variety of IP addresses in different countries. Our investigation shows that in some cases the attacker exploited both vulnerabilities on the device, as evidenced by the source IP. The first vulnerability was exploited to install a malicious binary on the device, and the second vulnerability was later exploited to reset the device."

And then, finally, later they reiterate as they conclude their posting: "For customers who have lost data as a result of these attacks, Western Digital will provide data recovery services." And we believe that those are free. They said: "My Book Live users will also be offered a trade-in program to upgrade to a supported My Cloud device." And of course we'll be discussing My Cloud in a minute. Watch your step. "Both programs will be available beginning in July, and details on how to take advantage of these programs will be made available in a separate announcement."

So overall, this impresses me. In the first place, we learn how and why that authentication bypass was introduced into the devices. That wholesale commenting out of the access authentication that was seen last week was troubling in the extreme. But their refactoring explanation makes sense, complete sense. And I can see how a coder would have easily intended, but ultimately failed, to apply the alternative authentication protection which the designed system provided. That's exactly the way these mistakes are made.

And WD's willingness to take responsibility for a device which it was selling 11 years ago, back in 2010, which has not been supported for the past six years, I think says a great deal about the company's management. So to that I say bravo. I'm sure they found that the apparent data loss from the factory reset was recoverable. So hats off to them for stepping up and offering to get their customers' data back. I'm impressed.

But before we get all choked up and weepy-eyed over WD's willingness to help their My Book NAS users, we need to note that a much larger group of WD users, those who are still using the My Cloud OS 3 edition, which was built into WD's newer My Cloud NAS devices, are today in trouble. It turns out that all My Cloud OS 3 devices - which is a newer set of devices. The My Cloud is what they were offering to trade the Live users' up to. The OS 5 is where they are now. OS 3 has a problem. It turns out that all of the My Cloud OS 3 devices contain a serious remote code execution flaw and that, wouldn't you know it, OS 3 is no longer supported.

This came to light when a pair of intrepid security researchers, and actually several other groups, were all planning to present their discoveries of these problems with Western Digital's current cloud devices during late last year's Pwn2Own competition in Tokyo, back in November. They all had the rug pulled out from them when, five days prior to the

Pwn2Own competition, WD released the completely rewritten My Cloud OS 5 just before, as I said, five days before the competition date. Being a complete rewrite, OS 5 inherently eliminated the bugs that these multiple researchers had hoped to cash in on. Since the ground rules for Pwn2Own require that qualifying software must be the most current, the flaws in OS 3, which had then been obsoleted, were no longer prizeworthy.

Of course, as we all know too well, the fact that OS 5 appeared doesn't spontaneously cause all of the OS 3's out in the world to be updated to the OS 5 firmware. And in fact it appears that not all of the WD hardware that runs OS 3 will even run OS 5. WD has a list of those hardware platforms that will. And even if it did, OS 5's complete rewrite, turns out, left out a number of OS 3's more popular features. So if WD's users of OS 3-based My Cloud devices even knew of the trouble with their current firmware and wished to update, WD would be asking those customers if they were able to update, given the hardware they have, to accept a feature downgrade in order to repair a previous apparently badly broken and now out-of-support OS.

Once again, while WD certainly has the legal right to do whatever they wish with their customers, it's not the best way to earn and maintain a reputation for standing behind one's products throughout their entire useful service life. If My Cloud devices were sold under the condition that, for example, they would run for exactly five years and then self-destruct, it seems unlikely that many people would choose that solution, though that's essentially what has happened here.

In any event, earlier this year, in February, which is a few months after Pwn2Own was going to happen, that research team, who was getting ready to release this, published a detailed YouTube video which documents how they discovered this chain -again, a chain, Leo, as you said - a chain of weaknesses that allows an attacker to remotely update a vulnerable device's firmware to add a malicious backdoor using a low-privileged user account having a blank password. Tens of thousands of devices appear to be vulnerable to that attack today.

So before the Pwn2Own competition, there appears to have been some sort of communication mix-up because the researchers said that WD had never responded to any of their reports. Curious about that, Brian Krebs apparently asked WD what the story was, and he was told, get this: "The communication that came our way confirmed the research team involved planned to release details of the vulnerability and asked us to contact them with any questions. We didn't have any questions."

Leo: We don't have any questions.

Steve: "So we didn't respond."

Leo: Well, there's your mistake. I have some questions now.

Steve: Really? That's what you're going with, WD?

Leo: That's really...

Steve: You didn't answer because they said only call us if you don't have any questions.

Leo: We don't have any questions.

Steve: And then WD continued: "Since then, we have updated our process and respond to every report" - even those that we don't have any questions about...

Leo: Yeah, seems like a good idea.

Steve: "...in order to avoid any such miscommunication like this again."

Leo: It does sound like they've learned their lesson a little bit, I have to say. They took a lot of pain here.

Steve: It seems like they keep - yeah, yeah. They said: "We take reports from the security research community very seriously [uh-huh] and conduct investigations as soon as we receive them." Even if we don't mention it. Right. So, and Brian added that Western Digital ignored questions, apparently from him, about whether the flaw found by the researchers had ever been addressed in OS 3. So they're still ignoring questions that they don't want to answer. Brian reports that a statement published on WD's site, dated March 12, 2021, says that the company will no longer provide further security updates to the My Cloud OS 3 firmware: "We strongly encourage moving to the My Cloud OS 5 firmware," the statement reads. "If your device is not eligible for upgrade to My Cloud OS 5, we recommend that you upgrade to one of our other My Cloud offerings that support My Cloud OS 5."

And we should note that these WD NAS gadgets are not cheap. They weigh in around $500. So telling their users who are stuck with OS 3 for whatever reason to "upgrade" to other WD offerings that support My Cloud OS 5 might be asking quite a lot. In order to save some of the value from all of their research, the team developed and released their own patch to fix the vulnerabilities they had found in OS 3. Unfortunately, the patch needs to be reapplied whenever the My Cloud device is rebooted since it will be returned to its previous unpatched and vulnerable state. Western Digital told Brian that they were aware of third parties offering security patches for My Cloud OS 3, but of course they couldn't stand behind them in any way.

So none of this is really confidence-inspiring, once again. And NAS devices in general appear to be perennially troubled. I love my Drobos, but no way would I ever consider exposing them to the public Internet. They are permanently linked to each other through Syncthing, both safely tucked away behind multiple layers of NAT routing.

And I was thinking about this. If I had to expose a NAS to the public Internet, I would use a well-maintained Ubuntu Linux running NextCloud. And boy, if you haven't, take a look at NextCloud.com/secure if you want to see some guys who have really gone way over the top with security. They have multiple code audits and security reviews, and even - get this - a live video verification option as part of their remote authentication process. You have to get on TV and say, "Hi, Mom. It's really me. See?" And then you qualify for folder sharing.

So anyway, we do see NAS devices as quite a problem. And I ought to also mention, if you do have some need to have a NAS on your network, you should arrange for it to be very much like my PHP server is at GRC, completely isolated from the rest of your network. You may need to get to it, but don't let it get to you. You could put a NAT router between it and the rest of your network so that your network can see it, but it

can't see your network, because this just seems to be a hard thing to get right. And Leo, what is not hard to get right is your choice of sponsors.

Leo: Thank you for that segue. By the way, update. Microsoft has just pushed an out-of-band fix for Windows PrintNightmare.

Steve: Good.

Leo: So if you are - yeah, I think that was the right thing to do, not wait till Tuesday.

Steve: Good. Go get it.

Leo: Yeah.

Steve: Do you have to get it, or will it self-install?

Leo: I presume it's going to self-install. This is from Lawrence Abrams' BleepingComputer. It's KB5004945, and KB5004946, 7, 9, and 50, depending on your Windows version. I would imagine they'll push it. But if you're worried, you might want to check it. But KB5004945 through 4950. So that's good news. That's good news.

Steve: Yes, yes. So I can confirm, as I just did, that the emergency out-of-cycle update is happening.

Leo: Good, good.

Steve: The Win10 machine that I'm talking to you on, I went to Windows Update. And sure enough, I'm seeing Cumulative Update for Windows 10 version - in this case it's 20H2, KB5004945.

Leo: Good, yup.

Steve: And that's the one. So all any of our listeners need to do is just you might have to give Windows Update a little kick, go check for updates.

Leo: Be a seeker, yes.

Steve: And then it'll find it, and you'll be good to go.

Leo: Don't be a sucker, be a seeker.

Steve: And boy, you know, this is a service, as we said, that's running in every version of Windows from time immemorial. So, ugh.

Leo: Need it or not.

Steve: For better or for worse, yes. And that's a good point, too. I mean, since it has been a source of constant problems, and since we already know that there's going to be some more announced during Black Hat next month, seriously, if you don't need the print spooler, turn it off.

Leo: Right.

Steve: You can still print, and you'll be shutting down untold numbers of vulnerabilities in the future.

Leo: Yes.

Steve: Okay. And I was just talking about NASes. While we're on the subject of mass storage, in addition to this week's utterly amazing Picture of the Week, I can report having passed another milestone on the road to SpinRite 6.1. At the end of my workday, day before yesterday, on Sunday, July 4th - I managed to put in eight hours, from 8:00 to 4:00 - I posted the news to GRC's spinrite.dev newsgroup that I had just finished the work on updating SpinRite's SATA/AHCI driver to add the features SpinRite would need to work properly with those controllers.

Up until that point the driver existed, and we were using it in the ReadSpeed Benchmark. Works great. But SpinRite needs for data recovery purposes all kinds of extra hooks into a driver. So it now has those. Last Friday I had finished the work on the similar thing, on SpinRite's PCI Bus Mastering driver. So that means that now all five of SpinRite's new drive-access interface drivers are now written.

And recall that I designed a drive-independent IO abstraction layer to be driven by a new SpinRite core. That core will finally switch SpinRite from its traditional track-based orientation to a linear storage model, which is what everything is today. After today's podcast I will begin implementing SpinRite's new core. It's already designed, and the IO abstraction was expressly designed for its use, so I expect the core implementation to go smoothly. And once that's done, all of the parts of SpinRite that needed redesigning and rewriting will have been. None of that new code I've been writing will have been tested and debugged yet.

So I'll set up test cases and work through the live code to watch it work and verify that in every case it does what I intend. Once it all appears to be working, I'll turn the newsgroup gang loose on it for their testing. And I'm certain we'll be discovering things that still require some tweaking. But we'll kind of be tweaking things. I mean, all of the heavy lifting is done. And at that point we'll be working with on a fully functional pre-release of the finished and final SpinRite v6.1. So things are starting to get exciting.

Leo: Woohoo.

Steve: And speaking of exciting, Leo, last Friday evening, after I had finished that work on SpinRite's new PCI Bus Mastering Driver, Lorrie and I watched and thoroughly enjoyed Amazon's new release of "The Tomorrow War."

Leo: Oh, good, yeah.

Steve: Starring Chris Pratt.

Leo: Loved it, yeah.

Steve: Yes. We did, too. Afterward, of course, we had the inevitable discussion about the paradoxes arising whenever someone arranges to travel backward in time. As we all know, traveling forward in time is no problem at all. But moving into the past creates all sorts of dilemmas. In any event, after the movie I tweeted to my Twitter followers. My tweet read: "Buckle up. If you have access to Amazon Prime and enjoy sci-fi action movies, I can recommend Chris Pratt in 'The Tomorrow War' - nonstop action, fun, astonishing special effects. How did they do those alien monsters?"

Leo: Those were pretty - I was thinking the same thing. Obviously CGI, but wow.

Steve: Oh, Leo. Well, yeah. And the actors are like, they're like interacting with nothing.

Leo: Right.

Steve: I mean, it's like it was astonishing.

Leo: Yeah.

Steve: Anyway, I wrote...

Leo: Actors are getting really good at interacting with nothing, by the way. That's the new skill, I think.

Steve: Yeah. I think so. And certainly Chris Pratt is because he has a lot of costars that couldn't possibly exist.

Leo: Yeah.

Steve: Like Groot. Anyway, I can't imagine, I said, that it would disappoint. With very few exceptions, the replies from those who were motivated to watch the movie as a consequence of my tweet were similarly very positive. In fact, Jason Hudson tweeted that he was immediately watching it a second time. And I get that, because it was a romp. There were a few "meh" replies. But one Twitter follower, Houdini7, was the least

impressed of all. He wrote: "I found it so full of plot holes and trivial clichs, I felt it was one of the worst movies I've ever seen."

Leo: Wow.

Steve: I know. So I suppose that Houdini7 has been quite lucky, Leo, with his movie choices throughout his life.

Leo: Because there are worse movies.

Steve: Because, oh, my lord, I have definitely seen a great many way worse movies. Nevertheless, IMDB does peg it at a 6.7, which falls below my normal 7.0 threshold of worthiness. So is it, as Houdini said, full of plot holes and trivial clichs? Absolutely. And yet we still found it to be wonderfully fun. And I guess, you know, when it comes to these kinds of movies, I'm a proud 10 year old. So for any other 10 year olds at heart, if you're in search of a deeply cerebral experience, you'll likely be as disappointed as Houdini7 was.

Leo: No, it's an action flick. You know.

Steve: Yes. But if you're looking for a wonderful sci-fi romp, I believe that I can safely encourage you not to miss Amazon Prime's "The Tomorrow War."

Leo: Nice.

Steve: And so apparently you and Lisa also...

Leo: We enjoyed it, yeah, yeah. It was fun. It was very loud.

Steve: I thought it was a lot of - yeah. Okay. The Kaseya Saga. Kaseya? Yeah, that's how we'll pronounce it.

Leo: Yes, Kaseya.

Steve: Kaseya. Okay. So before we plow into the saga, I wanted to share a little bit of interesting trivia. I found a Q&A interview which first appeared on October 23rd of last year. It was conducted between - they call themselves "Russian OSINT," Open Source Intelligence, between them and a member of the REvil gang. The link to the entire dialogue is in the show notes, for anyone who's interested. The interview was titled "Uncensored Interview with REvil / Sodinokibi Ransomware Operators," and most of what's there we already know.

But at one point the Russian OSINT interviewer asked: "What does the R prefix in the word REvil mean? Is that the word Reborn?" The REvil interviewee replies: "Ransom Evil. The thought came from Resident Evil." Now, I'd imagine that all gamers are familiar with

Resident Evil, also known as Biohazard. It's an older Japanese videogame series and media franchise which was created by Capcom, featuring plot lines and bio weapons and viral incidents. And, yes, I also very much enjoyed the many spinoff Resident Evil movies, too - because, as I said, it's sometimes fun to be 10 years old.

But a few other interesting tidbits arose from their much longer interview. And I've got a little - I've got, what, one, two, three, four, five, six back-and-forth Q&As. Russian OSINT asked: "Have you ever had problems when it was not possible to decrypt encrypted files after receiving a ransom? That is, something went wrong, and you yourself could not do anything?"

The REvil guy said: "Yes. If you have previously tried to use third-party data recovery software. If at least one bit of the file is modified, the key will be lost. Especially often this happens with antivirus. It simply deletes notes, and they contain keys." He said: "I say openly, such cases are extremely rare. I remember only 12 for the entire time of work. And of course we never took money. The note contains a warning to the victims. If they don't read it, their difficulties."

Russian OSINT: "Which industries are currently the 'fattest' for ransomware attacks? Where is the most profit?" REvil replies: "IT providers, insurance, legal firms, manufacturing - especially, oddly enough, the agro-industrial complex."

Russian OSINT: "You don't do any hacking and fixing into the infrastructure with your own hands. Your partners do it; right?" And REvil said: "We have our own flying squad, and we also have partners. We do this and that."

And, finally, Russian OSINT asked: "A recent report from Microsoft said that two extreme effective attacks for introducing ransomware are brute force and RDP hacking. How, do you think, will attack vectors change over time?" The REvil guy replied: "Brute force has been alive for 20 years. And he will be alive. RDP is the best vector. Especially the fresh BlueGate vulnerability will hit him very hard." So the word from REvil.

Okay. So what's the back story behind this biggest ever, record-breaking, single ransomware event? Let's begin with who is Kaseya? They're an international IT solutions provider based in Dublin, Ireland, with their U.S. headquarters located in Miami, Florida. And they maintain a physical presence in 10 countries. Among the IT solutions offered is something they call VSA. It's a unified remote monitoring tool for managing networks and endpoints. This VSA software is aimed at enterprises and managed service providers, and Kaseya says that over 40,000 organizations worldwide use at least one of their solutions.

Last week I was noting that MSPs are a very potent source of ransomware intrusion since, as we saw in that case of a managed service provider to dental offices, a single intrusion at an MSP could expand downward into all of that company's clients and customers. Essentially, all of an MSP's clients have extended their networks into that common service provider. And as we often like to rhetorically ask on this podcast, "What could possibly go wrong?"

What went wrong in this instance was that, just as MSPs serve many clients, many MSPs are using a single common VSA server provided by Kaseya, and that VSA software contained a number of zero-day vulnerabilities that were being leveraged by a clever and determined REvil affiliate. On July 2nd, at 2:00 p.m. Eastern, Kaseya's CEO Fred Voccola announced what he called "a potential attack against the VSA that has been limited to a small number of on-premise customers." Uh-huh. That has turned out to be nearly 40 of Kaseya's MSP customers, each of whom had many clients.

Two days later, by the 4th of July, day before yesterday, Kaseya had revised its estimate of this attack in its severity, calling its software "the victim of a sophisticated cyberattack." Apparently the truth is that Kaseya's CEO wishes that a sophisticated cyberattack was responsible. But as we learn in a minute, it was apparently embarrassingly trivial. FireEye's Mandiant team, in addition to several other security companies, were called in to help get a grip on the situation. Kaseya posted that: "Our security, support, R&D, communications, and customer teams continue to work around the clock in all geographies to resolve the issue and restore our customers to service." In other words, they knew they had been the vector of a serious problem.

The FBI described the incident as a "supply chain ransomware attack leveraging a vulnerability in Kaseya VSA software against multiple MSPs and their customers." Huntress has tracked 30 MSPs involved in the breach and believes with high confidence that the attack was triggered via an authentication bypass vulnerability in the Kaseya VSA web interface. And in a Reddit explainer, Huntress further added that an estimated 1,000 companies - and Leo, you have newer news. Now we're estimating that at 1,500.

Leo: Yeah, yeah. I'm sure that's not the end of it. It's going to be more, yeah.

Steve: Yup, yup, have had servers and workstations encrypted and noted that it's reasonable to suggest thousands of small businesses may have been impacted. Sophos has said that: "This is one of the farthest reaching criminal ransomware attacks that Sophos has ever seen. At this time, our evidence shows that more than 70 managed service providers were impacted, resulting in more than 350 further impacted organizations." And I don't know further to what. They said: "We expect the full scope of victim organizations to be higher than what's being reported by any individual security company." Because inherently this is, right, a distributed attack with distributed reports.

The REvil affiliate's discovery of vulnerabilities in Kaseya's VSA offering allowed them to cause malicious update payloads to be sent out to all of the devices being managed by each compromised Kaseya VSA server. Using this malware delivery channel cleverly provided the REvil malware with cover in several ways by supplying the initial compromise through a trusted channel, and leveraging the trust in the VSA agent code.

And get a load of this. Kaseya requires that its software agents running in their clients' systems be given antimalware exclusions for its application and its agents' working folders. That means that, thanks to those exclusions, anything executed by the Kaseya Agent Monitor in its clients' machines is allowed to run and is ignored by any antiviral protections. And once again, what could possibly be wrong with that strategy? It was these explicit exclusions which Kaseya requires that allowed REvil to deploy its dropper without any scrutiny in these thousands of client systems worldwide.

For these reasons, Kaseya's VSA solution platform was a perfect foil for REvil. Among other functionality of VSA is the deployment of software via these agents and automation of IT tasks. As such, VSA agents and their actions obtain and run with a high level of trust on customer devices; right? Trust what it does. Turn off antivirus because we were getting some pesky false positives on our IT automation, and we don't want those. We don't want pop-ups. We just want, you know, VSA should be able to do whatever it wants.

By infiltrating the VSA server, any attached client will perform, without question, whatever task the VSA server requests. Security analysts have suggested that this is probably one of the reasons why Kaseya was targeted in the first place. In other words, the REvil affiliate who managed to infiltrate Kaseya almost certainly did it deliberately because they appreciated the size and power, the scope of the attack that they would be

able to achieve. In that sense, it's very much like the attack against the SolarWinds; right? They realized, if they got into SolarWinds, they'd be able to push it out to all of SolarWinds' many customers via their update mechanisms.

Leo: Nothing like a supply chain attack, man.

Steve: That's right, baby.

Leo: Higher up in the food chain you're going to get more results, yeah.

Steve: Exactly. So as we all know by this time, that clever REvil affiliate was correct. In one headline-grabbing instance, the Swedish supermarket chain Coop was forced to shut down some 500 of its stores after those stores' retail checkout cash registers all stopped functioning en masse. And now we learn that Kaseya was aware of the zero-day vulnerabilities in its systems at the time of these attacks. I know.

Leo: That's frustrating.

Steve: On Sunday, the Dutch Institute for Vulnerability Disclosure (DIVD) revealed that it had alerted Kaseya to a number of zero-day vulnerabilities in its VSA software, and that it said they were being exploited as a conduit to deploy ransomware. DIVD indicated that Kaseya was in the process of testing fixes for VSA under coordinated vulnerability disclosure - and who knows how much time DIVD had given them - when the July 2nd attacks took place.

Although DIVD revealed no specifics about the flaws they had discovered, DIVD's chairman, Victor Gevers - and he's a young guy. I watched an interview of him. I couldn't understand what he was saying. But he suggested that the zero-days were trivial to exploit. And he tweeted, in English: "If I would show you the PoC [the proof of concept], you would know how and why instantly."

The attacks, of course, caught these researchers and Kaseya by surprise, and probably in horror. Since the immediate solution was to get all Internet-exposed VSA servers offline, DIVD has been providing a list of publicly accessible VSA IP clients, the IP addresses and customers' IDs to Kaseya to help that to happen. This effort led to a dramatic decrease in publicly accessible servers, from a starting count of over 2,200 known online exploitable VSA servers to now only 140 which are known to still be accessible today. Now, of course, those are not all MSPs. I'm sure they had many end-user customers, as well. But the MSPs were the big juicy ones because, again, supply chain. They were the tip of a larger iceberg of exploitability.

And this brings us to the curious case of the ransom demands, which appear to be far more sophisticated than we've seen before. The nature of the ransom offers and their negotiations, which appear to center around file extensions, networks, and wholesale attacks, has raised questions for me about the details of the Sodinokibi ransomware. I was wondering what design architecture would allow them to pull off what they were offering to do in terms of ransom response granularity. So I spent some time digging into it, and I was quite surprised by what I found. As a consequence, next week's podcast is already titled "REvil's Clever Crypto," where I plan to lay out the amazingly sophisticated cryptographic design of this king of the ransomware hill.

Here's what we've learned. We've learned that the files of the individual MSP victim clients, right, the ultimate end-users, were probably not exfiltrated before their encryption. So there's that. Probably just because there were too many of them. And Emsisoft's CTO Fabian Wosar said that MSP customers who were affected by the attack received initial ransom demands of $44,999. Now, I was wondering why we were seeing weird pricing of non-whole numbers, like remember, Leo, $1,000 shy of $22 million for the Irish health attack. But then when I see 44,999, I'm thinking that it's imitating retail pricing.

Leo: So it's not quite 50,000.

Steve: Yeah, we're not asking 45,000 here.

Leo: It's a deal.

Steve: We're giving you a bit of a bump here. We're only going to take $44,999. It's a bargain.

Leo: It's nonsense because nobody's making a buying decision. I mean, that's nonsense.

Steve: Right. Upon closer inspection, however, so it appears that the 44, well, we'll call it 45,000 for ease, ransom is "per file extension," and that REvil's Sodinokibi often encrypts files with many different extensions. So I don't yet know what that's about. Perhaps they're saying you can have all your DOC files decrypted for $45,000; but if you also want your SQL databases back, that'll be another 45,000, please, and so on. It's not clear, however, whether the file extensions of the encrypted files are the same as their original non-encrypted extensions, their real extensions, or whether they may be something assigned by the malware. There was something I read that led me to believe that it might be a way of offering to decrypt some specific files or a proportion of all files. But as far as I know, this is the first instance we've seen of what you might call "itemized file decryption by extension."

Then, moving up a level, the REvil affiliate also apparently has the ability to decrypt by MSP customer because ransom demands of $5 million, and their payment, would reportedly allow them to decrypt all of the files regardless of file extension, yet presumably not those belonging to any other of an MSP's customers. So you can see what I mean when I say that, if this is true, there's some fancy and cool hierarchical crypto happening here.

And there's yet another level. The REvil gang posted the following message to their wonderfully named "Happy Blog." The title of the blog posting is "Kaseya," and they've got it spelled right, "Kaseya Attack Info." They wrote: "On Friday, 2.07.2021, we launched an attack on MSP providers." Now, they said, "More than a million systems were infected." Okay, no. No one thinks it's that many. But fine. "If anyone wants to negotiate about universal decryptor, our price is $70 million in bitcoin," yeah, U.S. dollars in equivalent bitcoin.

Leo: That's retirement money.

Steve: That's right. "And we will publish publicly decryptor that decrypts files of all victims so everyone will be able to recover from attack in less than an hour. If you are interested in such deal, contact us using victims' 'readme' file instructions."

Leo: Such a deal.

Steve: Wow. 70 million, and everybody gets decrypted. But what this means is that it's possible for the entire encompassing multi-MSP Mary Kay pyramid distribution model of malware to, like, work for everybody, but then also to have a per-victim and a per-file extension decryption for varying levels of payment. So a very interesting system. And I look forward to digging into it further and providing our listeners with a deep dive into the technology of REvil next week.

So one thing should become very clear. Given the nature of this attack, very little of our networked software has been put under the sort of scrutiny and attack that it is being and will be subjected to in the future. And unfortunately, this is the shape of that future.

Leo: Well, well, well. What do you think the number will be eventually?

Steve: How about maybe twice what we've seen, so 3,000 clients?

Leo: The 1,500, I was just looking, comes from Kaseya's own CEO. So, yeah.

Steve: Okay. So, yeah. And also, so that would be 3,000 companies, each of whom has probably had lateral movement within their network.

Leo: Right.

Steve: So that could be 50 machines in a company.

Leo: Right.

Steve: So we could see that multiplied up. I mean, it's a mess.

Leo: Well, and we've been talking about supply chain since way back when, when that Supermicro story came out from Bloomberg.

Steve: Right.

Leo: About potentially this modification of the Supermicro motherboards. It was undetectable. And the conclusion of that is whether or not that happened, that supply chain attacks are going to be the wave of the future. And they're almost impossible to stop. And they're leveraged; right?

Steve: Yup.

Leo: Because you get Kaseya, you get everybody who uses Kaseya. So, boy, you're right, I don't think this is the end of that. This is just the beginning, yeah. And nobody's, you know, I mean, what do we do? You start over? You can't throw everything out. What are you going to do?

Steve: Yeah.

Leo: Steve Gibson, as always, thumbs up, aces. We do this show every Tuesday, 1:30 Pacific, 4:30 Eastern, 20:30 UTC. If you want to watch us do it live, TWiT.tv/live. There's live audio and video there, and you can also chat with us live at irc.twit.tv. Steve keeps copies of the show at his website, GRC.com. Besides the normal 64Kb audio, there's 16Kb audio for people with limited bandwidth, or bandwidth caps they don't want to exceed.

There's also, and Steve commissions this, so he should get all the credit for it, a very nice transcript of the show, which aids in two ways. One, a lot of people like to read while they listen. It helps with the comprehension. But, two, you can search it and find the shows you're looking for much more easily. Thanks to Elaine Farris for doing that. GRC.com. While you're there, it's getting close, time to pick up SpinRite 6, 6.1 on its way, getting close.

Steve: Yup.

Leo: I can feel it. And if you buy 6.0 now, you get a free upgrade to 6.1. All of that at GRC.com, along with other free stuff.

Steve: I'm dreaming about code now.

Leo: Yeah, that's a sign you're doing it a lot; right? It's in your head.

Steve: It's like, it's in my head, yeah.

Leo: You know, it's funny. Every year I attempt and fail a coding challenge called the Advent of Code, which is really fun, but I've never completed the whole thing. But the problems are such that often I just go to - I say, okay, I got it, I'm going to bed, hoping, and sometimes it actually works, I'll wake up with, oh, the insight. You really do work in your sleep on stuff like this. And if you've got kind of a debugging challenge, or just some coding challenge...

Steve: Well, and that's where the famous expression "sleep on it" comes from; right?

Leo: It works. Yeah, it really works. Let's see. We have of course the show at our website also, TWiT.tv/sn. There's video there, as well, if you want to watch us. It's kind of boring, but you can. There's also links to the YouTube channel because

there's a Security Now! YouTube channel, to the downloads, and all the podcast players you can use to get it automatically. In fact, if you do use a podcast player, and they offer reviews, please leave Steve a five-star review. Really we want the world to know this resource exists for everybody, for free.

Let's see. I think that concludes this session. I hope you all are enlightened and will go and run down your print spooler update. Thank you, Steve. Have a great week. See you next week on Security Now!.

Steve: Ciao, buddy.