SECURITY NOW!

Transcript of Episode #821

Epsilon Red

Description: This week we begin by examining the recent advances made by the just-released Chrome 91, and revisit Google's configurable long-term activity logging. On the ransomware front we look at yet another likely addition to the ransomware ecosystem: trusted third-party file decryptors. We anticipate next week's activation of the Amazon Sidewalk ultra-wide area network, look at the questionable claims of another massive cyberattack, and at WhatsApp's privacy struggles with India and Brazil couldn't happen to nicer folks. Then we'll touch on just a single bit of trivia before plowing into a detailed examination of the operation of the newest ransomware in town: Epsilon Red.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-821.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-821-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. Lots to talk about. Chrome 91 has some interesting new features that command line heroes will really enjoy. We'll talk about new ransomware. It's called Epsilon Red, and it apparently is mostly written in PowerShell? Plus a revisit to Amazon Sidewalk and why maybe you don't really want to turn it off. It's all coming up next with Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 821, recorded Tuesday, June 1st, 2021: Epsilon Red.

It's time for Security Now!, the show where we cover your security and privacy online with this guy right here, Mr. Steve Gibson. It's the musical.

Steve Gibson: For those of you don't have video, Leo is pointing at me on the screen.

Leo: I am. It's the greatest showman, ladies and gentlemen. We're doing a musical version.

Steve: I am here by voice or vision or whatever. So we're at June 1st, and lots of fun stuff to talk about. We're going to begin by examining the recent advances made by the just-released Chrome 91. Oh, and Leo, after I finished the show notes, I saw that Firefox just got its major expected facelift.

Leo: Yeah. Yes.

Steve: So I restarted my Firefox, and it's like, ooh, that is nice looking. So, yeah, that happened, too. We're also going to revisit briefly Google's configurable long-term activity logging, which sort of ties into Chrome 91. On the ransomware front, well, actually I skipped over the mention of the fact that this podcast 821 is titled Epsilon Red, which is the name of a, just discovered last week, yet another ransomware strain.

This one is really weird, though. And we have first of all a lot of information about it because it's easy to know a lot about it, for reasons we'll get to. And it just sort of also maybe suggests that we're seeing another change in this whole ransomware world. And of course changes keep happening every week because, unfortunately, it's a happening place. But before we get to that, we're also going to take a look at yet another likely addition to the ransomware ecosystem up at the top of the show, which seems to be emerging, which I guess I would call "trusted third-party file decryptors."

Leo: Oh, geez.

Steve: Yeah, I know. It's crazy. We're also going to anticipate next week's activation of Amazon's Sidewalk, which we talked about in early December of last year, 2020, Amazon's ultra-wide area network, using that LoRa 900 MHz radio stuff.

Leo: I've invoked your name several times in our discussion of it because you talked about it late last year and gave it kind of a preliminary, anyway, seal of approval.

Steve: Yes. From a technical standpoint, I think they did everything right. And of course now the tech press, well, and even the less tech press is jumping up and down screaming about...

Leo: Turn it off, turn it off, turn it off, turn it off.

Steve: Exactly, exactly. So we're going to revisit that. Also we're going to look at the questionable claims of another massive cyberattack. Microsoft got a lot of press last week saying, oh my god, 150 corporations have been attacked. It's like, okay, not really. And WhatsApp's privacy struggling is happening with India and Brazil, you know, couldn't happen to nicer folks, so we'll touch on that. I've got just a tiny bit of trivia, and then we're going to, as I said, plow into a detailed examination of the operation of the newest ransomware in town that has named itself Epsilon Red. And of course we do have a fun Picture of the Week. So I think 821 will be another good podcast.

Leo: Busy, busy, busy.

Steve: We have a picture of soup, looks like chicken noodle soup because it's got, like, I see little chicken bits and some carrots. But mostly it's star-shaped noodles filling the bowl. And of course you'd think, okay, how is that a picture for Security Now!? Well, the caption is what brings it all home. It says: "When your alphabet soup is password protected."

Leo: Then it's all little stars.

Steve: You can't see any of the letters. All you get is little stars.

Leo: I love it.

Steve: And it's like, hmm, yeah. Anyway, I thought that was a kick. Somebody sent it to me. Thank you, whoever you are, you nameless follower.

Leo: Meme maker.

Steve: I do appreciate it. Okay. So Chrome last week moved to 91. I needed to trigger an update, despite the fact that I sort of - like I always have Firefox open. That's my background, tabs down the left-hand side, always open. But I'm finding like I'll just jump to Chrome when I'm just doing sort of temporary things, a few tabs across the top, like when I want to go to GRC's forums, or TweetDeck lives on a tab in Chrome. So it's just it's easy for me to do that. So I'm, like, opening it, and I'm in there all the time. Yet it still doesn't update itself until I go About Chrome.

So they talk about we'll be rolling this out over the next couple weeks. And I guess that's what "rolling it out" means is that, if you happen to go looking for the new version or see where you are, then it's like, oh, okay, yeah, hold on a second, and then you get it. Otherwise you'll get it sometime. Anyway, so presumably it's going to be gradual. As of last Tuesday, all of the channels, the three different levels, have advanced by one. So the stable desktop channel gets 91. The beta gets 92. And the Canary, built constantly, gets 93.

The release announcement shows that Chrome 91 for the desktop fixes 32 security vulnerabilities, eight of them designated as high severity. So, what, one in four; right? Eight of 32. And of those 32 vulnerabilities which were fixed, 21 were reported to Google by external security researchers. And there's money to be made doing this, as we've talked about in the past. The researcher who reported a heap buffer overflow in Chrome's autofill earned themselves $20,000 for that little reported discovery. And that was one of the eight high-severity problems.

But even a report that Chrome rated as low severity, which was an out-of-bounds read in the V8 JavaScript engine, netted its discoverer $15,000. And there were a bunch of $3,000, $5,000, and $7,500 awards. So just kind of keep in mind that it might be possible to pay some bills while helping to make Chrome a bit safer for everyone, if you're someone who likes to poke around at this stuff.

Chrome 91 supports for the first time the use of the clipboard for pasting content into the browser. Like, for example, maybe it would be handy to have in webmail. Until now, data transfer could only be done using drag-and-drop. It was not possible to use a CTRL+C or CTRL+V to paste into the web browser from the clipboard. 91, I guess they figured out how to convince themselves that they were able to make that safe and not have it prone to abuse. So we get that in Chrome 91. And also they brought down now to the shipping release that additional protection of NAT slipstreaming. We talked about how they would be adding the block of port 10080. Remember that's that whole NAT slipstreaming problem. It was going to be coming soon, even though Firefox had been blocking this thing, that particular port 10080 since last November. Chrome finally said, okay, we're convinced that we need to do this. So that landed in 91.

There's also more good news for Chrome and for all Chromium browsers. As a result of a new JavaScript compiler and the use of the new way of optimizing code location in memory, Google is reporting that Chrome 91 will execute, that is, the Chrome we can all get now, executing JavaScript code 23% faster.

Leo: God, that's amazing. I don't know how they - it's incredible, yeah.

Steve: Isn't it? And that was exactly how I felt because, you know, they keep doing this; right? We've already had a bunch of surprising code improvements. The product manager, Thomas Nattestad said: "In 91, Chrome is now up to 23% faster with the launch of a new Sparkplug compiler and [what they referred to as] 'short built-in calls.'" He says - I got a kick out of this instrumentation. They said: "These save over 15 years of our users' CPU time each day." So it's like, whoa.

Leo: That's a lot of nanoseconds. Wow.

Steve: That's like you're going back in - you have to be going back in time in order to save 15 years in CPU time per day. Of course they mean aggregated over all of the use of Chrome. But still. He said: "Sparkplug is a new JavaScript compiler that fills the gap between needing to start executing quickly and optimizing the code for maximum performance." And I dug into this a little bit. Essentially, they're not doing that much optimization because optimization takes time when you could already be executing. So let's not worry about it too much. Let's get started doing something.

And then their short, built-in calls optimize where in memory, he said, "we put generated code to avoid indirect jumps when calling functions." This is all sort of it gets involved with 32- and 64-bit code where the length of the pointer determines how far you're able to describe a relative jump. And so if you're smart about packing where you need to go based on where you are, then if you need to go a shorter distance, you can use shorter pointers, and that ends up being faster.

So anyway, I dug into both of these new features to see whether there was anything that I could usefully report back to our listeners that would, like, fit in a podcast. But they both involve such deep computer voodoo - and that's not doo-doo, that's voodoo - and machine-level architecture considerations, that after coming back up for air, the only thing I can meaningfully summarize is to say wow, I'm sure glad these guys are on our side, and that we get the benefit of their apparently endless amazing technology for free. I mean, this browser, you know, the Chromium browsers, and of course Firefox is managing to keep pace, they just keep giving us more.

Since I couldn't just leave it at that, for anyone who is interested in how it could be possible - exactly following your immediate reaction, Leo - to still find another 23% to squeeze out of an already squeezed and resqueezed system, I have included links to the deeply technical articles I found in the V8.dev blog, which document and describe exactly what Sparkplug and short built-in calls accomplish, and how. So they're on page 2 in the show notes, for anyone who is interested. Again, I can't, like, get into it here. But if you have an interest in how this could still happen, and maybe, for example, in the depths of code-on-the-fly JIT compilers and the tradeoff between optimizing more versus getting something done, rather than keeping the person waiting, it's all there.

We've talked previously about Chrome's decision to begin enhancing the URL field with commands. And, you know, I'm not sure about this. It's possible to type "delete history" into the URL, or "wipe cookies," or "edit credit card," or "update card info," or "launch incognito mode," or just type "incognito." You can also enter "edit passwords," "update credentials," "update browser," like instead of going to About Chrome or Update Google

Chrome. I think maybe I should try just saying "update browser" next time and see if I can give it a little kick in the butt. Anyway, I could have used either of those last two, like "update browser" or "update Google Chrome," before doing the About Chrome thing, if only I'd remembered. Perhaps next time.

But that's also the trouble. I mean, the reason I'm wondering about this whole approach, anyone who's used the command line, like someone who immediately opens Terminal in Linux, we already understand - and I know you do, Leo - the power of the command line. It is arguably the most powerful way of getting things done. But it assumes a certain level of commitment and memory and interest and expertise.

Leo: I don't think most people are ever going to do it.

Steve: No, no. And meanwhile, as we know, the world has moved to multilevel nested discoverable menu systems. That's what everybody wants is just, you know, let me click in here and browse around, see what my options are. And then if there's an arrow that looks like I'm getting warm, let's go down that hole and see what's there. So unless you are clearing cache or wiping cookies often, and perhaps you are, to me it seems unlikely that you're going to hold seldom-used URL bar commands in your head.

Leo: Here's my guess. This is for support. This is so a support person can say, okay, type "delete history" in your command - although I have to say my experience has been, when I tell somebody to do something in the URL bar, they say, "What is that?" I mean, they don't...

Steve: Right, right.

Leo: The address bar, they don't really know. But if you can get over that hurdle, like there's a place where you type on the browser, type "delete history" on that, I think that's probably what they anticipate. And then people like us maybe will remember it and use it.

Steve: I've told the story of my realtor, who is a very good friend, who didn't understand that the Internet was not "The Google."

Leo: Right, right.

Steve: I mean, like she just - she asked questions of "The Google." And when I tried to tell her once, go type in http:, she's like, "What? Into the Google?" Okay, Judy, okay.

Leo: I've had that exact experience, yeah.

Steve: So in any event, the reason I bring all this up today is that the Chrome folks apparently think that they're really onto something with these URL commands. So back at the beta level of Chrome - this is not in Chrome yet, but it's coming - you can now type, or will be, well, in beta you can, and soon the rest of us, if we care. Get a load of this, Leo. "Run Chrome safety check."

Leo: Wow.

Steve: That's one. Or "create doc." You can actually type "create doc," which would immediately create a new doc in Google Docs, which, like, seems to be a stretch to me. But okay. Or "manage Google account." So it's becoming like they're tying it in more tightly into Google services, which you access from the Chrome URL. Which, again, it's like, uh...

Leo: They're nerds. They're just nerds, and they want to do it themselves, and that's crazy.

Steve: Though a more Google Account feature than a Chrome feature, I thought that our privacy-conscious listeners might also like to know that Google Accounts MyActivity monitoring page can now be password protected. So if you go to - and this is the way we do now. I guess you'll be able to go to Manage Google Account eventually.

But right now, myactivity.google.com/myactivity. Okay, that's not easier, certainly. But anyway, I went there last night. And sure enough, I was immediately prompted with a "Safer with Google" balloon which gave me the option for the first time of password protecting the MyActivity page, which uses the link in the show notes.

So their whole point is that, if you're sharing a machine and sharing Google with some lookie-loos who might be poking around to see what you've been up to, maybe you'd like to password-protect the page. Now, I don't think I've ever looked at MyActivity, though I know we've talked about this before. But we're again on the topic. And while we are, there are two other options to consider. First of all, you can opt to have Google auto-delete your activity once it ages to either three months or 18 months or 36 months. Or against the threat, which they caution you about, of receiving a less personalized web experience, you can instruct Google not to save any data at all, thank you very much.

And the last time I visited this page I apparently set it to auto-delete after 18 months, for some reason wanting to keep my personalized experience. But in revisiting it yesterday for the podcast, I decided that I could live with a less personalized web experience, all things considered. So I've instructed Google to delete everything and to no longer save anything. I really wasn't worried about anyone seeing what I had previously been searching for, but it's nice to remember that Google is keeping all of that history unless you tell them not to.

So it may come as no surprise to anybody, but for anyone who doesn't know, you can go to your MyActivity page, and you can say, you know, forget after 90 days, or just maybe don't save it at all. And at the risk of not having ads quite as closely tailored to you as Google seems to think they are, although I've really never really noticed the effect.

Okay. As our main topic today, we'll be taking a close look at Epsilon Red, a curious, for reasons that will become clear later, newly discovered breed of ransomware. But something else is emerging from the ransomware ecosystem that's worth examining. The other ransomware news of note, despite ongoing attacks here and there that don't really rise to the level of cataclysmic, was the news that New Zealand-based Emsisoft - whom we've referred to recently because they're very involved in ransomware. I mean, they're security researchers. They're good guys. They've created their own independent ransomware decryption tool which, when it's provided with the master key from the attackers - you know, no doubt by way of the victim.

You know, the victim pays the ransom. The attackers give the victim the decryption key. Then, should you choose to do so as a victim, you don't have to use the attacker's possibly sketchy decryptor. You can use Emsisoft's independent ransomware decryption tool, which is reputed to be safe and reliable and much faster. It turns out that the decryptors are not very fast. Emsisoft's tool is aware of the encryption employed by 50, five zero, different breeds of ransomware. And it has the added benefit of not having been written by the same people who just finished attacking you, if you're the victim in the first place. Instead, it was written by a reputable security firm.

This means that it's not necessary to take the added time as a victim to have this attacker-provided decryptor reverse engineered, analyzed, and validated to verify that it won't make an already bad situation worse. And it turns out that that's something that responsible victims are having to do. They get the decryptor, and then they find some security firm, and they say, uh, is this safe for us to run? We'd like to get our data back, but we just got this from the bad guys, and we just paid them. So what do we do?

So what's happening is that growing experience with attacker-provided decryptors shows first of all they are not all that reliable. Some inadvertently mangle larger files. They just don't deal with really huge files correctly. And almost universally they decrypt far less quickly than they encrypt. Now, I have no explanation for that, since the bulk data encryption that they would be doing would be by a symmetric cipher. And a symmetric cipher should be symmetric, not only in its keying, but in its performance.

We do know that the bad guys will be motivated to get as much encryption done as quickly as possible since any discovery of their ongoing encrypting operation of course would result in plugs being pulled out of walls as quickly as possible in order to shut down the encryption of whatever it's discovered that they're doing. So it certainly behooves the attackers to optimize their encryption speed wherever possible. But as for decryption, it's easy to imagine that there's no big rush there. They will have obtained their ransom payment. They will have provided a functioning unlock master key and some piece of software which you can apply the key to which will decrypt your files. So they probably feel they've met their obligation. But their victim will still be offline and out of business until presumably all or most of certainly their most important machines have been decrypted, which all reports indicate can take quite some time.

But in both cases of the two high-profile attacks we've recently discussed - the first one of course against Colonial Pipeline and the second against HSE, remember that's Ireland's national public healthcare system - their respective decryptors, the first for the DarkSide ransomware and the second for the Conti ransomware, which we talked about last week, were too slow to be of use. Colonial Pipeline, after paying $4.4 million in ransom, wound up restoring the bulk of their files from their own backups. It wasn't clear whether they might have selectively decrypted some individual files that had been critically changed since those backups were made.

So an intelligent strategy might have been to restore everything from our own backups, because that we could trust completely, and then where necessary selectively decrypt files that were newer than those backups, which also had critical data, and then make sure that those are properly decrypted. So maybe it was a hybrid strategy. We do know that HSE, Ireland's national healthcare system, used Emsisoft's decryptor which ran at twice the speed of the decryptor provided by the Conti gang and was much more trustworthy.

So what I think we're going to begin to see is yet another component being added to this ecosystem, with faster and far more trustworthy file decryptors being sourced by trusted and well-known security firms. For properly designed encryption, the master decryption key will still be required. In other words, having that decryptor won't help you without the key. But it certainly makes sense for the ransomware attackers maybe to even publish their file encryption formats which, thanks to the miracle of public key crypto, in no way weakens the encryption; right? All of that can be published, and without the key it does you no good. But doing so would serve to further mollify the victims and provide additional assurance of reliable file recovery which the bad guys, after all, are wanting to sell, essentially, as one of their services.

So don't be surprised if we don't see more of this. Emsisoft appears to have a head start, but there's probably some additional revenue for reputable security firms to be making by saying, hey, we've got decryptors for these ransomware products. Give us the key. You can trust the product because we're good guys and we want to help you get your files back faster.

I saw some metrics. In some cases the Emsisoft decryptor was three or four times faster. And if you're talking about thousands of systems, and you're worried about the integrity of them, first of all you want the decryption not to fail, so you want the decryptor to work right. And apparently they don't always. Ryuk's decryptor is known to have problems on large files. And you don't want it to take weeks to get back online if you've got lots of servers. So time is money.

Leo: That's what happened to Colonial Pipeline, I remember. They paid the fine, got the - was it REvil? Got the decryptor, and it was...

Steve: It was DarkSide.

Leo: DarkSide, that's right. It was so slow that they ended up just restoring from the backups and saying, oh, screw it. We'll just move on. How much do these guys charge, though, for their Emsisoft...

Steve: That's a good question. I could not see anything there. I would imagine it's something, but it's probably nothing like the ransom.

Leo: Yeah, but you already paid the ransom. You already paid the 5 million, or 50 million. It would be insult to injury to say, oh, and please, we need $5,000 for the Emsisoft decryptor.

Steve: So here's the problem. Are you going to run the decryptor from the bad guys without...

Leo: Yeah, you don't want to anyway, I'm sure, yeah.

Steve: Right, without paying someone to look at it. So if you're going to pay someone to look at it, why not instead just pay to run a known safe decryptor?

Leo: Exactly, yeah.

Steve: So I do think there is an aspect of economics there that really does...

Leo: It's an interesting niche.

Steve: It is; isn't it? It's weird.

Leo: It just makes you say don't get it in the first place. God.

Steve: Yeah, yeah.

Leo: I know that's not always possible, obviously.

Steve: So my little own show notes title for this next piece was "Stepping Off the Sidewalk." So it was our Security Now! Episode 796, which we recorded on December 8th of 2020, titled "Amazon Sidewalk." It was the topic for the whole podcast. And it presented our typical deep technical dive into the detailed design and operation of Amazon's announced and forthcoming Sidewalk offering. And independent of the creepy feeling that some people get from the idea of enabling bidirectional sharing of heavily encrypted low-bandwidth Bluetooth and 900 MHz LoRa (capital L, lowercase o, capital R, lowercase a, radio) over the participating networks of those in close proximity, we concluded - as you reminded us, Leo, correctly - we concluded at the time that from a technology standpoint, Amazon appears to have done everything right.

Sidewalk is back in the news for us today because Amazon has announced that one week from today, next Tuesday, June 8th, the Sidewalk system goes live. And as we discussed and expected at the time, it will be enabled by default for all those using compatible devices. And that's been an issue of some controversy. So unless individual users preempt its auto opt-in, their Echo speakers, their Ring video doorbells, their Ring floodlight cams and Ring spotlight cams, will be participating in this communal signaling network. Predictably, the click-seeking tech press is jumping up and down in a froth over neighbors stealing our WiFi, which has nothing whatsoever to do with Sidewalk.

Leo: Yeah, I was a little disappointed. Dan Goodin at Ars Technica...

Steve: Yes.

Leo: ...acted as if...

Steve: Yes.

Leo: I thought better of him, to be honest.

Steve: I did, too. I didn't quite shed a tear, but I thought, oh, Dan.

Leo: Yeah.

Steve: Yeah, he was very down on it. And it has nothing to do with anyone sharing anybody's WiFi. As we concluded in our careful analysis late last year, the system's total bandwidth usage is extremely low, only being useful for signaling-class applications, not big media streaming. You can't do that over this. Remember that LoRa, which is this low-bandwidth, long-range radio, it actually uses frequency chirps which are slow to do because you have to chirp the carrier. The good news is it makes it high penetration because it prevents there from being any resonances with the carrier that would prevent the signal from going through. But it means it doesn't have a high bit rate. You can't do a chirp very quickly.

Okay. So it is also quite thoroughly encrypted, in addition to being a signaling-class application, deeply encrypted. So Amazon's intention here is clear. They want the system to be adopted so they've designed themselves out of it. Remember that even they can't see into it the way it's designed. The upside of leaving this thing enabled is you get low-power roaming Bluetooth or LoRa devices able to access an unknown Amazon user's network over a triple-layered, deeply encrypted tunnel, which has - I think what we're going to see is many ultimately compelling use cases as this thing spreads.

And so, Leo, remember you and I were just talking last week about how once upon a time, if not most of us, well, probably most of us, if not all of us, were deliberately running with open unencrypted WiFi networks because we wanted to share our Internet connectivity with our neighbors. It was considered, you know, a neighborly thing to do. It's like, hey, why not? Let's let people use it if they're in the area. And today, of course, we no longer do that because we've learned that's not safe.

But allowing Amazon's Sidewalk to remain enabled is not the same as that at all. The design, which we talked about at the end of 2020 - anybody can go back to Episode 796 and listen to the end of it again, if you want a refresher. The design is clearly intended to absolutely prevent any possible abuse of the system. A roaming wireless device that reaches out and connects to Sidewalk has zero access to the hosting network it's connecting through, just as the hosting network has zero access to the roaming device's data. It was very well designed, and we know how to do this sort of thing now.

You could sort of think of it a little bit like a VPN tunnel that is, like, triple layer protected. And recall from our previous discussion that not even Amazon, as I mentioned, has access to the Sidewalk data. It is still encrypted. Think of the Tor network and successive onion layer routing. It's like that. When Amazon gets it and forwards it to the service provider offering the service that the device at the other end wants access to, it's still encrypted when Amazon has it. And it's only the service provider that is ultimately able to unwrap that inner layer of the onion in order to work directly with the device on a point-to-point basis.

So the hysterical press which talks about yet another intrusion into our privacy is really clueless on this. And, you know, we're beginning to see this more and more. These things are complicated. The example we used last year was the Apple and Google initiative for have these two users been in proximity to each other. It was like, oh, my god, the sky is falling. Even though we looked at it, and it was well designed.

Okay. So all that said, I fully understand that some of our listeners may be thinking, no way am I letting Amazon do this. In that case it's absolutely possible to opt your own devices' participation in Sidewalk out of the network. Under Amazon's - can I say the word, the "A" word? Anyway, we all know the word, A-L-E-X-A. You go to More > Settings > Account Settings > Amazon Sidewalk, and you'll find an on/off toggle. It'll be on until you turn it off.

Leo: Yeah, that's what I think some people, it bothers them that Amazon, knowing that no one's ever going to turn it off, has it on by default.

Steve: Yes.

Leo: But I think they also knew no one would turn it on if it were off by default.

Steve: Correct.

Leo: So why do you think Amazon's doing it? That's the real question. I think people don't trust Amazon, so they assume there's some nefarious intent.

Steve: I can't see any. I really do imagine, if you had a low-energy tag around the neck of your pet, and it wandered off, like away, you would, I mean, how many times have we seen like lost dog and cat posters stapled to telephone poles? That happens.

Leo: And Tile, which was really concerned because Apple was going to eat its lunch with their AirTags, was able to use it, which at least gives it a chance to succeed.

Steve: Right.

Leo: And I was trying to think, is it Amazon using it to track its delivery trucks? But no, I don't think they need that. Are they tracking delivery packages? Well, in order to do that you'd have to put a fairly expensive device with a radio transmitter and receiver in the package. You're not going to do that.

Steve: And, you know, I mean, maybe they've got some longer term game. Remember that it's only the newer devices that have the LoRa. So the whole system falls back to Bluetooth Low Energy unless you've got that newer 900 MHz radio. And they've only been putting it into some of their Ring things recently. So it's also going to take quite a while for this network to achieve critical mass. But I think, you know, how about like an elderly person...

Leo: Oh, yeah.

Steve: ...like "I have fallen; I can't get up."

Leo: Happens all the time.

Steve: Or panic alarm.

Leo: Or, you know, I get regular alerts from elderly people with various forms of dementia who've wandered off, and their family wants to know where they are. You get a little bracelet or a necklace for them, and you will know. And it's pretty accurate location, you think? I mean, how...

Steve: Yes, yes. Because even if it had access to multiple locations, it could do some...

Leo: Triangulate, yeah.

Steve: ...signal strength triangulation, exactly.

Leo: And it goes half a mile. I mean, you only need an Echo device every half mile to have some connectivity.

Steve: And remember, Amazon did an experiment, I think it was in Seattle, where they let their employees take home a Ring. And within, like, a month, there was no square inch that did not have LoRa coverage. The entire...

Leo: And that's what scares people, what you just said. There's no square inch that is not covered by Amazon's special network. I think there's a huge public benefit to this.

Steve: I do, too.

Leo: And Dan Goodin's entire argument on Ars Technica is, well, you know how wireless protocols are often flawed. Well, yeah. But...

Steve: Yeah, have you updated Windows lately?

Leo: The presumption that at some point somebody's going to hack it is what concerns him. And of course that's possible.

Steve: Yeah. So maybe they'll have to fix it. Oh, darn. That's been done before.

Leo: Right.

Steve: By the way, when I turned my Windows 10 machine on to do the podcast, Leo, I had no icons on the desktop.

Leo: Oh.

Steve: They just - they all went away. So I thought, uh, okay. And that was a problem because I use one of the icons to instantly log into our Zoom session. So I just thought, oh, let's just try rebooting. And they came back. So thank you.

Leo: Windows at it again. Well, now Edge has decided that it should remind me every time I use it, you really would like to have Bing as your search engine, wouldn't you?

Steve: Oh, are you getting that?

Leo: No.

Steve: I know.

Leo: I don't want Bing. No.

Steve: No, no.

Leo: It's very annoying, I have to say.

Steve: Okay. So I suppose that after the high-profile Colonial Pipeline attack and the HSE, you know, the Ireland attacks, the press is a bit keyed up for any news of cyber shenanigans. Consequently, when Microsoft announced last Tuesday that another major attack had occurred, although there was really nothing particularly special about this one, the popular press jumped on it as if it was big news. I listened to a number of non-technical newsy shows, and it was like, oh, my god, Microsoft announces 150 different organizations attacked. It's like, okay, what?

So, okay. So where did this come from? Tom Burt, Microsoft's Corporate VP for Customer Security & Trust, triggered all this by writing: "This week we observed cyberattacks by the threat actor Nobelium targeting government agencies, think tanks, consultants, and non-governmental organizations. This wave of attacks targeted approximately 3,000 email accounts at more than 150 different organizations. While organizations in the United States received the largest share of attacks, targeted victims span at least 24 countries. At least a quarter of the targeted organizations were involved in international development, humanitarian, and human rights work.

Nobelium, originating from Russia, is the same actor behind the attacks on SolarWinds customers in 2020. These attacks appear to be a continuation of multiple efforts by Nobelium to target government agencies involved" - I'm having a hard time keeping a straight face, but we'll get there - "involved in foreign policy as part of the intelligence-gathering efforts. Nobelium launched this week's attacks by gaining access to the Constant Contact account of USAID."

Okay. So, yeah. This was a significant phishing attack enabled by the breach of a single mass mailing account at the mass mailing service, Constant Contact. If USAID's account is compromised, as it was, then the result is pretty much guaranteed to be exactly what happened, and with exactly the demographic spread that we saw. This wasn't in any way targeting those specific organizations. The targets were entirely a function of the account that was compromised. Now, okay, perhaps USAID was targeted. That's possible. But were this not tied back to the same group who were behind SolarWinds, though this bears zero resemblance to that amazing work, it would never have made the news.

And by the way, everybody has their own name for these guys. Microsoft wants to call them Nobelium. Okay. But we know them better as APT29, sometimes as The Dukes, often as Cozy Bear.

Leo: Oh, it's Cozy Bear.

Steve: It's Cozy Bear.

Leo: I didn't know that. Oh, okay.

Steve: Yes. I know. FireEye calls them...

Leo: Can we just come up with one name for these clowns?

Steve: Yes. Exactly my point. Exactly. FireEye calls them UNC2452. Palo Alto Networks' Unit 42 refers to them as SolarStorm. CrowdStrike calls them StellarParticle. Volexity calls them Dark Halo, and Secureworks likes to call them Iron Ritual. But, you know, it would be far less confusing if we could all just agree to call them, what, something. Cozy Bear is fine.

Leo: Cozy Bear is well known, yeah.

Steve: Yes. Or APT29. But no. So as I said, otherwise this was just your run-of-the-mill email phishing attack. The email sent to those individuals on the USAID mailing list contained an HTML attachment. When the HTML was opened by the email's recipient, JavaScript in the HTML would write an ISO file to disk and then encourage its recipient to open it. That would result in the ISO file being mounted, at which point an autorun shortcut link would auto execute a DLL contained in the ISO, which would in turn result in the Cobalt Strike Beacon being executed on the system. In other words, yeah, don't click links in email. Right?

Leo: Oh, no.

Steve: Yeah. But since it really did come from USAID and was likely convincing, thus spear phishing, some recipients might have opened the attachment and proceeded to get themselves infected. Again, not good, but not any sort of high-level dastardly sophisticated attack reminiscent of SolarWinds. If we wanted to blame anyone, blame Microsoft. Why exactly is it that opening an attachment in an email can launch an HTML page...

Leo: Oh, good point.

Steve: ...that can run JavaScript, that can write an ISO file to our local machine's mass storage, and then mount the ISO and launch a DLL it contains? How is that ever going to be a safe thing to let users do?

Leo: Yeah. Wow.

Steve: Ugh. In any event, if you happen to hear about Microsoft warning of some huge new attack targeting 150, oh my god, different organizations, yes, those were 3,000 phishing emails sent to the addresses that were reachable from a breach of USAID's Constant Contact account and nothing more. So, yeah.

Leo: Okay. All right.

Steve: We have another instance of, and I just - to me this is fascinating because I have no idea how this is going to settle out, the great encryption struggle. India recently put in place new regulations that would require messaging apps, such as WhatsApp, to trace what they called the "first originator." I don't know how that's different than the originator. You can't have the second originator.

Leo: The second originator. That's a good point.

Steve: But okay. First originator, maybe that's an English translation thing, of messages shared on the platform, thus breaking encryption protections. Since India contains WhatsApp's largest user base by count, coming in at 530 million users, WhatsApp has sued the government of India - good luck with that - over their new Internet regulations. A WhatsApp spokesperson said, very indignantly: "Requiring messaging apps to 'trace' chats is the equivalent of asking us to keep a fingerprint of every single message sent on WhatsApp, which would break end-to-end encryption and fundamentally undermines people's right to privacy." Now, remember who's speaking here; right? They said: "We have consistently joined civil society and experts around the world in opposing requirements that would violate the privacy of our users."

Okay. Wait a minute. Wasn't it WhatsApp that was changing their privacy agreement, in contravention of their original promise to never share data with their parent company Facebook, to now do exactly that? And in doing so triggered a mass exodus from the WhatsApp platform, whereupon they quickly backpedaled? Okay, yeah, well, in any event, India's new legislation reads: "Significant social media intermediaries, which are defined as being platforms with 5 million or more registered users in India" - so, yeah, at what was it, 530 million? WhatsApp qualifies as a significant social media intermediary.

They said: "Providing services primarily in the nature of messaging shall enable identification of the first originator of the information that is required only for the purposes of prevention, detection, investigation, prosecution, or punishment" - in other words, pretty much anything we want - "of an offense related to sovereignty and integrity of India, the security of the State, friendly relations with foreign States" - in other words, if someone asks you who's generated that message. Anyway, "...or public order or of incitement to an offense relating to the above or in relation with rape, sexually explicit material, or child sexual abuse material punishable with imprisonment for a term of not less than five years. Intermediary shall not be required to disclose the contents of any message or any other information to the first originator."

Okay, now, the new legislation also requires the providers of qualifying messaging platforms, that is, pretty much anybody with at least 5 million users, to remove non-consensual sexually explicit material within 24 hours and appoint a resident grievance officer for acknowledging and addressing complaints from users and victims. In other words, getting themselves involved in the content. So this forms another step in the accumulating battle over encryption. States are understandably demanding access to their citizens' communications for the prevention of abuse that is doubtless helped along by having unbreakable encryption. WhatsApp is currently also doing battle with Brazil over their proposed legislation that would "force companies to add a permanent identity stamp to the private messages people send."

So in response to WhatsApp's legal challenge to India's new digital rules on grounds of violation of user privacy - and again, look who's talking - the Indian government last Wednesday said it is committed to the right to privacy of its citizens, but added that it's subject to "reasonable restrictions" and that "no fundamental right is absolute." Unfortunately, mathematics is absolute. You either do the best job possible you can to ensure privacy, and of course encryption makes that possible, and offer it as a compelling benefit of your service, or you don't. So again, states are beginning to say no. Companies are saying yes. And who knows what's going to happen? Wow, interesting.

I just wanted to mention to our listeners that after finishing Book #10 of The Frontiers Saga, Ryk Brown's 30-volume so far, or 30-novel sequence, and yes, it's my third reading, I'm a third of the way through...

Leo: Wow, you love those books.

Steve: I really do. They are just so much fun. I just, you know, I was thinking about this. It's very, for me, it's like music. People listen to music they like, even the same music they like, over and over. And for me it's like that. It's just a form of pleasure. So anyway, Book 10 ended at a good pausing point. And I thought, this is my opportunity. So I've just cracked the cover of Andy Weir's "Hail Mary."

Leo: Oh, good.

Steve: When I wrote the notes, my Kindle told me that I was at 10%. But I got finished a little early today, and as I was waiting for MacBreak Weekly to wrap up, I moved to 14%.

Leo: That's the weird thing about Kindle reading. They don't do page numbers, for obvious reasons.

Steve: Yeah. It's all resizable, yup.

Leo: Yeah. So they tell you a percent, which, you know, you can really tell a Kindle user because that's what they'll say. Oh, yeah, I'm at 14%, not page 58 or chapter 2. Although you could do chapters.

Steve: Well, I have a good buddy who wrote to me last night. He said, "Have you started 'Hail Mary' yet? I'm at 20%." To your point, Leo. And he said, "I think there's a physics problem that I want to discuss with you. But," he says, "I don't want to be a spoiler, so when you get to..."

Leo: 20%.

Steve: Oh, actually "When we know what the black things are," I think is what he said.

Leo: Oh, okay.

Steve: So he said, "Then let's talk." So he's at 20. So by the time I have 6 more percent, that'll happen today, or later today...

Leo: It's hard to put down. It's a real page turner.

Steve: Yes. I really like his writing style and his humor. It's just right for me. So I have no idea what's in store. But anyway, I may be on the other side of the book by next week's podcast.

Leo: Oh, I bet you will. I'd be surprised if you're not, yeah. Now, the guy who's doing all he can to eliminate ransomware, Mr. Steve Gibson. Good luck.

Steve: Thank you, yes. We will need it, collectively.

Leo: Yes.

Steve: The security tech press has jumped on the news of another new player in the unfortunately burgeoning field of ransomware with headlines including, let's see, Sophos said: "A New Ransomware Enters the Fray." BleepingComputer: "New Epsilon Red Ransomware Hunts Unpatched Microsoft Exchange Servers." Silicon Angle: "New Epsilon Red Ransomware Is Targeting Unpatched Microsoft Exchange Servers." Heimdal Security: "Epsilon Red Ransomware Goes After Unpatched Microsoft Exchange Servers." And Security Week: "Cybercriminals Target Companies With New Epsilon Red Ransomware." Okay. So...

Leo: There he is. Epsilon Red.

Steve: Yes, there he is. Boy, you do not - looks like every tentacle has a different bad tool on it. There's like a spinning saw blade and a pincher thing and a flamethrower. Anyway...

Leo: Watch out for the pincher thing, I've got to tell you. That thing hurts.

Steve: Yeah. His name, the name of the malicious group, comes from the Marvel universe. Apparently it's a lesser known character, but it's named Epsilon Red. And, interestingly, it's a Russian super soldier with four tentacles who can breathe in space. Because you know that's handy.

Leo: Oh, yeah.

Steve: If you're going to be in orbit, you don't want to mess with those pesky spacesuits. And besides, the tentacles are really incompatible with wearing a spacesuit. I'm not sure how you're going to do that with all those tentacles.

Leo: You don't want to bring a chainsaw into the spacesuit. That's always a bad idea.

Steve: No. That's not going to turn out well.

Leo: Yeah.

Steve: So what interested me about this was that Sophos encountered this new entry in the field several weeks ago and thoroughly took it apart, well, inasmuch as there was anything to be taken apart. This thing, such as it is, is predominantly - get this, Leo - a collection of PowerShell scripts. Which for me begged the question...

Leo: What?

Steve: Yes. It is mostly PowerShell.

Leo: What? Okay.

Steve: It begged the question, what explains this method of this thing's construction? And upon reflection, if I were to give this ransomware a longer name, I'd call it Epsilon Red Cashing in on a Craze.

Leo: Okay.

Steve: Sophos security researcher Andrew Brant phrased it in his report last Friday: "A bare-bones ransomware offloads most of its functionality to a cache of PowerShell scripts." He wrote: "In the past week, Sophos analysts uncovered a new ransomware written in the Go programming language that calls itself" - so they didn't name it - "calls itself Epsilon Red." In other words, yes, probably Russian and this lesser known super soldier with four tentacles. "The malware was delivered as the final executable payload in a hand-controlled attack against a U.S.-based business" - which is unnamed in their report - "in the hospitality industry" - that's all we know - "in which every other earlier stage component was a PowerShell script."

Okay. Now, based on the cryptocurrency address provided by the attackers, it appears that at least one of their victims paid a ransom of 4.29 bitcoin on May 15th, at the time valued at roughly $210,000. Okay, so they made some money. $210,000, that's not chicken scratch. They wrote: "While the name and the tooling were unique to this attacker" - so the name and the tooling, that is, the PowerShell, were unique to this attacker. Here's what's interesting. The ransom note left behind on infected computers closely resembles the note left behind by REvil ransomware, though it adds a few minor grammatical corrections. There were no other obvious similarities between Epsilon Red and REvil.

Okay. So I assume that Andrew is suggesting here that the purveyors of this new ransomware borrowed the ransomware note used by REvil, but otherwise wrote their own malware, such as it is, in PowerShell, from scratch. So Andrew said: "It appears that an enterprise Microsoft Exchange Server was the initial point of entry by the attackers into the enterprise network. It isn't clear whether this was enabled by the ProxyLogon exploit" - which of course were the things that were patched in March - "or another vulnerability." He wrote: "but it seems likely that the root cause was an unpatched Exchange Server. From that machine, the attackers used WMI" - Microsoft's Windows Management Instrumentation - "to install other software onto machines inside the network that they could reach from the Exchange Server."

He said: "During the attack, the threat actors launched a series of PowerShell scripts, numbered 1.ps1 through 12.ps1, as well as some that were just named a single letter from the alphabet." I think C and S, as I recall. He said: "That prepared the attacked machines for the final ransomware payload and ultimately delivered and initiated it."

He says: "The PowerShell orchestration was itself created and triggered by a PowerShell script named RED.ps1 that was executed on the target machines using WMI," the Windows Management Instrumentation. He said: "The script retrieves and unpacks into the system32 folder a .7z archive that contains the rest of the PowerShell scripts, the ransomware executable, and another EXE. It uses the machine's Task Scheduler to run scripts numbered 1 through 12, except for 7 and 8. It also creates tasks for scripts named 'S' and 'C.'

"For example, when attackers ran the 2.ps1 script on a machine, it executed a command that deleted the Volume Shadow Copies from the computer." He says: "This is an important precursor to the attack, as these files could be used to recover some or all of the files encrypted by the attackers." Right? The Volume Shadow Copies is the way you roll back a Windows machine if doing something hurts it. He says: "A PowerShell script named c.ps1 appears to be a clone of an open source tool called Copy-VSS, part of a suite of penetration testing tools named Nishang. The Copy-VSS script permits an attacker to copy the SAM file, which an attacker could use to retrieve and crack passwords saved on the computer."

The PowerShell scripts also use a rudimentary form of obfuscation in which the threat actors appear to have added in some square braces and brackets at random into the script, thus breaking up the lines of PowerShell script code, and then use a command that later strips out what they had added.

"While this technique doesn't have much of an effect on our ability to analyze the files after the fact" - because of course you just ignore them - "it might be just good enough to evade detection of an anti-malware tool that's scanning the files on the hard drive for a few minutes, which is all the attackers really need." Just a few minutes to get themselves going.

"That red.ps1 script unpacks RED.7z into the %SYSTEM%\RED directory, then creates scheduled tasks that run the unpacked scripts. But then it waits one hour and executes commands that modify the Windows Firewall rules such that the firewall blocks inbound connections on all TCP ports except Remote Desktop Protocol's 3389/tcp and [sadly] the communications port used by," he writes, "a commercial tool called Remote Utilities, which uses port 5650/tcp."

And as I've mentioned before, Remote Utilities is an excellent remote desktop management facility. It's the one I've chosen for my own use. Lorrie uses it, thanks to me, to remotely manage the laptops being used by her home neurofeedback clients. And my tech support guy, Greg, who runs a computer consultancy on the side, uses it to manage hundreds of his client machines. So it's wonderful, and it's annoying to see it abused like this. But I suppose that's how Mozilla felt when their wonderful free Firefox Send turned out to be totally taken over by bad guys so that they had to end up taking it down.

Anyway, Andrew notes that, oddly, the port blocking does this by first blocking inbound traffic to ports 80 and 443, then redundantly blocks entire ranges of ports that include 80 and 43, but also exclude those two, the RDP and remote utility ports. So it blocks 1 through 3388, 3390 through 5649, and 5651 through 65352. So, okay, this just sort of seems - the whole thing seems like amateur league.

"Upon closer inspection," he says, "one of the first things the attackers did after gaining access to the target's network was to download and install a copy of Remote Utilities and the Tor Browser. So," he writes, "this seems like a way to reassure themselves they will have an alternate foothold if the initial access point gets locked down."

Andrew then notes a few of the attractive features of Remote Utilities. He writes: "The commercial Remote Utilities software used by the criminals has several features they might find helpful." Unfortunately. "For one thing, they can use it for free. Anyone can submit an email address through the company's website and receive a free license key by email that allows them to use the full capability of the product on up to 10 machines, in perpetuity. The company's Viewer software includes the ability for a licensed user" - that is, licensed only to that degree - "to generate a digitally signed executable installer, preconfigured with a password and other preferences embedded into the EXE. Users choose their options, which get transmitted back to the company via the application to generate a unique one-click package executable, digitally signed," which again will help it to pass through any AV tools that are on the lookout, which then downloads.

"The threat actor can then deploy this installer, which runs unattended, and automatically synchronizes to their Remote Utilities Viewer console." And the Viewer console can also serve as a remote desktop client as an added convenience. Anyway, as I said, Remote Utilities is terrifically cool and very functional, and it's annoying that these guys are using it for a malign purpose. But that's the nature of all of these things. They're also using our Windows machines for malign purpose.

He said: "We found that the attackers had generated at least two of these one-click installer executables, which they downloaded to several machines on the target's network and ran. The installer was named 'rut' [so remote utilities], rutserv.exe, and the attackers stored it in different filesystem locations on different machines they downloaded it to." So trying to be a little more sneaky, apparently.

"Initially, the malware runs the scripts numbered 9 and 12. This is followed by a 180-second delay, before then creating the tasks for 1 through 6, 10, 11, S, and C. By default, the attackers extracted these files to a folder named RED under the %SYSTEM% path. Each of these scripts accomplishes a specific task" - again, remember all PowerShell, so just readable, basically command macros - "accomplishes a specific task the threat actors used to prepare the system prior to launching the ransomware. Many of these tasks involve hindering security or backup tools, but also involve disabling or killing processes that, if they were running, might prevent a complete encryption of the valuable data on the hard drive."

He said: "It isn't clear whether the attackers were just being thorough, or if they weren't sure they could do what they set out to do, because in several cases the scripts issue redundant commands to accomplish the same goal." I know, Leo. It's just a...

Leo: It's just classic crap coding. Like say it again just in case.

Steve: Yeah. It's a hodgepodge...

Leo: A hodgepodge.

Steve: ...of different methods. For instance, they say, 1.ps1 looks for processes that contain any of the following strings in their process name, and attempts to kill them. And then we've got like just a mass of strings: sql. Sql with a capital Sql. SQL all caps, you know, because they couldn't do a case-insensitive match, apparently.

Leo: Didn't understand regular expressions, obviously.

Steve: Yes, yeah. That would be, like, too much. Cylance with a capital C and not. Oh, here we have another instance of sql because they forgot they already did that first. I know. Backup. Oh, here's V-E-E-A-M. What do you know.

Leo: Oh, yeah, Veeam's in there, yeah. Oh, yeah. They want to disable Veeam. That's the first thing they want to do.

Steve: That's right.

Leo: But it's in there twice or three times, I noted.

Steve: Oh, my lord.

Leo: No, really, we don't want you to turn that one on; okay?

Steve: We got Outlook. We got Word. We got Excel. Office, OneNote, Firefox, wordpa, isqlplusservice. Oh, here's sql again, so that's now the third time they've done that.

Leo: Ironically, the chat room's saying PowerShell is case insensitive. So all of this is just silly, silliness.

Steve: Wow. Winword, MS Access, PowerPoint, Wordpad. Here we have VeeamAgent, so it's in there again. Oh, SQL, all caps, for the second time. Wow. Yeah.

Leo: Oh, my, it's funny.

Steve: So he says, and so Andrew says: "These strings indicate the attackers are not only trying to shut down security tools, but also database services, backup programs, office applications, email clients, QuickBooks, and even Steam, the gaming platform." Oh, yeah, Steam is in there in the middle. Oh, and The Bat!. Because, you know, that's a super popular email program.

Leo: I use it. I like it. At least like the name. That's funny. Do they have the exclamation mark with The Bat?

Steve: Wow. No. Just The Bat.

Leo: No? Oh, they're going to have to add another entry.

Steve: Uh-oh.

Leo: Uh-oh.

Steve: So that was 1.ps1. 2.ps1 deletes all the Volume Shadow Copies on the system by running a single command, "vssadmin.exe delete shadows /all /quiet," because, yeah, you don't want to echo anything anywhere. 3.ps1 disables automatic repairs that Windows might try to run upon a reboot. And of course you wouldn't want to do this all like with one PowerShell script because - we don't know why. 4.ps1 then attempts to delete the Volume Shadow Copies using a different method. WMIC, you know, Windows Management, shadowcopy delete /nointeractive. Then we do a Get-WmiObject Win32 shadowcopy, piping it to a number of different expressions because why not.

5.ps1 executes two commands that, between them, delete Windows Event Logs, which would hinder an investigation. Similarly to 1.ps1, 6.ps1 attempts to kill, not processes, but services, based, yes, on a list of strings that may appear in the services' names. Guess what: sql, Sql with a capital S, SQL all caps, and Titan, Cylance with and without a capital C, Defend, Veeam again, oh, also with a lowercase v and uppercase V. Backup twice. Oh, yeah. Anyway, it also disables Windows Defender by setting the following Windows registry key. So surprisingly, they apparently didn't give it its own PowerShell. They just figured, oh, let's be a little fancy and do two things here in a single PowerShell file. Wow.

9.ps1, which is executed first, attempts to invoke the Uninstaller for security software from Sophos, Trend Micro, Cylance, Malwarebytes, Sentinel One, Vipre, Webroot, and several cloud backup agents. 10.ps1 then redundantly runs the dropped p.exe executable, which suspends the processes that contain the following strings and clears their logs. And this is a catchall. Here's Veeam again, Outlook, Word, Excel, Office, I mean, Thunderbird, SyncTime, WinWord, MS Access, PowerPoint. So I guess - oh, The Bat! is there again. VeeamAgent. Sophos. VSS, you know, anyway, just a grab bag of things that, hey, let's stop this process if it's running.

11.ps1 adds yet another layer of redundancy, if that's what you want to call it, executing the following commands that delete Volume Shadow Copies - they really want to get rid of those - again, for the third time, as well as changing recovery options and clearing event logs in yet another way. So I won't bother everybody with these, but another list of commands, a bunch of BCD edit things and so forth. Anyway, this level of redundancy, they say, may be an indication that this threat actor is unsure of their own tool's capabilities, but aren't taking any chances. Eh, why not? We found this on the 'Net. Let's run it.

12.ps1 grants the "Everyone" group access permissions to every drive letter that might exist on the machine to ensure as many files are encrypted as possible. Whew. The red.ps1 script also deletes itself, the .7z archive, and the local copy of 7-Zip from the system when it runs, removing that additional evidence. In addition to the ransomware executable itself, Sophos recovered and analyzed another ancillary executable that the attackers deployed on the target machines.

The file, just called p.exe, appears to be a custom-compiled version of an open source tool called EventCleaner, which was created to erase and manipulate the contents of Windows event logs. So again, no big custom single EXE that, like, takes responsibility and does this. Instead, just sort of this weird hodgepodge of PowerShells and random small EXEs that each only do one thing, that they run a few times just to make sure that the last time they ran it, if it didn't finish or get everything cleaned, that maybe it would do it a next time.

We also mentioned that there were other PowerShell scripts delivered in that .7z archive the attackers dropped on the target machines. Although they saw no evidence that they were executed in the context of the attack, the scripts numbered 7, 8, and 9 serve important purposes: 7 logs off practically all open sessions on the computer; 8.ps1 is a redundant copy of the same firewall rules script included in RED.ps1. The ransomware itself, finally we get to that, is called RED.exe. It's a 64-bit Windows executable written in the Go language, compiled using MinGW, and packed with a modified version of UPX.

The executable contains some code taken from an open source project called godirwalk, which is a Go program to do a walk of the directory system. It gives it the ability to scan the hard drive on which it's running for directory paths and compile them into a list. Get this. The ransomware then spawns a new child process that encrypts each subfolder separately, which after a short length of time results in many copies of the ransomware process all running at once, contending for the limited resources of the machine. So not the most efficient way to encrypt the thing. The ransomware itself is quite small as it only really is used to perform the encryption of the files on the targeted system. That is, it doesn't do anything else. PowerShell scripts do the rest. It makes no network connections. And because functions like killing processes or deleting Volume Shadow Copies have been outsourced to the PowerShell scripts redundantly, that program, RED.exe, is very simple.

In the sample that Sophos saw, it doesn't even contain a list of targeted file types or file extensions, which all well-behaved ransomware do. That is, you know, they encrypt the important things. They don't bother encrypting EXEs and DLLs. This thing will encrypt everything inside every folder it encrypts, including other executables and DLLs, which of course can render programs or the entire system nonfunctional, if the ransomware decides to encrypt the wrong folder path in the process of encrypting every file. Then you end up with a dead machine. And it adds the file suffix .epsilonred to the files and redundantly drops a ransom note in each folder because of course you have run a separate copy in every single folder.

And interestingly, the ransom note closely resembles, as I mentioned before, a shortened version of the note used by REvil. But where the REvil note is riddled with spelling and grammatical errors, the note delivered by Epsilon Red has gone through a few rounds of edits, making its text more readable to an audience of native English speakers. And the ransomware note is familiar. It starts off with the same headline: "What happened?" which is the question that REvil asks. And then it says: "Your files have been encrypted and currently unavailable." So still not got English quite right, but better. "You can check it. All files in your system have Epsilon Red extension. By the way, everything is possible to recover (restore), but you should follow our instructions. Otherwise you can NEVER return your data."

Then: "What are our guarantees? It's just a business, and we care only about getting benefits. If we don't meet our obligations, nobody will deal with us. It doesn't hold our interest. So you can check the ability to restore your files. For this purpose you should come to talk to us. We can decrypt one of your files for free. That is our guarantee. It doesn't metter" - M-E-T-T-E-R - "for us whether you cooperate with us or not." Okay, I don't know what that means at all.

Leo: It doesn't metter. It does not metter. Is not metter. You do what you wish to do. We don't care. We make money either way.

Steve: "But if you don't, you'll lose your time and data 'cause only we have the private key."

Leo: Only we.

Steve: Oh, I see, yes. It doesn't matter whether you do it, though we really would like your money.

Leo: You'll be sorry, but it's okay. You don't have to worry about it.

Steve: They say: "Time is much more valuable than money." Okay.

Leo: Except to us because money is everything to us. We wrote many PowerShell scripts over many, many, many nights, yes.

Steve: It took, yes, big ASCII editors. Then they say: "Data Leak." They say: "We uploaded your data, and if you don't contact with us, then we will publish your data." And now, Leo, I'll just take a moment to mention there is no indication that any exfiltration was ever performed. So...

Leo: Oh, that's interesting.

Steve: Yes. So...

Leo: As great Comrade Nimzowitsch once said, the threat is greater than execution. Is chess. You would understand.

Steve: So get this. Under "How to Contact," they say: "You have two options. Chat with me," so that's interesting. "Chat with me. Visit our website: http://epsilons.red/" and then Sophos blacked this out. "When you visit our website, put the following key into the input form. Then start talk to me." Option 2: "Email me at," and then there was an address blacked out @protonmail.com.

Okay. Now, note that Sophos discovered no indication that any of this hodgepodge of bits and pieces of PowerShell scripting or small single-function executables ever did any exfiltration of the victim's data.

Leo: Wow.

Steve: Yeah, huh. So given everything else we've seen...

Leo: We also incompetent.

Steve: Yes. And we borrow extortion letter from REvil because they're better with English.

Leo: They are good writers, very good writers. We love their prose. Is good.

Steve: So given everything else we've seen about this concoction, it seems almost certain that no actual exfiltration of any kind was done. After all, all that is is a threat; right? They don't have to produce any plaintext. They will just say they'll decrypt a file if they're given one. So there's that. They don't evidence having any infrastructure to back up either their threat or their victims' data. And in order to engage with attackers, their victims are instructed to visit a specific page on a website located, not on the dark web, where all other ransomware sends its victims, but to a regular normal public Internet site at the domain Epsilons, plural for some reason, dot red. Note that since this was written up, the Epsilons.red domain has disappeared. No surprise there. Wonder who could have, I mean, anybody could have taken it down. It wasn't hidden.

So, you know, operating styles of this sort leave their own sort of fingerprint; right? What do the facts in evidence suggest? The encryption malware as described is bare bones, but it does get the job done. It uses a publicly available directory recursion tool to build a list of directories. Then it spawns individual instances of an encryptor for each discovered directory. Each encryptor operates indiscriminately, without any file extension-based encryption filtering. It simply encrypts the entire contents of every directory it's run in.

Does it even use a public key? Maybe. But it might simply use a static key. In which case obtaining a copy of the encryption EXE, if you could undelete it from the hard drive where this was run on, this is a PowerShell-based approach, so it does delete it after the fact. But that would allow for decryption without paying the ransom, potentially. We've certainly seen many instances of lame ransomware whose analysis resulted in the creation of free decryptors in the past.

And besides that one encryption EXE, everything else was either freely obtained and reused, or written as PowerShell scripts. Being scripts, that saved them from issuing the commands by hand. But it is certainly far lower tech than the ransomware systems that have come before. And this certainly doesn't lend itself to an affiliate model. You know, you can't sub this out. This is just ridiculous.

So this guy used a public website for his extortion and cribbed much of the text of the ransom note being used by the REvil gang. Taken as a whole, more than anything else, this has all the hallmarks of somebody in a hurry who's attempting to get into the diminishing pool of Exchange Server machines before they're all gone. As we all know too well, it's trivial to locate Exchange servers and to penetrate any that haven't been patched since March. But as I noted at the start, Sophos did track down the cryptocurrency address being used by these guys, or as seemed more likely, this person, since this feels like a one-man shop. And they found that someone paid the equivalent of $210,000 to the address where this person was trying to collect money. It would be very interesting to know whether the victim who paid that money ever got their files back.

The reason I'm curious is that this attacker didn't bother to set up a Tor hidden .onion site, and the exfiltrated data extortion threat has all the appearances of being empty. So what else might be empty? In our current environment of rampant and high-profile ransomware, it seems inevitable that there will be low-end attackers, probably like this guy, who trade on the reputation, such as it is, of high-end ransomware, which does go to some pains to assure the successful recovery of encrypted files because they want to maintain the reputation of, you know, their reputation as if you pay us the ransom, you actually will get your files back, and we won't leak them on the 'Net. Any naive victim who doesn't know any better would have no way of discriminating whether they've been attacked by a - and I can't believe I'm saying this - "reputable ransomware attacker."

Leo: You know.

Steve: Yeah, one of the good ransomware attackers.

Leo: One of the good guys, the well done ones, yeah.

Steve: Yeah, exactly. Operating in good faith, who actually has developed the capability to restore encrypted systems versus this half-baked attacker who's trading on the public's knowledge that once ransoms are paid, it's actually possible to bring systems back online. Yeah, if you get attacked by one of the good ransomwares, instead of this PowerShell nonsense. Presumably, the attacker is able to decrypt a single file as proof of their ability to do so. At least he does offer that in his ransom demand. And since all files were encrypted indiscriminately, the affected systems probably no longer boot or run at all. So each one would need to be booted using recovery media in order to gain access to the system's mass storage. What a mess.

Leo: Wow. You have found a real gem in the annals of ransomware, I've got to tell you. At least it's got a good logo. And it's not the logo, that's just the character it's based on.

Steve: Yeah.

Leo: It's got a good name. Didn't even bother getting a logo yet. That's how you could tell he's one of those amateurs. All good malware has a logo.

Steve: That's right, yup. Not Epsilon Red.

Leo: So I can't wait to hear what your physicist friend says about that problem in - and I think I know what he's talking about. You know, I asked Andy, because there are a lot of - there's a lot - he tried his best, of course, to make it scientifically accurate.

Steve: And it is, after all, fiction.

Leo: It's fiction. So there's a couple of things, yeah, that are a little bit made up. But he, you know, I think was quite admirable in his, you know, his first book, "The Martian," was used in classrooms as science curriculum. And I suspect he thinks the same thing might happen to this one. And it's true. I mean, if you gave people those problems and said, okay, how would you solve this, it'd be kind of fun. Kind of interesting.

Steve: At least we know that, yes, well, especially the beginning with the string and, you know...

Leo: Yeah, exactly; right? There's a lot of that, yeah.

Steve: Yeah. It was a lot of fun.

Leo: Yeah, yeah. I really enjoyed it. I think he's great. And you know I think he's back on form. There's somebody in the chat room who is Canadian, so he insists that it's Emsisoft, not Emsisoft. How the hell you'd know that, I don't know.

Steve: Okay. Well, I - yeah.

Leo: He's a Canadian. He cares about these things.

Steve: So he would know about them in New Zealand?

Leo: I have no idea. I have no idea. It's all in the Commonwealth, Steve. They all bend a knee to the Queen. That's what matters. Steve Gibson will never bend a knee to bad guys. He is the king, as far as we're concerned, our security guru. You'll find his work at GRC.com. That of course includes SpinRite, the world's best hard drive, sorry, mass storage recovery and maintenance utility because it works on all mass storage including SSDs, which is really good news because that's pretty much what everybody's, certainly what I'm using. I haven't bought a spinning drive in a long time. Except for my NAS, come to think of it. SpinRite 6 is current. 6.1 is imminent. If you buy 6 now, you'll get a free upgrade to 6.1. But even more importantly, you'll get to participate in the development of 6.1. That's at GRC.com.

Also there, of course, this show. Steve has two unique formats of this show. We both have the 64Kb audio. I have video at the website TWiT.tv/sn. He has, uniquely, 16Kb audio. Do you have an ffmpeg script that you do this with? Or you manually...

Steve: Actually, I still use Cool Edit.

Leo: Cool Edit.

Steve: From the old days.

Leo: You go, drop this down. Okay.

Steve: Yeah, because I normalize the amplitude to 100%, which brings it up to full. And then I scrunch it down by a factor of four.

Leo: It sounds like Thomas Edison singing "Mary Has a Little Lamb." But it is the smallest audio version of the show. There's also a very small transcription of the show which is very handy if you like to read along as you listen, or just read along by itself, or use it for search. Those are by the great Elaine Farris. You can get that and the 16Kb and the 64Kb audio at GRC.com. We have audio and video at TWiT.tv/sn. You can download it there.

You can also, if you want, there's a YouTube channel. In fact, if you go to that website, TWiT.tv/sn, there's a link to the YouTube channel, also a link to automatically subscribe in Google Podcasts, iTunes, and a variety of other podcast applications, plus an RSS URL that you can paste into Google Chrome and see what it does. I don't think Chrome probably does RSS anymore, but other browsers maybe. No, none of them do. But paste it into a podcast app, and it should say, yeah, subscribe. And you should say yeah. And then you'll get it automatically. If that podcast app does offer reviews, please leave Steve a five-star review. He has earned it today, and every week works very hard to bring you the show.

We also have a free IRC, if you want to chat along while you're watching live at TWiT.tv/live. That's irc.twit.tv. After the fact, the conversation continues at our TWiT Forums, that's twit.community. Steve has his own forums, as well. What is that, GRC.com/forums?

Steve: Forums dot.

Leo: Forums.grc.com. Excellent. And we also have a Mastodon instance which is like Twitter, minus the noise. And that's at TWiT.social. Both of those are free to join. We welcome your participation. Steve, have a wonderful week. Have fun with "Project Hail Mary."

Steve: I'm going to do that. And we'll be back next week for Episode 822. Yay.

Copyright (c) 2014 by Steve Gibson and Leo Laporte. SOME RIGHTS RESERVED

This work is licensed for the good of the Internet Community under the Creative Commons License v2.5. See the following Web page for details: http://creativecommons.org/licenses/by-nc-sa/2.5/