The BlackMatter Interview

Description: This week we look at Firefox's declining active user count, at the evolution of the Initial Network Access Broker world, and at several different ransomware group renamings and revivals. We encounter a well-informed Active Directory security researcher who feels about Microsoft's July pretty much as we do. I want to turn our listeners on to a very interesting-looking Hamachi-esque overlay for WireGuard, and share a fun diagnostic anecdote that cost me a day of work last Friday. We have a bit of closing-the-loop feedback from a couple of our listeners. Finally, we're going to share an interview with a member of the "maybe new or maybe rebranded" ransomware group BlackMatter which Recorded Future posted yesterday.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-830.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-830-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here with bad news about Firefox and a plea to turn the bad news around. We'll also talk about a new critical feature in the infrastructure of ransomware attacks. It's called the IAB. And then an interview with BlackMatter. It sure sounds like the return of DarkSide. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 830, recorded Tuesday, August 3rd, 2021: The BlackMatter Interview.

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

Steve Gibson: Ho.

Leo: Hey, of GRC.com. Hello, Steve.

Steve: Leo?

Leo: Yes?

Steve: This is the - and I'm using this word advisedly because I misused it once, and I've never heard the end of it.

Leo: Let me guess. Penultimate.

Steve: That's the word. Yes.

Leo: But wait a minute. I can't guess what it's the penultimate of.

Steve: This is the penultimate episode of Year 16.

Leo: Oh.

Steve: Of the podcast.

Leo: We're coming up on an anniversary.

Steve: We are.

Leo: That's hard to believe. That's amazing. 17 years old.

Steve: We look a little different than we did back then.

Leo: Wish we looked like 17 year olds.

Steve: I saw a picture of you on one of the TWiT thumbnails. And I thought, who is that? And I said, oh, that's supposed to be Leo.

Leo: Yeah, a long time ago.

Steve: It was one of those cartoon ones, and I never really was that pleased with mine, either.

Leo: We never got them updated. But we do sell that mug of you looking cocky. Quite a few of them, actually.

Steve: Yeah, I'm quite cocky today. Do we still have the mask on me? Or did that come off?

Leo: Oh, that's a good question. Anthony, have we removed masks from the album art yet? I don't remember. If we did, we have to put them back on again because we have been instructed by the County Health Department that we all have to mask up again in the studio.

Steve: Well, thank goodness that a biological virus cannot crawl through the audio link that you and I have, or I'd be further away from the microphone than I am, like kissing it right now.

Leo: Actually, don't tell anybody, but I kind of am glad because remember this studio was inside the cordon sanitaire. No one could come in here. And then when the mask mandate went away, and everybody came back to the office, people started coming in here. And now they can't come in here again. I like it.

Steve: Well, and you get to have Padre on the Sunday show and not have him feel like a third-class citizen because he's not there with everybody else.

Leo: Everybody's on Zoom now, yup. Everybody's back on Zoom, sad to say. So what's the matter of the moment?

Steve: This is, I think, going to be fun. I've got a lot of stuff to talk about. Security Now! Episode 830. And as I said, second to the last of our 16th year. Yesterday the security group Recorded Future posted an interview they conducted with an individual from maybe an upstart, but we don't think so, ransomware group known as BlackMatter. So what I found interesting about this, there's not a lot of new detail. But the interview was conducted by a Russian-speaking member of Recorded Future, speaking to a Russian member of Black Matter. Then it was professionally translated into English. So it doesn't read like pidgin English. It's well translated. But you get, well, our listeners will see, a sense of the attitude which I think is really interesting of, like, how these people see themselves in the world, and some recent history of what's been going on in the ransomware business.

But before we get to that, we're going to be talking about some evidence we have of where BlackMatter came from and why there's strong, strong evidence that this is the reemergence and rebranding of DarkSide.

Leo: Oh, boy.

Steve: The group that of course made the mistake of hitting the Colonial Pipeline operation and shutting down the U.S. Eastern Seaboard's petroleum supply. And that did not work out well for them. But lots more to talk about. We're going to look at, and I heard you mention this somewhere recently, so I went and tracked it down because I was curious, Firefox's declining active user count.

Leo: Yeah, yeah. Disappointing, I'm sorry to say.

Steve: Yes. The evolution of the initial network access broker world, those are the guys who are now, in this increasingly specialized ransomware industry, the guys who are only doing the initial penetrations and then turning around and offering them for sale to ransomware groups to then monetize them. We've also got several different ransomware group renamings and revivals. And we encounter a well-informed Active Directory security researcher who I was glad to say, or see, feels about Microsoft's July pretty much as we do. So that was sort of fun. I also want to turn our listeners on to a very

interesting-looking Hamachi-esque overlay for WireGuard, and share a fun diagnostic anecdote that cost me a day of work last Friday.

Leo: I love your diagnostic stories, by the way. Keep those up.

Steve: Well, I got a lot of positive feedback from the last one.

Leo: Yeah.

Steve: So I thought, you know, this happened. I posted all the details to the GRC spinrite.dev news group by way of introducing the next increment of, like, where I am. And I thought, yeah, it'd be fun to share that.

Leo: Oh, good.

Steve: Also we've got a bit of closing-the-loop feedback from a couple of our listeners. And then we're going to look at the BlackMatter 'tude.

Leo: I look forward to the BlackMatter 'tude.

Steve: Oh, and Leo, a Picture of the Week. It's not - nothing will ever top that ground wire stuck into a bucket of dirt. That's, to me, that's got to be - that's a classic for all time.

Leo: Although that one could have been a setup. There's no way this is fake.

Steve: No.

Leo: No way.

Steve: I just gave this the caption, "How does this happen?"

Leo: Yeah.

Steve: Because, you know...

Leo: You can't fake this one. This is clearly real.

Steve: Maybe someone's alive in there. That's a frightening thought.

Leo: Okay. We don't know, but we'll find out in just a little bit, the Picture of the Week. Okay, Steve. This is the picture. I'm ready. Fire away. Did you take this in our server room, I'm asking, I'm wondering?

Steve: So I did learn a lesson during some of my early equipment setup. There's a tendency when you're a newbie to go overboard with the tie wraps, to determine the optimal length for every cable and get that length of network cable and plug it in each end, like route it carefully around.

Leo: I used to have Colleen custom-make cables so they'd be just the right size.

Steve: Right, right.

Leo: No excess, yeah.

Steve: Right. And then you want to kind of gather them as they go along with successively larger wraps to create a bundle, and then route the bundle down, blah blah blah.

Leo: Yeah, tidy, yeah.

Steve: And inevitably you get that all done, it's like, oh, look. I mean, it is the most beautiful thing...

Leo: It's gorgeous.

Steve: ...you've ever seen.

Leo: And if I showed you our current server room, you would say that because they really did a good job. But in the first days of the old studio, everything was like, plug it in, quick. Get it going. We only gave them a few hours for the move.

Steve: Well, and the problem with that kind of beautiful work is when you have to change something.

Leo: Yeah. It's not very flexible.

Steve: Because change inevitably occurs. Now, at the opposite side of that spectrum, we have this, where change is also a problem.

Leo: Yeah, actually that's true. This is no more flexible, is it. Because you have no idea what's going to what.

Steve: No. And the problem is when a port dies, like, deep inside that nest. So I feel more sorry that we have non-video, non-visual listeners for this than I can remember feeling because I cannot adequately describe. I can describe the fence planted out in the middle of the desert that's locked with the car tracks running around on either side of it, which, you know. But I can't describe this picture, I mean, except to say it is the most godawful, like, insane cable room. I just, you know, it is worth for our listeners who don't normally bother with the show notes. This is Episode 830. Get the show notes and look at this picture.

Leo: This picture, yeah.

Steve: And again, I captioned it "How does this happen?" Because this...

Leo: I know exactly how it happened because...

Steve: This demonstrates a lot of...

Leo: I mean, it wasn't this bad in the old studio. But if you're in a hurry, and you've got to get stuff connected so you can operate - still, this is pretty bad.

Steve: Leo, yeah. I mean, this feels like it is the evolution or devolution of what was once organized. I mean, look at the very bottom there. There's a little white bundle.

Leo: Oh, there is a bundle, yeah.

Steve: Like kind of going off by itself.

Leo: At one point, yeah.

Steve: It's like, you know...

Leo: And the bundles in the rack are tied together, the cables.

Steve: Now, apparently the aesthetic taste of the person is reflected in the chair that we can see in the foreground. So the chair might go a long way to explaining the rest of this because, whoa.

Leo: Yeah, yeah, a little optical art.

Steve: Anyway, this was tweeted to me by one of our listeners. I will thank you forever. This is one for the ages. This is quite something.

Leo: Yikes. That's amazing. And you know it's not fake because it would take so much time to make that rat's nest.

Steve: No, in fact, there are some lights on in there. They're lonely, but they're in there. And, oh, lord. And god help you if you have to change something, if like a port dies or someone moves their office to somewhere else.

Leo: Oh, yeah.

Steve: It's like, well, Marybeth is now on the third floor, and so she needs her network connection moved. Uh, well, okay.

Leo: You sure? Can we just move the floor? It might be easier.

Steve: Exactly. Okay. So I was concerned when I heard you, I guess it was on Sunday, talking about the news that Firefox had lost on the order of 50 million of what they call their Monthly Active Users, MAUs. It turns out that number is 56,003,700. So a 56,003,700 users drop from the peak shown in the chart that they're tracking, which was at - and this is the good news. It's not like it's 56 million out of 57 million, so like there's only one million left.

Leo: No, but it's a pretty good portion of the total.

Steve: As a percentage, yes, it is. So they started out on January 27th of 2019 at 250, nearly 254 million active users. They are now, as of July 25th, 2021, just a couple weeks ago, just they dropped below 200 million - 197,874 million. So, and, you know, I guess I'm not surprised. Chrome is strong. People who may have been in Firefox to be the counter-browser, they're now able to go to many Chromium browsers. I don't know, it would be interesting to know where these people went, and why.

My feeling is, you know, we always talk about this notion of a hard floor, is there like a hard ceiling or a hard floor above which something won't go or below which something won't go. My guess is there is a hard floor on this, that is, there are users who were on Firefox because someone told them they should be once upon a time, or something they needed to do didn't work on Firefox where it did on Chrome, or they got moved over because of the pandemic because someone said, oh, no, you've got to use Zoom with Chrome, and then they just sort of stayed there. I mean, who knows? It would be really interesting if there was some way to track the rationale for it. But I just sort of, because we talk about browsers a lot, browsers are important, I thought it was worth noting that this happened.

Leo: Yeah.

Steve: And, boy, we really don't want a browser monoculture.

Leo: No, no. That's the really important thing. And I feel a little guilty because I am not in that category. I actively chose Firefox to support open source and to support a

diverse ecosystem. And I have switched, as well. And the reason I think is, unfortunately, so many sites don't work unless you're using Chromium or a Chromium derivative.

Steve: Is that true? Because I've not hit any.

Leo: A lot of the sites - it's mostly commercial sites, video, stuff like that. And I'm increasingly having difficulty using Firefox. And the thing is, I'm using Vivaldi now, which is still, you know, it's a Chromium derivative, but it has a lot of nice features. But it just - it's easier. Yeah, see, you don't do, like, it's not unusual that you'll use, for instance, when I do the training for Premiere Networks, Chrome's required. A lot of RTC-style video clients just don't work as well if you're not using Chromium. I mean, it's a shame. It really is a shame.

Steve: It is. And we have seen all of the...

Leo: And I feel bad.

Steve: We've seen all the other independent browsers just give up, right, and switch to Chromium. And our podcast generates takeaways, in general. And certainly among those, near the top, is how difficult it is to do a browser. It's like China saying they're going to do their own OS. It's like, no, you're not. You know. Nobody can do - you just don't do an OS anymore. It's too late. You take Linux, and then you do some things to it call it your own. And similarly, you take Chromium, the Chromium core, and do some things to it, and call it your own browser. It's like, okay, we like the features that Brave has, or we like the features that Vivaldi has. But they have a common core.

Leo: Yeah, unfortunately.

Steve: Except for Firefox. Except for Firefox.

Leo: The other thing I'm a little mad at Firefox because they abandoned progressive web apps, which I think is really important. And so Chrome supports that.

Steve: Really. I didn't realize that. I heard you mention that, and I thought, wait, I thought Firefox did support them.

Leo: I thought they did, too. So, I mean, it's not completely our fault if they're an open source browser and they're not supporting these technologies that are good for open source.

Steve: And they're still getting a lot of money from Google.

Leo: Oh, yeah. They're basically a Google subsidiary.

Steve: Right. Because it's...

Leo: It's a search engine.

Steve: Right. I was just going to say, right, right, right.

Leo: It's affiliate fees from Google. It's millions, hundreds of millions of dollars a year.

Steve: Hundreds. It's like 500 million or something like that.

Leo: Yeah, yeah. And by the way, so does Apple. Apple gets billions. So Google pays a lot of money to keep people using their services. Yeah, it's very difficult politically for me. It's very difficult. But ultimately I have to opt for the ease of use.

Steve: Well, and the problem is, yes, I completely, obviously, sympathize. If there's something that you want to do, and the browser doesn't, then you go find one that does. I mean, it's not like there's, for most people, there's no compelling reason to use Firefox unless you have some anti-Google, anti-Chrome...

Leo: Yeah, that's a good reason. That's a hell of a good reason. And, you know, I guess Chromium is open source, I mean, it's developed mostly by Google employees, but it is open source, and so a Chromium-based browser like Edge or Brave or Vivaldi is still at least using open source technology.

Steve: Well, and how many zero days has the Chromium had?

Leo: Oh, yeah. A lot this month, 13.

Steve: Which affects every single browser which is based on the Chromium engine. So that's of course the danger of the monoculture is that you end up with a position, you know, like what we have with Windows desktop, frankly, where problems can be devastating because everybody's using the same one. But it seems inevitable, and I can understand, I mean, I wouldn't want to be responsible for a browser these days. Performance and bugs and capabilities and the feature spread, it's not easy.

Speaking of Chromium, Google will finally be assuming HTTPS in their UI. We're all currently, those of us who are updated on the latest Chromium, or Chromium and Chrome browser, we're at release 92. And as you surf around in these post-Snowden days, you'll most likely be, well, you'll always be seeing a little black padlock. They didn't spend any extra pixels or nuance on this thing. This is just the simplest, flattest, most uninspired black padlock, probably because they know it's about to fade away, that you could have. Anyway, it's there, to the left of all the URLs you go. Unless you somehow arrange to land on - and I'm told there's like 10% of sites that are still not HTTPS. None that I ever visit. I don't know where they're hiding. I had to go, like, search for one.

And just as a little tip for our users, http://neverssl.com is your trusted source for a non-SSL/TLS connection. Neverssl.com. Reminds me of Never10, my little gizmo that disarmed Microsoft from pushing Windows 10 on everybody who was happily using 7 or 8 at the time. Anyway, I had to go find it because I wanted to take a screenshot of what Google shows, what the Chrome browser shows when you are at a non-TLS-encrypted connection. And it's prominent. It says "Not Secure." And of course that's always annoyed me also because there are legitimate use cases for a site not having TLS, you know, being HTTP-only, if it's just like an old-school pure, like, pages that lay there. You can't create a session. There's no cookies that it's holding for you. There's no login. You just click on things, and you look at different pages. There's, like, zero reason to secure that. There's no transactions. There's no cookies. There's nothing that needs to be kept secure. But Chrome says "Not Secure." Well, right. But also no need for security.

Anyway, the point is with the next release, 93, of Chrome, the little black padlock, for which hopefully they didn't pay anybody much, it's going away. So you will no longer see a padlock of any kind, anywhere, in the default case of secure because, yeah, everything is. You'll still get that "Not Secure" if by some strange happenstance you go somewhere that doesn't have HTTPS, like you went deliberately to Neverssl.com. You'll still get it. But anyway, the point is no more padlock. It's going away. That's just the way the world is now secure. Thank you, Edward, for helping us get there.

Okay. As we know, unfortunately, ransomware has rapidly grown into an established and entrenched form of cybercrime that's not going away anytime soon. As a consequence, it forms an unapologetic large percentage of today's podcast. The first aspect of specialization that emerged was the idea of separating the developers of the ransomware from its use to attack victims. Some evil genius somewhere conceived of the notion of Ransomware as a Service, and that just took off. It created the so-called affiliates who would perform the attacking using ransomware that they'd essentially rented. You know, basically for a piece of the action they'll go do that work.

It wasn't long before the affiliate role also split and further specialized into so-called Initial Access Brokers, or sometimes Initial Network Access Brokers and pared down the affiliates who now purchased access to the enterprises that they wanted to get into from a third party. So now we've got an additional player by cracking that apart.

Yesterday, the cybersecurity firm KELA, that we've never referred to before, K-E-L-A, and their domain name is Ke-la.com, they published a report documenting their year-long exploration into the dark web and specifically the nature of the market that's forming around these Initial Access Brokers. Their report provided so much interesting detail that it was, until yesterday, originally going to be the main focus and topic of the podcast, since I think this is an interesting offshoot of the whole Ransomware as a Service happening. But that plan was preempted by what did become today's main focus and topic, as I said, this really interesting interview and sort of the sense you take away from it.

So instead of digging deeply into every detail of what KELA found and reported, I'm going to summarize what they discovered about the nature of today's initial access broker market. They framed their research by explaining. They said: "For more than a year, KELA has been tracking Initial Access Brokers and the initial network access listings that they publish for sale on various cybercrime underground forums. Initial Network Access refers to remote access to a computer in a compromised organization. Threat actors selling these accesses are referred to as Initial Access Brokers. Initial Access Brokers play a crucial role in the Ransomware as a Service (RaaS) economy, as they significantly facilitate network intrusions by selling remote access to a computer in a compromised organization and linking opportunistic campaigns with targeted attackers, often ransomware operators themselves.

"The research includes an in-depth analysis of Initial Access Brokers and their activity for a full year, from July 1st of 2020 through June 30th of 2021. KELA analyzed IABs' activities over the past year, when their role became increasingly more popular in the cybercrime underground and summarized five major trends that were observed throughout their analysis."

Okay. So they have a set of bullet points as primary research takeaways. They explored over a thousand access listings offered for sale over the last year. The average price for network access during this period was 5,400 USD. So $5,400 is the average price, while the median was $1,000. The top affected countries are the U.S., France, U.K., Australia, Canada, Italy, Brazil, Spain, Germany, and the UAE. IABs built a pricing model for initial access. The most valuable offers include, not surprisingly, domain admin privileges on a computer within a company with hundreds of millions in revenue. RDP and VPN-based access are the most common.

IABs find new attack vectors and accommodate the changing software targets of ransomware gangs, including network management software and virtual servers. Successful IABs find regular customers, some of which are ransomware affiliates, and move most of their operations into private conversations. They said, however, new actors continually enter the scene. Some IABs adopted "ethics" - and I'll put that in quotes, right, because, okay, ethics for a cybercriminal - that were introduced by some ransomware gangs.

And we of course talked about those after the attacks which caused them to disappear. "Namely," they said, "there's a certain criticism against actors trading access to healthcare companies, though it's still an initiative of a few actors and not a typical attitude." So sort of a new thing that hasn't fully taken hold. They said: "IABs are eager to monetize their access and are using all means available to do so. Some IABs were seen stealing data from the affected company themselves to gain profits even if the access is not purchased." So that is to say, they're not solely selling access. They may dip in a little bit themselves.

And, finally, "IABs have become professional participants of the RaaS (Ransomwhere as a Service) economy. They constantly find new initial access vectors, expand the attack surface, and follow their customers' demands. It requires network defenders to track IABs' activities and all other actors who have formed around this whole ransomware ecosystem."

So KELA found that, not surprisingly, an important metric for setting the access price is the level of privilege that the access enables, with domain admin access being the most expensive, costing at least 10 times - not surprisingly - 10 times more than access to a machine with standard user rights. I would expect it to be way more than 10 times, but that's what they found. The priciest offers from reputable threat actors KELA observed included access to - and these are specific instances - access to an Australian company with 500 million in USD revenue that enables an attacker with admin-level privileges, most likely domain admin. That was offered for sale for 12 BTC, which at today's price is just shy of $500,000, $465,000 for a 500 million, okay, so that's half a billion dollar in U.S. revenue, Australian company.

Access through ConnectWise to a U.S. IT company was offered for 5 BTC, which puts it at about $200,000. Access to a Mexican government body was offered for $100,000 USD which was used for the LockBit ransomware attack. So this is interesting, too, because the fact that affiliates are purchasing access for some number of bitcoin means that they have an expense upfront associated with gaining access to the network that's been purchased. Which means they have an incentive not to walk away from this. They don't have zero dollars invested. They've got some, you know, some bitcoin has been

transferred in order for them to gain access. So they're in there for some money, maybe as much as half a million dollars, in the case of that Australian company.

On the other hand, they got high-level access into that network. They must have believed it was going to be worth, you know, they were going to be able to squeeze that company for some money. So the dynamics of how this is evolving are interesting. KELA is also seeing a diversification of access that is sort of access types as the market, such as it is, of illegal behavior is evolving. That's the entire point of splitting off this IAB role.

So as I was saying, KELA is seeing a diversification of access that's being requested from the IAB guys. Network access is loosely defined. Threat actors use it to describe multiple vectors, permission levels, and entry points. Over the course of this year, KELA observed that the most commonly offered access was RDP, of course, Remote Desktop Protocol, and VPN-based access. So brute forcing attacks which suddenly succeed and then those credentials which are discovered go up on the dark web for sale. Remote access can also be supplied through the ConnectWise and TeamViewer software, which can provide actors with RDP-like capabilities. VPN access can be gained and sold through various software such as Citrix, Fortinet, and Pulse Secure VPN products. And those have all been subjects of known vulnerabilities, which their parent companies have patched. The question is, did their own customers update with those patches? Those are all popular in the cyber underground.

In addition, IABs are finding new attack vectors and ways to supply access to buyers, meaning that the overall attack surface is expanding. For example, and we'll actually come back to an instance of this later, access to VMware's ESX servers, which have recently become quite popular among ransomware attackers. REvil and DarkSide both had custom versions of their malware specifically targeting the VMware ESX servers. Tracking and counting IAB transactions is difficult because once an IAB's advertisement is responded to by a credible and interested buyer, in general nothing further appears - well, in the accessible dark web, I was going say the "public dark web," but the accessible dark web - after these guys take their communication private.

And it also appears that after the parties have first met through an advertisement, and a relationship is formed, the buyer may say that the quality of the access you're selling is good. We'll buy anything else you have to sell for a fair price. So let us know first, since we may pay top dollar, or top ruble, I guess. So what happens is an IAB and somebody wishing to purchase access sets up a relationship where they say, you know, cool, the quality of your stuff is good. We want to buy other access that you get in the future. So that IAB may not continue advertising, if they've got a buyer that's willing to pay for all the access that they're able to discover.

KELA also confirmed the trend we've seen reported about the so-called "professional ethics," at least with regard to who is an acceptable victim. Both their disbanding and disappearance that we saw with the DarkSide gang and their promise then not to target certain sectors. This trend is spreading, and it's solidifying, although it's not yet established, and it varies depending upon the specific gang. But there have been bans on attacking healthcare, government, education, and non-profit sectors so as not to cause damage to patients, students, and citizens, and other categories of people. The ransomware gangs appear to be passing the message that they will only hunt companies and aim only for financial gain. And we'll actually see a beautiful example of that in this dialogue interview at the end of the podcast.

In line with this, IABs have been seen posting access ads for victims from the healthcare sector, then later deleting the offers after receiving criticism from other users. Like, you know, posted criticism saying, hey, you really shouldn't be pushing attacks on healthcare sectors. And then they go, oh okay, well, shoot. We could have gotten some money.

Leo: Oh, shoot.

Steve: Yeah, shoot. However, there are still no hard-and-fast rules on this matter, with most brokers being glad to sell all the access they're able to gain. So, yeah, there are less - again, I hate to use the word "ethical" in this context. But there are ransomware gangs that will attack anybody that they can get access to. So that's the situation there.

Leo, after our second break, or after our first break, I want to talk about the return of DarkSide.

Leo: Oh, boy.

Steve: Which didn't take long.

Leo: Yeah, no kidding. To me it's so interesting, and I don't think these guys are ethical ever. I think they just say whatever Putin lets us do.

Steve: Yeah.

Leo: We don't want to get in trouble with the GRU. That would be, you know.

Steve: Yeah, well, I think that you make a very good point. They didn't take themselves down.

Leo: Yeah.

Steve: They got pushed off or taken down. And so they're reemerging under a new name because, well, they can.

Leo: And who knows? You know, maybe their real ethical concern was they didn't want to pay the affiliate fees owed to the people who did the pipeline attack. And so if we just disappear and rename, rebrand, no one will know. Is surprise.

Steve: Yes, that's not DarkSide. We're not them, no.

Leo: Is not DarkSide. No.

Steve: So, okay. So as I'm explaining why the industry is virtually certain that we are witnessing the return of DarkSide, keep that in mind when we hear the guy from BlackMatter being interviewed, claiming that that's not the case. Okay. So as we know, an affiliate of the Ransomware as a Service group, which was at the time known as DarkSide, and "was" is the operative word here, made what turned out to be a big mistake by attacking critical U.S. infrastructure in the now-famous Colonial Pipeline attack that shut down the U.S.'s largest fuel pipeline, causing fuel shortages across the

Eastern Seaboard of the U.S., and gained what I think you can fairly say would be unwanted attention to themselves.

Shortly afterward, DarkSide's ransomware operation suddenly shut down. They lost access to their servers. And at least some of their ill-gotten funds, their cryptocurrency, was seized. We later learned that the FBI had somehow recovered 63.7 BTC of the approximately 75 which was the $4 million ransom payment made by Colonial Pipeline. So a chunk of that was recovered.

Since ransomware, when it's done right, can generate so much money, no one thought for a moment that the culprits had learned their lesson and had decided to update their LinkedIn profiles and start interviewing for jobs in the Russian IT sector. What we all thought was that they would return under another name, probably with at least the intention of not again stepping in such a big pile of trouble. And sure enough, a recent detailed forensic analysis of the cryptographic algorithms being employed by an apparent newcomer that has named themselves BlackMatter, and that will be the interview that we share at the end, suggests that BlackMatter is actually DarkSide 2.0. However, since this new group is soliciting initial access brokers themselves directly, it may be that they've scrapped their previous affiliate model, at least for the time being, probably in the interest of maintaining more control, and thus preventing a recurrence of the disaster that shut them down last time.

So this new BlackMatter group actively is, already, actively attacking victims and purchasing network access from other threat actors to launch new attacks. Over the weekend, BleepingComputer reported that multiple victims have been targeted by DarkMatter with ransom demands ranging between 3 and $4 million, and that one victim had already paid a $4 million ransom to delete data that had been exfiltrated from their network and to receive both a Windows and a Linux ESX, that's that VMware ESX decryptor.

So why do we believe that this is the work of DarkSide rebranded? Over this past very busy weekend, Emsisoft's Fabian Wosar, who we've been talking about lately because he's been very active in this area, he tweeted, he said: "After looking into a leaked BlackMatter decryptor binary, I am convinced," he tweeted, "that we're dealing with a DarkSide rebrand here. Crypto routines are an exact copy pretty much for both their RSA and Salsa20 implementation, including their usage of a custom matrix."

Okay. So what does he mean by that? Salsa20 is a symmetric stream cipher. And, as we recall from all the work we did talking about crypto years ago, what that means is that it XORs any data it's given, either for encryption or decryption, with the output of its cryptographically strong, pseudorandom bitstream generator. As we know from our previous talk about this, and as counterintuitive as it may seem, simply inverting random bits of a plaintext, which is what XORing does, by essentially XORing the plaintext with noise, totally scrambles that plaintext to yield a cryptographically strong ciphertext. Essentially, if you XOR something that has meaning with noise, you get noise as a result. And when that noisy stuff, that ciphertext is later re-XORed with the same random bitstream, in other words, reinverting exactly the same inverted bits, naturally the original plaintext is restored. That's Salsa20.

Okay. So Salsa20's internal state, that is, the data that it stores and grinds on in order to produce this cryptographically strong pseudorandom bitstream, it's held as 16 32-bit quantities. They are conceptually arranged in a 4x4 matrix. The formal Salsa20 spec specifies how those 16 values are to be initialized. This is specified sort of to create a standard implementation for inter-Salsa20 implementation compatibility. Even though technically it's arbitrary. So interlaced through four of those 16 32-bit values is the 16-character string "expand 32-byte k," That's all lowercase. Expand space 32 hyphen byte

space k. In other words, just some constant stuff. This is Dan Bernstein's construction. He did Salsa20.

Two of the 16 32-bit values are used to specify a stream position. So it's sort of a way of starting in different locations. And of course since they're 32-bit values, and there's two of them, that's a 64-bit position, so plenty big. Another two are nonces. And the remaining eight 32-bit values are used to specify the key. So that's the formal spec. DarkSide, okay, the original DarkSide, blows all that off and simply initializes that entire block with random data. It then encrypts that Salsa20 initial state matrix with a public RSA key, which is appended to the end of the encrypted file. Fabian said that this implementation of Salsa20 was previously only ever seen by DarkSide's crypto.

And now this approach has resurfaced, unchanged, being used by BlackMatter. Additionally, DarkSide's implementation of a 1024-bit RSA was also unique to their code, and BlackMatter also uses exactly the same unique implementation. So, yeah, deep down in the crypto they're identical. When we also consider that both groups use similar language and similar color schemes on their public and dark web sites, evidence that - oh, also they have a similar lust for media attention, and that the "new," in quotes, BlackMatter group is going to great pains this time to note that it will not target the oil and gas industry, and they specify pipelines and oil refineries - it seems about as certain as it could get that DarkSide has returned.

And at the end of this podcast, as I said, we're going to hear from a member of the group and see what they think of themselves. They're not the only ones. I wanted to also note because as things happen in the future we'll be referring to these gangs. The DoppelPaymer group has renamed themselves Grief, which is what they give their victims. It's just a simple rebranding. There's really no big news about the group beyond the observation that, just sort of for the record, DoppelPaymer has become Grief.

None of these groups, like, say that they're, like, they don't declare that they've been rebranded and renamed. But everything that they're doing is the same in the same way. They don't, like, rewrite their code from scratch. They don't, like, retranslate from their native Russian into English from scratch, probably because it's difficult to get English that they like. So to anyone who's observing these guys from the outside, duh. We can still see you. We know who you are. You changed your name, but nothing else changed.

Leo: Isn't that cute.

Steve: Yes, they have, in this case, both groups had different-looking colored CAPTCHAS, but the code underneath was custom, and identical. So did you forget to change, like, anything under the surface?

Leo: Well, why change anything that works?

Steve: Yes, exactly. And finally, Avaddon has also become Haron, H-A-R-O-N. So essentially I think what we're seeing here is there's been such a mess created by the REvil attacks and the DarkSide attacks that everybody, even if they weren't, like, attackers, everyone thought, oh. Well, everybody else is changing their name. We should, too. And so they're doing this rebranding. So from a podcast standpoint it's a little tricky because suddenly we're going to be talking about apparently new ransomware gangs. Not so much. They're just the same gang with a different name.

Okay. I wanted to begin with a brief look back at the month we've just survived. I found a nice set piece for this in the form of a little corner of GitHub which belongs to a guy named Christoph Falta, who's in Vienna, Austria. He describes himself as - I think this was in his little short bio on GitHub: "Random infosec guy. Rainbow teamer. Focusing on Windows security." And his past work, which is also published on GitHub, clearly shows that he has an interest in Microsoft Windows Active Directory security issues. So perhaps maybe he's a Security Now! listener. He doesn't follow me on Twitter, so maybe not. But I have many fewer Twitter followers than I know we have podcast listeners, so certainly not everyone who listens to the podcast follows me on Twitter. And many of the listeners my age have grumbled and said, "I'm not doing any of that social media stuff."

So okay. In any event, he seems to be channeling me on his latest page, which is titled "Microsoft Won't-Fix List, July 2021 Edition." He updated the page just yesterday. He posted on 08/02/2021. He said: "Update: Thank you for all your feedback. This list was intended to be a summary of what happened in July of 2021, and I decided I'll keep it that way because I honestly think I don't have the energy to maintain an up-to-date list of ALL [in caps] won't-fix issues Microsoft has to offer. So I'll keep this remark here for clarity and change the description." So then he said a growing list of design flaws Microsoft does not intend to fix. "Since the number is growing, I decided to make a list."

And anyway, I'm not going to go through it all. It's everything we've been talking about. Basically the page consists of a table with its columns labeled "Vulnerabilities," "Associated/Assigned CVEs," "Attack Type Descriptions." He has a column titled "It's NTLM again; right?" where in many of their entries are "Yup." And then also he has "How it works, in a nutshell." And basically he just goes through all the things that we talked about - PetitPotam, SeriousSAM, PrintNightmare, the ADCS problems. He has two that we talked about that hadn't been named that have now been given a name by the security community, SpoolSample and RemotePotato0. We've talked about all these things.

Anyway, it's just heartening for me to see that I at least was not alone in this overall sense I came away from July with, which I've been conveying through the podcast, that not only was July 2021 an unusually rough month for Microsoft, but that what appears to be emerging is a long-term problem with Microsoft's legacy protocols, which as I noted last week are all still enabled by default, just in case someone might need them; and that some of these problems work as designed, or as Christoph terms it in his CVE column, where there is no CVE because it's not a bug, it's a feature. So, yeah, you're not going to assign a CVE to something that works as it's intended to and that isn't going to be changed.

So there is a larger takeaway from this that I just wanted to make a point of. It's probably the case that the IT staff of many enterprises have become accustomed to assuming that whatever's wrong with Windows will be auto-patched as soon as Microsoft can get around to it. And while that might not be soon enough, as it was in the case of the ProxyLogon debacle with Microsoft Exchange Server early this year, Microsoft does eventually get their machines patched. So applying updates is clearly critical. But the shift that July's revelations of significant problems which all work as designed creates, means now that simply applying Microsoft's monthly patches will no longer mean that an enterprise network is being kept safe and secure. These things have diverged. When Microsoft wrote, and they wrote it "vulnerable by design" in that announcement a couple weeks back, they meant it. And that means that there's no patch forthcoming, late or ever.

So I just wanted to make sure that our listeners fully appreciated that we've entered a bit of a different world with this raft of discoveries throughout July, the publication and multiple proof-of-concepts of these vulnerabilities that Microsoft says they have no plans to fix because nothing's broken, in their view, despite the fact that somebody getting in

can use these things to wreak havoc within an enterprise, and Microsoft's not going to change that.

So what's going to be needed is for those professionals who have been falling back on Microsoft's updates, figuring, okay, yeah, all I have to do is that, that's not going to be true. For their enterprise's network security, they're going to need to go beyond pressing Microsoft's "update us" button and look carefully at what have become multiple edge cases and corner cases to determine how to set up their enterprise-wide policies to disable these dangerous features on a case-by-case basis. And I thought I really needed to put a point on that to make sure people get it that something changed this past month, and not for the better, for Windows security.

Okay. Something called Tailscale, T-A-I-L-S-C-A-L-E. As we know, WireGuard is widely, and I think appropriately and accurately, regarded as the logical and overdue successor to the venerable OpenVPN, and even to some degree IPSec, inasmuch as it can replace them both. OpenVPN, like OpenSSL, is suffering from its age and from the fact that it has been for decades the test bed for many experiments as we've been learning the right way to do things only after first doing many of those things wrong. For example, TCP cannot be the protocol used by a VPN's tunnel. We know that now. It's not what it was designed for, and doing so is just wrong. Yet OpenVPN offers the option. So once all of the wrong solutions have been tried, and the right solutions have been found, it's really best to lighten one's load and just start over again from scratch with a blank slate that can host an entirely new design. That's what Jason Donenfeld set out to create when he launched what has turned out to be the incredibly successful WireGuard project.

Exactly three years ago yesterday, it was yesterday three years ago, Linus Torvalds posted the following. It happened to be in the subject under networking. He said: "BTW [by the way], on an unrelated issue," he said, "I see that Jason actually made the pull request to have WireGuard included in the kernel," meaning the Linux kernel. He said: "Can I just once again state my love for it" - okay, this is Linus; right? He doesn't like anything. "May I once again state my love for it and hope it gets merged soon? Maybe the code isn't perfect, but I've skimmed it. And compared to the horrors that are OpenVPN and IPSec, it's a work of art."

So of WireGuard, Wikipedia reminds us. Wikipedia says: "WireGuard is a communication protocol and free and open-source software that implements encrypted virtual private networks and was designed with the goals of ease of use, high-speed performance, and low attack surface. It aims for better performance and more power saving than the IPSec and OpenVPN tunneling protocols. The WireGuard protocol passes traffic over UDP."

It continues just a little bit more. I'll say: "In March 2020, the Linux version of the software reached a stable production release and was incorporated into the Linux 5.6 kernel and backported to earlier Linux kernels in some Linux distros. The Linux kernel components are licensed under the GNU General Public License, GPLv2; other implementations are under GPLv2 or other free open source licenses." And then what I loved about this is it said: "WireGuard utilizes Curve25519 for key exchange, ChaCha20 for symmetric encryption, Poly1305 for message authentication, SipHash for hashable keys, BLAKE2 for cryptographic hash function, UDP-based only."

In other words, best of breed, one of each, period. We're done, thank you very much. There's no need for options. There's no need to choose this or that. We just did it once correctly. And that of course is where it gets its benefit, right, is it's like it minimizes the attack surface; uses very robust, well-understood ciphers. That's WireGuard.

Okay. So I want to introduce everyone to Tailscale, which two of our listeners, Ben Hutton and Jack Hayter, that's just for the record H-A-Y-T-E-R, recently turned me onto. A search on the phrase "WireGuard versus Tailscale" brought me to a page asking and

answering exactly that question. Should I use Tailscale or WireGuard to secure my network? The answer is yes.

So I'll mention that Tailscale's founders are some highly credentialed ex-Google and Alphabet developers who go on to explain. They're the founders of Tailscale. They said: "Tailscale is built on top of WireGuard. We think very highly of it. We designed Tailscale to make it easier to use WireGuard to secure your network connections. You might decide to use WireGuard directly, without Tailscale. This is a guide to using Tailscale versus configuring and running WireGuard directly." So we sort of have Tailscale providing a connectivity and ease of use and additional capabilities layer, with WireGuard providing the super-secure packet level transport.

For configuration they explain: "WireGuard is typically configured using the wg-quick tool. To connect two boxes, you install WireGuard on each device, generate keys for each device, and then write a text configuration for each device. The configuration includes information about the device - port to listen on, private IP address, private key and so forth; and information about the peer device - its public key, its endpoint where the peer device can be reached, private IPs associated with the peer device and so forth. It's straightforward, particularly for a VPN. Every pair of devices requires a configuration entry, so the total number of configuration entries does grow quadratically in the number of devices if they are fully interconnected to each other. To connect devices using Tailscale, you install and log into Tailscale on each device. Tailscale manages key distribution and all connections for you. This can be particularly useful if some of the devices belong to non-technical users."

Regarding connectivity: "WireGuard ensures that all traffic flowing through two devices is secure. It does not ensure that those devices can connect. That's up to you. WireGuard has a persistent keep-alive option, which can also keep the tunnel open through NAT devices. But in some cases, to ensure that your devices can communicate, you may need to open a hole in your firewall, or configure port forwarding on your router. WireGuard can detect and adapt to changing IP addresses as long as a connection remains open, and both ends do not change addresses simultaneously. Establishing a connection or reestablishing a broken connection requires updating configuration files."

Compared to Tailscale: "Tailscale takes care of on-demand NAT traversal so that devices can talk to each other directly in most circumstances, without any manual configuration. When NAT traversal fails, Tailscale relays encrypted traffic, so that devices can always talk to each other, albeit with higher latency in that one case. There's no need to modify firewalls or routers. Any devices that can reach the Internet can reach each other. Tailscale traffic between two devices on the same LAN does not leave the LAN."

For security: "Tailscale and WireGuard offer identical point-to-point traffic encryption." Performance. Oh, wait, I did skip something. They said: "Using Tailscale introduces a dependency on Tailscale's security. Using WireGuard directly does not. It's important to note that a device's private key never leaves the device, and thus Tailscale cannot decrypt network traffic. Our client code is open source, so you can confirm that yourself.

"With the Team and Business plans, Tailscale adds an ACL" - so Access Control List - "layer on top of WireGuard, so that you can further control network traffic. You can do some of this directly with WireGuard by not setting up tunnels between devices that should not communicate, or by using the operating system firewall to control traffic flow. Tailscale ACLs allow you to express ACLs for everything in a single place using users, groups, and tags, which are easier to maintain than a list of which device pairs may communicate. Even without the Team or Business plans, Tailscale offers some basic unidirectional ACL controls. For example, any node may turn on 'Shields Up' mode, which prevents all incoming connections."

And of course I got a kick out of that. And I should mention that Tailscale is completely free for personal use with a single user, and it offers single sign-on and multifactor authentication and will link up to 20 devices for free. Multiple users, access control lists, advanced network segmentation and other group features are billed for the pay-for plan per user per month.

So, okay. Just a couple last things. Performance: "Using WireGuard directly," they acknowledge, "offers better performance than using Tailscale. Tailscale does more than WireGuard, so that will always be true. We aim to minimize that gap, and Tailscale generally offers good bandwidth and excellent latency, particularly compared to non-WireGuard VPNs. The most significant performance difference is on Linux. On Linux, WireGuard is available as a kernel module. Tailscale currently uses the user space WireGuard implementation, which has more overhead. The most common scenario in which Tailscale users notice bandwidth or latency issues is when Tailscale is relaying network traffic, which is unavoidably slower. In that case, the devices would be unable to connect at all using WireGuard directly, so no direct comparison is available."

And I'll just note that I think they're being a little bit excessively harsh on themselves. I think they're trying to be scrupulously factual because any performance hit would be initial setup once you've established point-to-point link, except as that issue regarding Linux in user space versus the kernel. I guess you could perform a benchmark yourself and see whether you see much difference. I don't think you'll find much.

And finally, bonus features. They said: "By design, WireGuard provides secure point-to-point communication. It's intended to be a building block. Tailscale has a broader set of features. For example, we offer MagicDNS to make it easier to reach other devices on your VPN. We have out-of-the-box support for subnet routing to allow employees access to an office network via an exit node running Tailscale. And more features are in the works."

So the bottom line, they say: "We suspect that using WireGuard directly will be most appealing if you have a small, stable number of Linux servers whose connections you want to secure. Using Tailscale will make the most sense if you want things to just work, you are administering a VPN for many different users, or you want the extra features or centralized ACLs that Tailscale offers. But everyone's network and needs are different. And we've helped debug a lot of networks. When we say everyone's network is different, we know whereof we speak, and we mean it. Using WireGuard directly is a very reasonable choice; and if you're thinking about doing it, we encourage you to give it a try. If you later decide that you want the convenience and extra features that Tailscale offers, it's easy to switch."

So I just wanted to make everyone aware of this. I think it sounds like a very cool add-on, especially free for a single user who likes the idea of switching to WireGuard, but wants a little, you know, also likes the additional features, like that feature overlay that WireGuard offers. And really I was reminded of CryptoLink, which was my project that was targeted doing exactly these things. Except as we know I chickened out due to my concern that governments were eventually going to require that we refer, you know, we end up with what we would call "warrant-compatible encryption," and we still don't know how that's going to shake out. But in any event, this looks like a beautiful solution.

I love the idea of having multisite networks statically glued to each other into a simple, big, privately routable network. The downside, of course, is the threat presented by today's ransomware. When you were talking about CrowdStrike earlier, Leo, I was thinking of exactly this problem. You know, I'm unwilling to keep static links up between my various facilities. I would love to just have my network here where I'm working part of the GRC network at Level 3. But I just can't take the chance of having everything on the same network.

So what I do is I bring the link up when I need it and bring it down when I don't. Of course you could also do that with WireGuard. It's just nice to have everything glued together. And I know there are lots of scenarios where it would make sense to do that. You can imagine a corporate environment with satellite offices, or people at home who just want to tie their systems statically into a central enterprise hub. So I just wanted to put it on everyone's radar. It looks like a great offering. Offers a useful package for free. I think they were $5 per user per month for the first step up from the free package. And for all of the extra controls that they offer, it might make sense for people.

Leo: We're having some good conversations about WireGuard on our FLOSS Weekly show, if you're interested.

Steve: Yeah, good. They really did, the WireGuard team, it ended up expanding beyond Jason. And I would use it without any hesitation.

Leo: Jason's on FLOSS Weekly 626, which is last April, if you want to hear Doc and Jonathon talking to Jason Donenfeld, who is the creator of WireGuard. A work of art.

Steve: I wanted to mention that a couple of our listeners caught me mentioning that the problem with Chrome having as much as a five-second delay - this was my discussion last week - having a five-second delay while it's doing that wacky color-based website spoofing detection. I said, yeah, you wouldn't want your password manager or form fill-in to automatically populate the field, and then you hit login before you get the notification that it's a spoofing site. Several people said, uh, Steve, one of the advantages of an auto-form-fill password manager is it's not tricked the way users are. If the URL has a lookalike domain, that's not going to populate. And so you're going to go, wait a minute, why isn't it filling itself in? And it's like, oh, it's because that's a fraudulent site.

So I stand corrected. Thank you, listeners, for paying such close attention. And I wanted to make sure everybody realized that that was the case. I don't say that often enough, and I should, that that is clearly a benefit of a password manager like Bitwarden, is it looks at the exact URL, and only if it's an exact...

Leo: It's not fooled, yeah.

Steve: ...match will it do the population. Unlike the typical user, who's like, oh, yeah, my password is monkey123, and I'll type that in.

Leo: On bravei dot com, yes.

Steve: So a listener, Clay Seale, tweeted: "Steve: Any recommendations after 'Project Hail Mary'? It was an outstanding read." And so I wanted to share that the "Bobiverse" trilogy is highly and often recommended by our listeners as being fun and a bit whimsical, I guess, in some way reminiscent of "Project Hail Mary."

Okay, so the teaser on Amazon about the book, it reads: "Bob Johansson has just sold his software company and is looking forward to a life of leisure. There are places to go, books to read, movies to watch. So it's a little unfair when he gets himself killed crossing the street.

"Bob wakes up a century later to find that corpsicles have been declared to be without rights, and he is now the property of the state. He has been uploaded into computer hardware and is slated to be the controlling AI in an interstellar probe looking for habitable planets. The stakes are high, no less than the first claim to entire worlds. If he declines the honor, he'll be switched off, and they'll try again with someone else. If he accepts, he becomes a prime target. There are at least three other countries trying to get their own probes launched first, and they play dirty.

"The safest place for Bob is in space, heading away from Earth at top speed. Or so he thinks. Because the universe is full of nasties, and trespassers make them mad - very mad."

Leo: This is a great premise. I love it. I love it.

Steve: So I do not yet have any firsthand knowledge or recommendation myself. But Leo, I feel as you do about that hook. I'm currently on Book #19 of my incredibly enjoyable reread of Ryk Brown's 30 books so far out of his planned 75 Frontiers Saga. I love the Frontiers Saga. As we know, I love reading science fiction. So perhaps the bar isn't that high. And it does feel as though it is time finally to move on. So I doubt I will reread them again until I'm in my dotage, fully resigned from software development and R&D in areas of human health and wellness.

And I think that from now on I will hold off on anything Ryk does until he finishes each subsequent 15-book arc since it's too frustrating to be waiting month after month for the next book to drop. So for what it's worth, I have also received a lot of positive feedback about the Frontiers Saga, so it's not just me loving them. In any event, once I finish this current reread, the Bobiverse trilogy, beginning with "We Are Legion," will be up next.

Leo: Yeah, that sounds good. I'd like to read that. Very funny.

Steve: So since I got a ton of feedback after sharing my story of the recovery of that inaccessible BitLocker-encrypted drive, I thought I'd share an engaging recent anecdote that I posted to the spinrite.dev newsgroup last Saturday after I lost an entire day.

Leo: All right, Steve. I can't wait to hear the story of your lost day.

Steve: So my posting, I'll just read what I posted to the newsgroup last Saturday. I said: "Gang, I hadn't checked in for a while, so I thought that after a lost day of work, yesterday, I'd do so before settling back down to it. The day before yesterday, the 29th, around noon, the ecommerce system I wrote back in 2003 began failing and reporting timeout errors when attempting to connect to our backend credit card processing provider. I would normally have been informed of this immediately, but the monitoring system I have been using for years" - actually ever since '03 - never recovered after a power outage a few months back, and I hadn't wanted to take the time away from work to fix it.

"So yesterday, Sue let me know that a few would-be customers had reported that they'd been unable to purchase SpinRite. She sent me a text message which captured my attention. The short version is that I spent nearly the entire day pulling out what very little hair I have trying to figure out WTF was going on. The error reports that my own code was logging was a 0x2EE2 from the WinINet API, which is 'operation timed out,' and

Windows' own error logging was complaining of 'TLS handshake errors,' which could have been more informative.

"That sent me off on what turned out to be a wild goose chase, assuming that my provider had changed their TLS connection parameters in a way that was incompatible with my aging Win2008 R2 Server. The fact that DigiCert, also their cert provider, had just revised some of their intermediate certs, and GRC's server certs were reporting an invalid intermediate, didn't help.

"Many hours later, the final clue came when a ping to the service to the IP address I received from NSLOOKUP worked, whereas a ping to the same service with 'ping' doing the IP lookup did not. When I looked more closely, I saw that NSLOOKUP and ping were resolving different IPs. I use my network's own Unix BIND instance as my recursive DNS resolver, so I became suspicious of it. But additional testing showed that it wasn't at fault. That was at the end of the day.

"So I finally thought, fine. I'll just force the resolution to an IP that I know works by adding an entry to the local HOSTS file. And there I found the override to that domain's old IP, already in the local HOSTS file. For some reason, sometime in the distant past, I had hard-wired the backend provider's IP myself. And then, two days ago, they finally changed their server's IP, no doubt doing so with great forethought, running over all IPs while giving DNS caches times to expire and refresh, and my old hard-wiring didn't allow my system to follow. I removed the entry from the HOSTS file, and everything worked again perfectly. I love computers because they always do exactly what we tell them to."

So anyway, spent a day, couldn't figure out what was wrong. It was because who knows how long ago, for some reason, I don't even remember why would I have done that, why would I have wired that domain name to their IP.

Leo: Well, you were about to do it again, so I'm sure there was a good reason then.

Steve: Yes. Very good point. I was about to do it again.

Leo: Wow. That's like an "ohhh" moment, where you slap your face.

Steve: Yes. And, you know, it was costing me SpinRite sales.

Leo: Yeah, yeah.

Steve: Everybody was saying, you know, it was timing out.

Leo: Well, that's the thing. You're working under pressure because you've got to fix it. You can't go to bed with it broken.

Steve: Exactly. And that's what it was, was it was like, okay. I can't figure out what's wrong. I'm just going to put some glue in here to fix it. And it was like, oh, wait.

Leo: I already did.

Steve: There's already glue in there. And it's gummed up the works.

Leo: Wow. Yeah, yeah. This is why engineering departments have protocols and log books and all this stuff, because this stuff is so easy. If it's just you, you're not going to document all the changes you make.

Steve: Well, sadly there's no one to blame. Not like I ever had Harvey, who was that intern who wandered off. Like, eh, no.

Leo: That's so funny. Oh, lord.

Steve: Anyway, I finished my note by giving everybody an update on SpinRite. And in fact I thought of you, Leo, because you mentioned macros in assembly language on Saturday.

Leo: Yeah, we were talking about that. I was thinking of you, yeah.

Steve: So I wrote: "On a happy note, in the same vein of loving computers because they do exactly what we tell them to, I wanted to report that the use of my built-to-suit virtualized I/O function, and the new way I'm handling errors occurring in a massively long block of sectors, has turned out to be somewhat jarringly correct. As can happen when everything is designed properly, everything has just fallen into place by itself.

"When I was interrupted yesterday" - by that self-created problem - I said: "I was working on synchronizing SpinRite's logging system with the new inner loop, since the information that can be logged has changed significantly. It took me a while to understand why I had originally built the logging system the way I had, since it seemed way over-designed and overly complex. It uses short log entry trigger tokens which are accumulated into a queue, then later flushed, expanded into their full-size log entries and written.

"I couldn't figure out why I went to so much work until I remembered the challenge that I had taken up and accepted, that SpinRite could log onto the same FAT partition that it was operating on, without any compromise. This meant that the log file itself might be written to the same track and sectors that SpinRite was in the middle of working on at the same time.

"But I already had full track virtualization. I was intercepting DOS's writes to the drive through the BIOS or device drivers, or compression drivers <shudder> and rerouting any reads and writes to the drive to a virtual buffer of the current track. So that wasn't why I was deferring the logging with a queue. It turned out that I was deferring the logging with a queue of short event tokens since I was later reusing the track buffer for token expansion to reduce SpinRite's memory footprint to the absolute minimum." Remember back then we didn't even know we were going to have 640K. There were systems with 320K or less. And people would have device drivers and TSRs and other stuff bloating their DOS.

So I wrote SpinRite so that it didn't use a byte of RAM that it didn't have to in order for it to be able to work in every case. So what I ended up with was I ended up with a tokenized log system where once SpinRite was through with the track, it would put it all

back. That would free up the 32K track buffer that I could use to expand the logging events into as I wrote them out to the device. So I really engineered this thing like crazy.

And I finished up: "Anyway, the system I built is pretty slick. It uses macros to implement its own meta language to make the implementation and result visually clean and clear. Although I don't need any of that anymore, it's all in place, and it works, so I'm leaving it alone. I just needed to remember and understand how it worked so that I could confidently modify and extend its operation today." And I finished: "I'm returning to work on SpinRite, now with the mystery of the dead ecommerce system nicely resolved. Sheesh." So yes, Leo. What you and I both mentioned was the idea that it was possible, even though you're writing in assembler, to use macros to design a meta language so that you are able to implement something at a higher level which is expanded by the assembler and doesn't require any runtime interpretation.

Leo: Yeah. It's very simple, but it saves a lot of typing.

Steve: Yes, it does.

Leo: You do stuff over and over and over again in assembler. There's just some things you just do all the time.

Steve: Well, and MASM, Microsoft's assembler, it has - it's called PROC and ENDP.

Leo: Right.

Steve: So I'm able to define something and say PROC, and then I say uses, you know, EBX, ESI, and EDI, and then give it a list of parameters that this procedure will receive and what types they are. And it's like, yeah, it's not like a string type, but it could be a pointer, and it can be a byte, well, not a byte actually, you can't push or pop bytes, but a word or a double word. And so within the constraints of the machine code, you're able to create very good-looking code. And the compiler, or the assembler rather, it does all of the stack setup. You're able to define locals, so it creates a stack frame for you, and does a lot of that stuff that we're used to only getting in high-level language in assembly language to make it look really good.

Leo: That's the M in MASM, Macro, yeah.

Steve: That's right. Okay. The BlackMatter Interview, or 'Tude from Russians. The security firm, as I mentioned, Recorded Future, introduced their exclusive interview to a representative, well, introduced their exclusive interview of, sorry, of a representative of the group which now calls itself BlackMatter. They opened their interview by saying: "In July, a new ransomware gang started posting advertisements on various cybercrime forums announcing that it was seeking to recruit partners, and claiming that it combined the features of notorious groups like REvil and DarkSide.

"Named BlackMatter, the gang said it was specifically interested in targeting large companies with annual revenues of more than $100 million. However, the group said some industries were off limits. It would not extort healthcare, critical infrastructure, oil

and gas, defense, non-profit, and government organizations." I notice that in this they didn't mention education.

Anyway, they said: "A representative from the group talked to a Recorded Future expert threat intelligence analyst recently about how BlackMatter is learning from the mistakes of other ransomware groups" - or maybe their own previous mistake - "what they look for when they recruit partners, and why they avoid certain targets. The interview was conducted in Russian and translated to English with the help of a professional translator, and has been edited for clarity."

Okay. So as we're listening to this conversation, remember that there's no honor among thieves, and we already know with virtual certainty that BlackMatter is DarkSide, sharing virtually identical and unique codebases. And I'll also note, based on the timing of this, not being off the air very long; right? They're making too much money to go away for long. So that all further explains why they didn't further obfuscate their own crypto. It's like, yeah, why bother? We'll just change our name.

So Dmitry is the guy at Recorded Future. He says - and this was conducted online in writing as opposed to real time, because at one point they talk - the BlackMatter group talk about getting the question and checking around for the answer. So Dmitry asks: "Your product appeared quite recently; and as far as we know, there have been no public attacks using BlackMatter yet. How long ago did you start developing it?"

BlackMatter replies: "There haven't been any attacks yet, if you are judging by the public blog. In fact, there have been, and the companies we attacked are already communicating with us. As long as the negotiations are successful, we do not publish a blog post on the main page of the blog. The product has been in development for the past six months." Uh-huh. "Perhaps it seems simple, judging by the blog or the communication page. But it is not. What users see publicly is the tip of the iceberg."

Then they continue: "Before starting the project, we studied the following products in detail. LockBit has a good codebase, but a skimpy and non-functional panel." And by the "panel" they're talking about the interface that the affiliates use in order to log in and manage their particular own instance of the ransomware. They said: "At the time we used their product." So that sort of sounds like they're saying these guys were once affiliates who used LockBit, and they decided to become ransomware authors themselves. They said, and this is a weird analogy: "If you compare it to a car, you can say that this is a Japanese car production line with good engines, but an empty and non-functional interior. You can ride one, but with little pleasure." Okay? So they don't like the control panel that LockBit was using.

They said: "REvil is a good product on the whole, time-tested software. Since GandCrab, they haven't made any significant edits since that time. And actually we can confirm that since we talked about the REvil codebase. They said: "A fairly functional panel, but focused more on the overall number of successful 'loads' as opposed to specific targeted cryptography." Okay. They said: "DarkSide is a relatively new software with a good codebase, partly problematic, but the ideas themselves deserve notice, and an interesting web part compared to other Ransomware as a Service."

And then finally they said: "The executable itself has incorporated the ideas of LockBit, REvil, and partly DarkSide. The web part has incorporated the technical approach of DarkSide since we consider it the most structurally correct," he says, "(separate companies for each target, and so on)." And of course were you to actually be DarkSide, then yes, the backend crypto structure would be the same because that's a function of the crypto structure of the code, which we know from analysis is the same.

So Recorded Future asks: "How difficult is it to organize an affiliate program, also known as Ransomware as a Service?" They respond: "On the whole, less difficult than not. The level is important. RaaS can also be offline, when builds are issued via Jabber/Tox. But there is no market demand for this; and current customers, after using REvil and DarkSide, are not ready to take such affiliate programs seriously." In other words, you have to have a good-looking control panel to look like you're really in the game. He said: "We created a project and brought it to the market exactly at a time when the niche is vacant" - yeah, because everyone disappeared - "and the project fully meets the market demands. Therefore its success is inevitable."

Recorded Future asks: "Most recently, the largest groups - DarkSide, REvil, Avaddon, BABUK - have disappeared from the scene. Many researchers believe that this was due to the attention of the top leadership of the United States and Russia to the situation with ransomware attacks. Is this true? Do you think your product will have the same fate?" Their reply: "Yes. We believe that to a large extent their exit from the market was associated with the geopolitical situation on the world stage. First of all, this is the fear of the United States and its planning of offensive cyber operations, as well as a bilateral working group on cyber extortion. We are monitoring the political situation, as well as receiving information from other sources.

"When designing our infrastructure, we took into account all these factors, and we can say that we can withstand the offensive cyber capabilities of the United States. For how long? Time will tell. For now, we are focusing on long-term work. We also moderate the targets and will not allow our project to be used to encrypt critical infrastructure, which will attract unwanted attention to us."

Question: "You mention that your product brings together the very best of DarkSide, REvil, and LockBit. What are their strengths?" They said: "Our project has incorporated the strengths of each of the partner groups. From REvil, Safe Mode. Their implementation was weak and not well thought out. We developed the idea and thoroughly implemented it. We also implemented the PowerShell version of the ransomware variant given the REvil implementation. From LockBit, an approach to the implementation of the codebase. We took some things from there, mostly little things. From DarkSide: First of all, this is the idea of impersonation, the ability of the encryptor to use the domain administrator account to encrypt the shared drives with maximum rights. We also borrowed the structure of the admin panel from there." Uh-huh. Probably the code itself.

Question: "Based on the latest reports published this week, BlackMatter is visually very similar to DarkSide. Can you confirm that your infrastructure is based on DarkSide?" Answer: "We can confidently say that we are fans of dark mode in design. We are familiar with the DarkSide team from working together in the past, but we are not them."

Leo: No.

Steve: Fear not, Alexander. "Although we are intimate with their ideas." Okay. Question: "LockBit 2.0 is considered the fastest locker at the moment. What is the encryption/decryption speed of your variant?" And they respond: "This is not true. After reading the question, we decided to prepare ourselves by downloading the latest publicly available version of LockBit, that's 6.21, and conducting tests. We can state the following: BlackMatter time required, 2.22. LockBit time required, 2.59."

They said - and this is interesting. I did not ever know this. I've never seen this reported. They said: "The tests were carried out under the same conditions. Moreover, LockBit encrypts the first 256K of the file," they said, "which is pretty bad from the point of view

of cryptographic strength. We, on the other hand, encrypt 1MB. Essentially, that's the secret to their speed." Now, that's interesting, Leo.

Leo: So they don't encrypt the whole file.

Steve: No. I've never encountered that. And it's interesting when you think about, it's like, okay. It doesn't kill everything. It kills executables completely. Obviously it covers anything up to, in the case of LockBit, 256K; in the case of BlackMatter, 1MB. That's interesting. But not the whole file. Clearly they do that because they can't afford the time. They're in a big hurry to get this stuff encrypted. And so encrypting the front, a big chunk of the front, they figure, okay, that's enough to merit an extortion payment.

Question: "Are you planning to add new features to the product, following the example of StealBit?" And they said: "Yes, the software is constantly being improved, in terms of the new functions that will appear in the near future, printing the text of the note on all available printers. We also watch our competitors and always implement what we consider promising and in demand by our clients."

Question: "I've already seen several recruiting announcements for your team. How many penetration testers would you like to recruit? Is it easier to work with a small but strong team, or with an army of script kiddies?" Answer: "We are geared at strong, self-sufficient teams with experience, their own technical solutions, and a real desire to make money, not someone who wants to try the business out. We usually filter out script kiddies before they get access to our admin panel."

Question: "Obviously, there are many talented professionals on your team. Why is it that this talent is aimed at destructive activities? Have you tried legal penetration testing?" Answer: "We do not deny that business is destructive. But if we look deeper, as a result of these problems, new technologies are developed and created. If everything was good everywhere, there would be no room for new development." Like we're good for security because the problems that we exploit are being fixed. Oh, okay.

Then they say: "There is one life, and we take everything from it. Our business does not harm individuals and is aimed only at companies. And the company always has the ability to pay funds and restore all its data. We have not been involved in legal pentesting, and we believe that this could not bring the proper material reward." In other words, yeah, it doesn't pay so well.

Leo: We make more money, yeah, extortion, yeah.

Steve: $4 million from some company, yeah.

Leo: Yeah.

Steve: Question: "What do you think about the attacks carried out against Colonial Pipeline's infrastructure or JBS? Does it make sense to attack such large networks?" Answer: "We think that this was a key factor" - gee, you think? - "for the closure of REvil and DarkSide. We have forbidden that type of targeting, and we see no sense in attacking them."

Question: "The U.S. Department of Justice said they were able to recover some of the bitcoins paid by Colonial. How do you think this has happened?" Answer: "We think that the DarkSide team" - and they may have reason to know - "the DarkSide team or their partners transferred bitcoins to web wallets, which led to the seizure of their private keys."

Leo: That's what we speculated, some sort of escrow wallet.

Steve: Yeah, exactly. Question: "You are actively buying access to the networks and declare that you are not interested in government and medical institutions. At the same time, you stated that you will not encrypt a wide range of industries, including critical infrastructure, defense, non-profit, and oil. Who has the last word to encrypt the network or not?" Answer: "The last word is ours. We check each target and decide if it has potential negative consequences for us. The discrepancy between the industries in the blog and on the forum is related to marketing. In personal correspondence we filter out those which we are not interested in."

Question: "What type of primary network access is the easiest in 2021 in your opinion?" They say: "We do not work with VPN and other time-consuming types of initial access, but are focused on getting direct access to the network immediately." Which I thought was interesting. They don't like VPN access. They want RDP or, you know, they're getting greedy. They like domain admin, please.

Leo: Didn't they use a VPN to get into Colonial Pipeline?

Steve: Yeah, yeah. But, yeah. Who knows what that's about? And certainly a VPN would give you lots of access.

Leo: Yeah. I would prefer give me passwords to server, please. Thank you very much, yes. That's my preferred way of getting in.

Steve: So, question: "What carries more effect motivating the company to pay, the infrastructure being unavailable or the fear of a data leak?" Answer: "It varies from company to company."

Leo: But we use both, just in case.

Steve: Yeah. "For some it is important to maintain confidentiality, for others it's restoring infrastructure. If the network is completely encrypted, and there is also a risk of data being published, the company will most likely pay."

Question: "Unknown" - that's the name given to REvil's public spokesperson - "spoke about a special outlook toward insurance companies. Do you think that if insurance companies abruptly stop covering ransomware incidents, it will change your interest in ransomware?" Answer: "It will not change. The companies will continue to pay money regardless. It is possible that the amount being paid may decrease. Now the insurance fees have increased. But fearing that they will be left alone in the situation, everyone will continue buying the insurance."

Question: "What's happened with Unknown? There are a lot of rumors. Can you clarify the situation?" Answer: "We do not know. Most likely, after the last payment, he went on vacation or is preparing a rebranding of their project."

And then the last one, last question: "Tell me a secret." And the answer: "There are no secrets. But we believe in our motherland, we love our families, and we earn money for our children."

Leo: We are good people. We don't hurt anyone. No. Is for the children. That's why we do it.

Steve: That's right.

Leo: That's depressing. I almost kind of regret giving these bozos any attention at all. But it is interesting. It's informative.

Steve: Yeah.

Leo: Oof. Oof.

Steve: Yup. Forewarned is forearmed.

Leo: Yeah, yeah, yeah. And they're really, you know, it's so interesting how they rationalize. Oh, we don't hurt individuals. We hurt no people. Just big companies.

Steve: Just big fat Western companies.

Leo: Yes, is for our children we do this. So sad. Well, Steve, thank you. I appreciate it, as always. A very interesting Security Now!. We do the show every Tuesday, 1:30 Pacific, 4:30 Eastern, 20:30 UTC. So you can watch us do it live, if you want, if you want the latest, freshest version of Security Now!. The livestreams are at TWiT.tv/live, audio and video. People who listen live often like to chat with others also listening live. That's irc.twit.tv. That's our IRC channel.

If you're just looking for copies of the show after the fact, Steve has both 16Kb and 64Kb audio, the 16Kb for the bandwidth-impaired. That's a unique format. Only he has it: GRC.com. Also you'll find transcripts there that are really helpful for searching and reading along as you listen: GRC.com. While you're there, pick up the world's best mass storage maintenance and recovery utility, SpinRite v6. Version 6.1 is in progress. You buy it now, you'll get 6.1 for free, but you'll also get to participate in its development on the SpinRite forums and all of that.

Actually there's a lot of great stuff at GRC.com, not just the forums, but all sorts of information about a variety, a wide-ranging variety of topics because Steve is absolutely wide-ranging in his interests.

We also have copies of the show at our website, TWiT.tv, 64Kb audio and video. TWiT.tv/sn is the specific link. Once you're there you'll also see a link to our YouTube

channel. There's a Security Now! YouTube channel with all the shows there. There's also links to the various big-name podcast players, but you also get an RSS feed, so you can subscribe in any podcast player.

But do us a favor. If you subscribe in Google Podcasts, Apple Podcasts, Pocket Casts, Overcast, if they have a directory and a chance to review, please give us a five-star review. Let the world know. You know about Security Now!. But let everybody else know. The more people that listen to this show, I think the better off we all will be. We'll be a lot safer, anyway. So a five-star review would be much appreciated.

I think that concludes everything I needed to tell you, all the business parts of the show. Steve will be back next week. Have a great week.

Steve: Will do.

Leo: See you then.

Steve: Thanks, buddy.