The WiFi Frag Attacks

Description: This week we follow up on last week's "News from the DarkSide" with a surprising amount of happenings including the dark web's rejection of further ransomware. We look at blockchain analytics which are used to follow the dark money, the mixed signals now coming from the DarkSide group, and a live list of more than 2,000 ransomware attacks during the past two years from the dark web. We cover last week's Patch Tuesday that you won't want to miss. We have a bit of miscellany, including the "Unidentified Aerial Phenomena Task Force" which is actually a thing, and some closing-the-loop feedback from our listeners regarding last week's Andy Weir's "Hail Mary" book mention. Then we take a close look at the biggest non-Colonial Pipeline news from last week: a new round of research which revealed a range of attacks on WiFi's security.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-819.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-819-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. We are going to kick off by explaining last week's Picture of the Day for those of you who couldn't quite figure out why it was funny or even interesting. But then we're going to talk about the DarkSide attack and what's happening to the DarkSide hackers. We'll also get a review of Patch Tuesday. That was last Tuesday. Steve has a thumbnail for you. And then finally we're going to wrap things up with this new WiFi attack that affects every version of WiFi encryption known, the Frag Attacks. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 819, recorded Tuesday, May 18th, 2021: The WiFi Frag Attacks.

It's time for Security Now!, the show where we get you and your loved ones to safety somewhere in the middle of your house, let's hope within a concrete bunker. It is getting crazy out there. But there is nobody better to report that than Mr. Steve Gibson, the host of Security Now!. Hi, Steve.

Steve Gibson: Yo, Leo.

Leo: What's up?

Steve: Great to be with you again. Well, the big news, actually it was like a week ago, was the announcement of some new attacks on WiFi. So I thought, okay, that's what we're going to talk about. But then we just kept getting more news, as our last week's

episode was titled, from the DarkSide. So we're going to follow up on last week's News from the DarkSide with a surprising amount of the happenings, I mean, including the dark web's rejection of further ransomware. We look at bitcoin analytics, which are used to follow the dark money as it moves around. We've got mixed signals now coming from the DarkSide group themselves.

And something that's really interesting, when I was digging around I found a live list of more than 2,000 ransomware attacks during just the past two years that is posted and maintained on the dark web. We're also going to cover last week's Patch Tuesday because this is the third Tuesday of the month, and we don't want to miss that. We've got a bit of miscellany, including - I don't know, Leo, if you saw "60 Minutes" from Sunday?

Leo: No.

Steve: The second of the three segments that "60 Minutes" always does, they do three per Sunday, was on the "Unidentified Aerial Phenomena Task Force," which is actually a thing.

Leo: Oh, yeah. They don't call them UFOs, notice.

Steve: That's correct, they're no longer UFOs. They are UAPs.

Leo: Yeah, because they don't want to imply that it's really an alien, it's just we don't know what the hell it is.

Steve: We don't know what it is, but it appears to be something is going on.

Leo: Well, it is something, but I don't think it's aliens. That's a little [crosstalk].

Steve: I'm not saying it is. I'm just, you know, these things are behaving in ways they don't understand.

Leo: Right.

Steve: So we'll talk about that. Also we've got some closing-the-loop feedback from our listeners regarding last week's recommendation of Andy Weir's "Hail Mary" book, which you and I were talking about before we began to record this. So we'll touch on that with no spoilers.

Leo: Yeah.

Steve: Then we're going to take a close look at the biggest non-Colonial Pipeline news from last week, which as I mentioned is a new round of research which comes to us from some people who have paid their dues and whose research we believe. They were the

guys behind the original, it was like 2017, the WiFi Frag Attacks. I mean, not frag attacks, no, sorry, the - now I forgot it because I got myself confused with frag attacks. Frag Attacks is this week. It was - we'll get to it when we get to it.

Leo: They were KRACK; right? It was called KRACK.

Steve: KRACK, the KRACK Attacks, yes. They are back with more attacks after the KRACK attacks.

Leo: KRACK is back. This time it's FRACK. All right. Big show. Really big show. And will you explain the Picture of the Week from last week for those...

Steve: Yes, I will.

Leo: No spoilers. And we have a new Picture of the Week.

Steve: Oh, good point, good point. We did promise to close that loop. Yup.

Leo: Yeah, yeah. Do you want to explain first, or show the new one?

Steve: Explain first.

Leo: Okay. Let me pull up the old one.

Steve: If I were to do a two-word clue that would, like, people would smack their foreheads against their hands, I would say "Doppler shift."

Leo: Yeah, that should pretty much do it for you.

Steve: That ought to do it.

Leo: All right. So let's show you the picture again real quickly. So it starts - there's two frames, two panes. One, an old man looking to the left. There's a little blue car coming toward him.

Steve: Towards him, yes.

Leo: Looking to the right, there's a big red car going away from him.

Steve: Right.

Leo: How did this happen?

Steve: So we know a couple things. Everyone's familiar with the classic phenomenon because it's not something we...

Leo: [Demonstrating]

Steve: Exactly, that we experience when, for example, a train roars past. You hear a higher frequency as it's approaching and a lower frequency as it's leaving because the waves, in this case sound waves, are compressed as it's moving towards you because the source is approaching you, and the reverse happens as it's moving away. Well, exactly the same thing happens with light, at of course a way higher, well, not air being compressed and rarified, it's electromagnetic radiation. So you get both physical foreshortening, thus the scrunched-up car which is blue because that's a higher frequency of light as it's approaching. And as it's leaving you get it appearing stretched out and red, which is a lower frequency of light.

Leo: Which Edwin Hubbell, the astronomer, called "red shift." Right?

Steve: Exactly, you have blue shift and red shift, exactly.

Leo: That's what gave it away to me. Hubbell in 1929 figured out that you could use the shift in the spectrum of the light of stars to determine how far away the star was, which is pretty darn cool.

Steve: Exactly, by determining their relative motion to you.

Leo: Yeah, yeah.

Steve: So very cool. And this week's picture is just sort of, comparatively, a throwaway. I had it in the stack. You stumbled upon it last week, probably from someone posted it in the chatroom. I mean, it's fun. It shows the classic plastic-shelled 3.5" diskette that has a - actually I have a Sony label that looks just like that, but mine does not say "Bitcoin Wallet" on it. I wish it did because then maybe there would be a chance I could recover it.

Leo: You could use SpinRite to get it back.

Steve: That's right. And there have been many, you know, a lot of fun has been had with the idea of messing magnets with diskettes of all forms through the years. So here we have probably a strong round refrigerator magnetic, looks like it's on a refrigerator. I'm familiar with that texture of plastic-coated sheet metal that the "Bitcoin Wallet" labeled diskette is being held against the refrigerator with. So anyway, yes, how not to store your cryptocurrency. I wouldn't put it on a diskette, by the way, anymore. I mean, they're reliable, but there's way better ways to do that. So anyway, just sort of a fun picture. And we've got more coming in the future.

Okay. So some DarkSide follow-up. The team at FireEye - they also call themselves Mandiant, the research group. Eight of them put their names on this report because it was extensive. And I'm just going to talk about the first third of it because they go deep into the operating mechanism of the actual ransomware that DarkSide is known to be pushing and which of course now famously infected the Colonial Pipeline organization. They've done a bunch of deep and delicious research into the group and their software. And they originally took this work public last Tuesday on the 11th, while we were doing this podcast, essentially, last week. But after the news of the apparent DarkSide takedown surfaced, they updated their post just last Friday, adding the following preface.

They said: "Mandiant has observed multiple actors cite a May 13th announcement that appeared to be shared with DarkSide RaaS (Ransomware as a Service} affiliates by the operators of the service. This announcement stated that they lost access to their infrastructure, including their blog, payment, and CDN servers, and would be closing their service." That is to say, DarkSide apparently announcing that they're closing their service. Now, I've got a little story about Toshiba here in a minute that sort of makes you wonder about that.

But they also said: "Decryptors would be provided for companies who have not paid, possibly for their affiliates to distribute. The post cited law enforcement pressure and pressure from the United States for this decision." And the FireEye Mandiant guy said that: "We have not independently validated these claims, and there is some speculation by other actors that this could be an exit scam." So I'm just putting that out there because it's out there. We don't know one way or the other.

What we do know is that beginning in November of 2020, the Russian-speaking actor known as "darksupp" (D-A-R-K-S-U-P-P) began advertising the DarkSide Ransomware as a Service on the Russian language forums, two of them, exploit.in and xss.is, obviously as in cross-site scripting. And interestingly, in the past few days, both of these sites, and I've got a lot more to say about that in a second, have indicated that they would no longer host ads and forums or postings, contents, and threads, for ransomware services, stating that it has drawn too much unwanted attention from law enforcement. I actually - we have some translated-from-Russian quotes that we'll get to. Anyway, since that's also big news, we'll have more to say about that later.

Okay. But last month, April 2021, darksupp, apparently like the guy behind DarkSide, posted an update for the DarkSide 2.0 Ransomware as a Service that included several new features and a description of the types of partners and services they were currently seeking. And so from that we gain some more information about them that we didn't have before. Affiliates retain a percentage of the ransom fee from each victim. Of course I would argue affiliates get the lion's share, right, of the ransom fee, which was one of the things that impressed us when we first started talking about this several years ago was that the services were doing the right thing by basically taking a commission, essentially.

So based on the advertisements that have now been seen, the operators, that is, the Ransomware as a Service operators, in this case DarkSide, take 25% ransom fee when the amount paid is less than half a million dollars. And that decreases from 25% for less than a million dollars down to 10% for fees greater than 5 million. In addition to providing builds of DarkSide ransomware, the operators of this service also maintain a blog accessible via Tor.

Leo: I think it's ironic that Apple takes a larger cut on the App Store than DarkSide does of the ransomware.

Steve: Yes. Oh, and Leo, on the next page of the show notes - you might want to put this on the screen - we have a picture of the control panel that the affiliates use in order to do this. It's sort of amazing. The actors use this site, their Tor site, to publicize their victims in an attempt to pressure those organizations into paying for the non-release of the stolen data. A recent update to their underground forum advertisement also indicates that actors may attempt to DDoS victim organizations.

The actor darksupp, who's apparently behind DarkSide, has stated that affiliates are prohibited from targeting hospitals, schools, universities, nonprofit organizations, and public sector entities. And this may be, as we would imagine now, an effort by the actors to deter law enforcement action since targeting these sectors may invite additional scrutiny. Affiliates are also prohibited from targeting organizations in Commonwealth of Independent States (CIS) nations.

So the original November 2020 advertisement boasts some features which they wanted to make clear of their service, the DarkSide. The ability to generate builds for both Windows and Linux environments from within the admin panel. Encrypts files using - and we knew this last week - Salsa20 encryption along with RSA-1024 public key crypto. Access to an administrative panel via Tor that can be used by clients, meaning their affiliates, to manage DarkSide builds, payments, blog posts, and communication with their victims. The admin panel includes a blog section that allows their clients, their affiliates, to publish victim information and announcements to the DarkSide website for the purposes of shaming victims and coercing them to pay ransom demands.

Then in an update that we talked about, middle of last month, in April, they added automated test decryption. They said the process from encryption to withdrawal of money is now automated and no longer relies on support, meaning there's no response delay from darksupp and his minions behind the scenes. It's all now an automated process. They're also available, they have DDoS for targeting both at Layer 3, which is at the network layer, and Layer 7, at the protocol layer.

And they said: "Seeking a partner to provide network accesses and a person or team with pentesting skills." And just for entertainment value, and actually to show how slick and polished this looks, I have in the show notes a screenshot of this control panel, which is available through the Tor network, a means to get to their site, showing all the switches and bells and whistles and stuff that is there.

Leo: It's really kind of polished.

Steve: It really is.

Leo: It's surprising. But it shows you that they're acting, they feel, with complete impunity. And probably because they're Russian nationals, maybe even because they have some government protection, they just don't feel vulnerable to anything. So they figure, well, let's do it right. Let's make a nice little site here.

Steve: Right.

Leo: They're probably very good coders.

Steve: Their physical security is safe.

Leo: Right.

Steve: They feel like they're able to put things up in Tor. They're transacting using bitcoin. So it's like, you know, nanny nanny nanny, you can't get us. So would-be affiliates are required to pass an interview, after which they're provided with - yes, they're interviewed.

Leo: Yeah, we don't want any - no losers here.

Steve: That's right. That's right. Then they're given access to the admin panel and told to have at it. And using this panel, affiliates can perform various actions such as creating a ransomware build for themselves, providing content to the blog, managing their victims, and contacting the backend DarkSide support if they've got questions or need help. The Mandiant guys have identified at least five Russian-speaking actors who may currently or have previously been DarkSide affiliates. The relevant advertisements associated with a portion of these threat actors have been aimed at finding either initial access providers or actors capable of deploying ransomware on accesses already obtained.

Some actors claiming to use DarkSide have also allegedly partnered with other RaaS affiliate programs, including Babuk and the Sodinokibi, also known as REvil. And I guess it should not be surprising that affiliates might be maintaining relationships with more than one Ransomware as a Service provider at a time. I suppose that at some point the convenience of using the RaaS service, maybe the size of the piece of the action which the ransomware provider takes from the ransom payment would become a consideration, how responsive they are, how trusted they are and so forth. So, you know, nothing prevents the affiliates from setting up relationships with multiple Ransomware as a Service providers.

So in their report the FireEye Mandiant guys provided detailed affiliate-specific information about three specific affiliates. I won't go into each of them here. But it was interesting to see that - I did go through them myself. And I saw that each of the three were clearly distinct and quite different from the others in their means of initial penetration and the way they moved within networks once they were in. They clearly felt like very different threat actors where the only obvious link between the three was that they all decided that they were going to use DarkSide as their ransomware attack package.

And so the Mandiant guys concluded their general discussion in the first part of this long blog posting by writing. They said: "We believe that threat actors have become more proficient at conducting multifaceted extortion operations, and that this success has directly contributed to the rapid increase in the number of high-impact ransomware incidents over the past few years. Ransomware operators have incorporated additional extortion tactics designed to increase the likelihood that victims will acquiesce to paying the ransom prices.

As one example, in late April of 2021, the DarkSide operators published a press release" - get this, Leo, the DarkSide put out a press release - "stating that they were targeting organizations listed on the NASDAQ and other stock markets. They indicated that they would be willing to give stock traders information about upcoming leaks..."

Leo: Everything but the squeal, baby. Just use it all, baby, everything. Gonna make money in every possible way.

Steve: That's right. We're going to switch into the insider trading business, giving stock traders information about upcoming leaks "in order to allow them potential profits due to stock price drops after an announced breach." Wow. "In another notable example," they wrote, "an attacker was able to obtain the victim's cyber insurance policy data and leveraged that information during the ransom negotiation process, refusing to lower the ransom amount given their knowledge of the policy limits. This reinforces that during the post-exploitation phase of ransomware incidents, threat actors can engage in internal reconnaissance and obtain data to increase their negotiating leverage." They said: "We expect that the extortion tactics that threat actors use to pressure victims will continue to evolve through 2021."

And they finished: "Based on the evidence that DarkSide ransomware is distributed by multiple actors," and in fact I think, oh, no, I was getting myself confused about a number that we'll get to in a second. Anyway, they said: "...distributed by multiple actors, we anticipate that" - and this is a term of art now - "TTPs, the tactics, techniques, and procedures used throughout incidents associated with this ransomware will continue to vary." And as I said, given the three very different users of DarkSide affiliates, that they did detail, they really looked like entirely separate entities.

So thanks to the colossal focus brought to bear by the Colonial Pipeline attack which, if nothing else, the DarkSide operators certainly regret in retrospect the industry at large has been able to get a detailed look into the operation of a Ransomware as a Service operation, arguably with more detail and focus than we've had so far. It's been widely noted that cryptocurrency has been an enabling factor for ransomware since it potentially solves the problem of the bad guys getting away with the goods. But does it really? Let's take a look at what we find when we follow the money.

A company called Elliptic was founded eight years ago to develop and deploy blockchain analytics. And they're certainly not alone now. Blockchain analytics is a thing. In this case, they use it for tracking financial transactions on the dark side of the blockchain. Tom Robinson is Elliptic's co-founder and chief scientist. He recently shared what they had learned about DarkSide after aiming their blockchain analytics at DarkSide's transactions. First, they needed to identify DarkSide's wallet. He wrote, based upon - and I guess I've changed the person of this. So based upon their intelligence collection, that is, on Elliptic's intelligence collection and analysis of blockchain transactions, they were able to positively identify the bitcoin wallet used by DarkSide to receive ransom payments from its victims.

Now, "bitcoin wallet" is sort of a shorthand; right? What it actually means is the bitcoin address, which is to say the public key which is associated with the private key stored by the wallet. But because the blockchain is just an immutable ledger of all transactions which have been asserted and verified by the mechanisms, the crypto mechanisms of the blockchain, when you say "we have the wallet," what it really means is they identified the public key associated with one transaction. Then they went back through the entire transaction history in order to track everything that has happened, all the transactions against that particular public key that's been posted to the blockchain ledger.

So what they said was - so that is blockchain analytics. They said: "This was the wallet that received the 75 bitcoin payment made by Colonial Pipeline on May 8th." They said by following the blockchain backwards they were able to determine that this wallet has been active since March 4th, meaning that was the first appearance, right, of a transaction against the same public key and, they wrote, has received a total of 57 payments from 21 different wallets.

Now, depending upon the size of those, they didn't articulate those any further. We don't know if that was 57 individual extortion payments or if other financial transactions were happening using the same wallet. But money was apparently coming in. They said "received a total of 57 payments from 21 different wallets." So not 57 different wallets. But it could have been from some exchanges that would tend to aggregate payments through the exchange. So you would see money coming in from fewer wallets representing still more ransoms.

They said some of these payment amounts exactly match ransoms known to have been paid to DarkSide by other victims, such as the 78.29 bitcoin, worth 4.4 million at the time, that was sent by the chemical distribution company Brenntag a few days earlier, on May 7th. And I don't explicitly cover Brenntag. It's in the tech press now. And it absolutely is a confirmed, another DarkSide ransom that was paid, 4.4 million in this case. They're a big German firm with several, I mean, like 1,200 employees in hundreds of locations. So a big operation.

And they said: "The affiliate payment for both the Colonial Pipeline and Brenntag ransom payments were transferred to the same bitcoin address, which suggests that the same affiliate was behind the original infections and intrusions into both of these organizations. This also revealed that a previously unknown ransom payment for approximately $320,000 was made to DarkSide the day before, on May 10th. And those bitcoins originated from the same exchange that was used by Colonial Pipeline. That was presumably just a coincidence, since Colonial's payment had already been received in full earlier." But as I said, you might have fewer wallets sourcing money into a single wallet because they're being consolidated through an exchange, which as these guys note is the case here.

So they said: "In total, that DarkSide wallet has received bitcoin transactions since its March inception totaling $17.5 million. Now, we know that DarkSide has been active since last August. So previous ransoms would have been paid to other wallets." And again, there's no reason that anyone needs to stick with the same wallet for any length of time. You just, you know, you can create those literally out of thin air by generating a new private key, creating its matching public key, and then having transactions occur against that public key.

So we know what's coming in, and we've seen some affiliate payments going out. What else is going out? Thanks to modern blockchain analytics, the destination wallet of any monies sent from another wallet can also be determined. We know that there are reports that DarkSide had ceased operations and that it had its funds seized. First of all, that's easier said than done. And those in the know are highly skeptical that the people behind DarkSide would be maintaining a so-called "hot wallet" online. The blockchain is, as I have said, able to accrue transactions to a wallet without the wallet being present. And if it's not online, and/or if its private key is not compromised, it's not possible to confiscate a wallet's funds.

So again, they claimed that their money was stolen. It's like, okay, maybe if you're really lame. Anyway, what we do know, thanks to blockchain analytics, is that the wallet in question was emptied of the 5 million in bitcoin it contained last Thursday afternoon. Some have imagined that the funds were seized by the U.S. government. But if so, they didn't get the same ransom bitcoins which were paid to DarkSide since the majority of those coins were previously known to have been moved out of the wallet the Sunday before, on May 9th. So again, the bitcoins, it's not like which bitcoins came in and which ones went out. It's just a quantity. It's not a number of individual things.

So okay. By tracing previous outflows from the wallet, Elliptic was able to gain some insights into how DarkSide and its affiliates were laundering their previous proceeds. They found that 18% of the wallet's bitcoins were sent to a small group of exchanges,

and an additional 4% was sent to Hydra, which is the world's largest darknet marketplace. It serves customers in Russia and the Eastern bloc. Hydra offers cash-out services alongside other illicit things - narcotics, hacking tools, and fake IDs. And these allow bitcoin to be converted into gift vouchers, prepaid debit cards, or cash rubles. So if you're a Russian cybercriminal, and you want to cash out your crypto, Hydra is a place where you would do that. Although in this case, 4% was sent to Hydra from the money that Elliptic was tracking, so not a huge amount.

The owners of any wallet are known and identified only by their public and private keys, which are themselves cryptographically strong random numbers. And bitcoin transactions are conducted between those random numbers, making them inherently anonymous. And in that sense the blockchain is a little bit reminiscent of the Tor network. As we know, traffic goes into Tor nodes and emerges elsewhere such that the interconnections among the endpoints are not directly knowable. But also, similar to the Tor network, the appearance of absolute and perfect anonymity which they both present, it actually begins to collapse as soon as either one, the Tor network or the bitcoin blockchain, begins to interact with the outside world.

By carefully examining and modeling individual transactions on the blockchain, which functions, as I said, as an immutable public ledger, we can know when a ransom victim pays a known sum to a known bitcoin wallet. That transaction exists because it's recorded on the blockchain. And the subsequent movements of its funds can be followed. Bitcoin mixing services, which we've talked about briefly before, have arisen specifically to fragment, confuse, scatter, and gather bitcoin funds to thwart this sort of transaction tracking. And we even now have the notion of so-called "chain hopping," where funds are moved between different forms of blockchain in order to further obscure their movement.

So in the typical cat-and-mouse back-and-forth, there has been an attempt to evade the fact that, yeah, bitcoin has many advantages; but, in reality, perfect anonymity is not one of them. Just as it isn't perfect with Tor.

So one last note is, and I don't know what - the timing of this was interesting because Toshiba was attacked by DarkSide. Last Friday, the French subsidiary of Toshiba Tec Corp., which manufactures barcode scanners, point-of-sale systems, printers, and other equipment, said that it was struck by the DarkSide ransomware, which has impacted some regions in Europe. Toshiba Tec shut down networks between Japan, Europe, and its subsidiaries to, as they put it, "prevent the spread of damage," while recovery protocols and data backups were implemented. Reuters reported that the Toshiba subsidiary said that only a minimal amount of work data had been lost.

Toshiba apparently said: "We have not yet confirmed that customer-related information was leaked externally," though the company did acknowledge that "it is possible that some information and data may have been leaked by the DarkSide group."

So when this news surfaced Friday, DarkSide's leak site was still inaccessible, but DarkSide said that they were taken down. Remember that there is some decoupling here; right? So DarkSide is the source of the ransomware, but it was an affiliate that would have done the breaching of Toshiba. So it's certainly possible that DarkSide could have said, as they appear to have, okay, we're done. This is not worth it, all the grief this is causing. We're sorry about your pipeline. We're out of business. Then an affiliate used the ransomware which had been produced by that control panel earlier to attack Toshiba. Maybe they'll get a free key in order to decrypt themselves. We don't know.

Anyway, when this news surfaced on Friday, DarkSide's leak site, as I said, was still inaccessible. But ZDNet successfully accessed a cached version of their site which had been archived by KELA's Darkbeast search engine, which was news to me. Https://ke-la.com is a search engine for the dark web. The archive data that ZDNet found shows

stolen passport scans alongside project documents and work presentations allegedly belonging to Toshiba. So it appears that some exfiltration did occur, and DarkSide's leak record posted last Thursday the 13th indicates that over 740GB of data was stolen from Toshiba. So exactly as you were saying earlier, Leo, lots of gigabytes of data is often exfiltrated by these guys.

Leo: Yeah.

Steve: And the timing of this is interesting since, as I said, it does follow by several days the apparent takedown of much of DarkSide's operational infrastructure. But again, these things are decoupled.

Leo: Brian Krebs had a really weird trick, I don't know if you saw it on his blog. It turns out DarkSide and many other ransomware programs will not activate if you have a Russian language virtual keyboard installed.

Steve: Keyboard installed, yup.

Leo: Russian, Ukrainian, Belarusian, Tajik, Armenian, Azerbaijani, Georgian, Kazakh, Kyrgyz, Turkmen, Uzbek, Tatar, Romanian, Russian, Azerbaijani, Uzbek, or Arabic. And so it could be, he suspects, could be a couple of things, partly that they don't want to get in trouble with Russian security. Right? So, and he also points out this probably isn't a good mitigation. Although why not?

Steve: Well, what will happen is it's different to have it installed than to have it active.

Leo: Right.

Steve: And right now the ransomware is naive to whether you're actually using the Russian keyboard or not.

Leo: Right, right.

Steve: So it'd be good in the short term. But, yeah, you don't want to rely on it.

Leo: I wouldn't completely count on it.

Steve: It's a cute hack. And Leo, let's take our second break.

Leo: Okay.

Steve: And then we're going to talk about some more stuff. The real world inconvenience caused by the Colonial Pipeline attack has brought unwanted scrutiny unwanted by those

being scrutinized to the entire supporting ransomware ecosystem, and that's from advertising for new affiliates to the laundering of their ill-gotten proceeds. As we know, obviously this new model for ransomware, Ransomware as a Service, requires bringing the presence of that service to the attention of new potential affiliates on an ongoing basis. So it's extremely significant that the two most popular Russian language hacking forums on the dark web, "xss.is" and "exploit.in," after feeling the pressure of that new and definitely unwanted scrutiny, have reacted by banning all future discussion of ransomware across their sites.

Last Thursday the admin of xss.is, which has been serving as the central hub, that is, xss.is has been serving as the central hub for almost all of the top Ransomware as a Service providers, announced that Ransomware as a Service on the forum is hereby prohibited. All prior posts relating to ransomware will be deleted, and no new posts relating to ransomware will be allowed. The admin's post states that: "Ransomware affiliate programs, ransomware rental, and the sale of lockers, as they are called, are prohibited, and all existing topics will be deleted." I found a translation of the Russian language posting, which has some interesting bits of feeling in it.

The translation reads - it's got a couple topics. "Degradation on the face." And again, remember this is a translation from Russian. But this is what was posted by the person running the admin of xss.is: "Newbies open up the media, see some crazy virtual millions of dollars that they will never get. They don't want anything, they don't learn anything, they don't code anything, they just don't even think. The whole essence of being comes down to 'encrypt - get $.' They just run to GitHub, look for locker sorts there, and run to encrypt everything they see. Since our forum is aimed at beginners, this factor is important to us."

Then the next subject was "Too much PR." It says: "Lockers (ransom) have accumulated a critical mass of nonsense, nonsense, hype, noise. When you meet the 'Ransomvarny negotiator' profession, you understand that you are in the looking glass or just crazy. Moreover, 90% of this madness was created artificially, feeding this hype. Those who make good money on this noise," he says, "(exchanges, insurance, intermediaries, media, et cetera)."

And then "Ransomware became political." Peskov, that's the Russian guy who was forced to explain this over on Russia's side, "Peskov is forced to make excuses in front of our overseas 'friends.' This is some kind of nonsense and exaggeration. The word 'ransom' was equated with a number of unpleasant phenomena: geopolitics, extortion, government hacking. This word has become dangerous and toxic." And then he finishes: "Lockers will exist for a long time. This phenomenon was too loudly promoted."

Okay. That's the end of that original posting. The initial response to that by several of the ransomware gangs - so now we're talking the REvil gang, Sodinokibi, well, same, DarkSide, you know, those guys, was that they would be leaving xss.is and moving to exploit.in. That is, until exploit.in followed suit the following day, last Friday, and also moved, as xss.is had, to ban all ransomware discussion and advertising from their forums also. And perhaps not surprisingly, on Sunday, day before yesterday, both forum sites went down due to sustained DDoS attacks, doubtless launched by one or more of the now-banned RaaS gangs.

Xss.is has been struggling to remain online, and here's the post recently made by its admin, and this one was translated to English by a Russian-speaking English speaker. So but this is what xss.is admin just posted: "We are under a powerful DDoS attack. Requests and orders to 'eternally kill' the forum are sent to almost any more or less serious DDoSer in the community. They offer decent money. I'm sure that the attacks were paid for by one of the offended adverts of RaaS programs banned. Guys, calm down. Do not be offended and bring chaos around you. We are tech specialists, not

thugs. For those who are having difficulty getting the message, I will repeat it more bluntly. We receive 'signals,'" which he has in quotes, "including political signals. The era of ransomware is over for all sane people."

Leo: Oh, I wish that were true.

Steve: I know.

Leo: I don't think so.

Steve: I know. He said: "I consider myself and the forum to be an adequate component of our society. Please accept this information. If you happened to work in ransomware, it's time to forget everything and find other activities or come up with other options for monetizing your accesses."

Leo: Go get a job.

Steve: He says: "Believe me, my decision for the ban will save your own," and then asterisks, so probably your own asses. He said: "Honestly, you should strongly and sincerely thank the forum from the bottom of your heart and understand the 'signals,'" again in quotes, "that we all receive. I state this now with all seriousness and responsibility. For those who have some free money left, you can always donate to our favorite forum, XSS, instead of wasting this money on DDoSes. We will keep running hacking contests and pay the authors of the articles. Thank you all for your attention."

So okay. There are some people who live in this world, and their take on this is this is, I mean, obviously, Leo, I agree with you. This is not the end of ransomware. It's not going to go away because the two forums that were the main clearinghouses and meeting places and advertising venues for these things have said not here any longer. But it's going to, I mean, it's going to probably slow things down or change things a bit. The oblique references to "signals," you know, we receive signals, including political signals, strongly suggests that there is an overwhelming amount of anti-ransomware pressure being brought to bear in the wake of this Colonial Pipeline disaster.

Leo: As there should be, yes.

Steve: Exactly. And of course it's not up to the admin of this popular Russian meeting place to unilaterally declare that, quote, "The era of ransomware is over for all sane people." Unfortunately, it's turned out to be highly lucrative, so it will continue. But this does suggest that moving forward the organization of Ransomware as a Service will likely need to be conducted much more quietly and less overtly than it has been until now. And it probably also means that to some extent the exploitation of these ransomware lockers, you know, the actual ransomware itself, may return to their previous origins, being used more by their own developers than those who were able to farm out that and create the whole affiliate concept.

Okay. So I have one other really cool tasty bit. During my recent digging around, I stumbled upon a live spreadsheet which purports to list, and based on my quick checking appears to, the past two years of ransomware attacks by victim, gang, and date. At the

moment, this list carries the headline "List of victim organizations (2,203) attacked by ransomware gangs (34) released on the dark web." The list appears to have been compiled by an organization calling themselves DarkTracer, and they have a nice-looking site. DarkTracer (T-R-A-C-E-R) dot com. And it likely lags a bit in its listings since it does not yet list the Colonial Pipeline attack. But to check it out a bit, I noted that it does contain 99 entries for DarkSide, starting with August 8th, 2020. And we have heard previously that that's when DarkSide first emerged. And I looked for the first DarkSide entry in the list.

And for anyone who's listening, I created a bit.ly, I mean a GRC shortcut to a PDF of it. I did not want to directly point anybody at this live list from lord knows where. So I carefully created a PDF: grc.sc/darktracer. So grc.sc/ D-A-R-K-T-R-A-C-E-R. That will redirect you to a PDF I am hosting at GRC, a 66-page listing of more than 2,200 attacks. Anyway, I looked at the first one that was allegedly by DarkSide, and it said that Brookfield.com was attacked on August 8th. I did a bit of googling and revealed that, yes indeed, the Toronto Star carried the report dated August 25th with the headline "Canadian real-estate company Brookfield Residential suffers data breach by new ransomware group DarkSide." And for anyone who's interested I have a link to that Toronto Star report.

So anyway, as I said, since I would not feel comfortable pointing our listeners at a live spreadsheet being hosted by an apparently benign but still unknown entity. I printed a snapshot of it as it is today to a PDF, stripped it of all extraneous metadata, and am hosting the PDF at GRC.com. It is fascinating and a little sobering to look at it, grc.sc/darktracer (T-R-A-C-E-R).

And because I don't want to keep anybody from the live data if they want it, I have a link in the show notes with a big red "ORIGINAL SOURCE: LIVE GOOGLE SHEET (WARNING)." So you are able to view it, the original source material, live. And the original snapshot that I saw that led me to this one was older than this one, and this one is current as of today. I think there was an attack on the 17th, yesterday, and a few shown on the 18th. So it appears to be legitimate, and it certainly is fascinating. And I thought that our listeners would find it interesting. So grc.sc/darktracer will take you to today's snapshot, a safe PDF, which was printed from the actual spreadsheet.

And then just to end this discussion of ransomware on a lighter note, I saw a tweet from PeterM, who repeated something that he saw, tweeting from @AltShiftPrtScn, dated 6:17 this morning. Avaddon, which is one of the Ransomware as a Services, and there's lots of listings for them in that PDF, "Avaddon victim who didn't pay asked the attackers to please leak their data in full because they were having trouble restoring some backups from their files. The threat actor clearly didn't understand, as they responded by saying if the victim didn't cooperate they would leak their data."

Leo: Oh, whatever you do, don't leak my data, bad guy. Whatever you do. Holy cow.

Steve: Yeah.

Leo: Oh, my god.

Steve: Okay. So we're at the third - yeah, right, please, we're having problems restoring from backup. Please leak our data. Yeah. There are some files that we need that we can't get otherwise. Wow.

Leo: That's a great one.

Steve: Okay. So we're at the third Tuesday of May. Wait. The third? Oh, yeah, third Tuesday of May. So we're able to look back on last Tuesday's comparatively sedate Patch Tuesday. Whereas we have seen past updates delivering fixes, as we know, for well over 100 flaws, last week was a mere 55 fixes affecting Windows; Exchange Server; Internet Explorer, believe it or not; Office; Hyper-V; Visual Studio; and Skype for Business. However, that said, there was definitely some excitement.

Of those 55, four of those fixed were critical vulnerabilities, 50 were important, and one was moderate. Three of the vulnerabilities are publicly known, although unlike last month, none of them are under active exploitation as of the time of this release, which is good. Unfortunately, it's not clear how long that will be the case. But it probably doesn't matter.

There was one particularly juicy baddie that is worrying the industry a little bit. It was assigned CVE-2021-31166, and it's a potentially wormable remote code execution vulnerability in the HTTP protocol stack of only the most recent releases of IIS, which is Microsoft's web server, for Windows 10. It's wormable because it requires no action on the recipient's part. An unauthorized, unauthenticated remote attacker simply needs to send a specially crafted packet, a query, to any vulnerable Windows 10 server. And they all were vulnerable. All of those that were vulnerable, were vulnerable - what? - before the patch came out, which will run the attacker's code in the kernel. And if that code chose to scan for other publicly accessible, or even internally accessible for that matter, hosts, we'd have a new Internet worm on our hands. Consequently, this one carries a CVSS rating of 9.8 out of 10.

And wouldn't you know it, some security researcher just couldn't help but show off their mad haxor abilities by publishing a working proof of concept which is now up on GitHub. He wrote: "This is a proof of concept for CVE-2021-31166 (HTTP Protocol Stack Remote Code Execution Vulnerability), a use-after-free dereference in http.sys patched by Microsoft in May of 2021. According to this tweet" - and then he cites it - "the vulnerability has been found by @_mxms and @fzzyhd1." Looks like "fuzzy," doesn't it. Yes. Do a fuzz on your hard drive.

Anyway, even so, this probably won't amount to much because non-corporate users, who are more likely to have the latest version of Windows 10, will probably have updated and patched and are also typically isolated behind their NAT routers. And these days few home users are running a public web server, and certainly not on port 80, probably. I don't even know if you can still. And at the other end of the scale, it's unlikely that any corporate Windows Server installations are crazy enough to be running the latest Windows 10 instances of Server. This bug was recently introduced into the code and only affects Windows 10 Server 2004 - poorly numbered, of course - and 20H2. So the two most very recent instances of Windows 10 Server, hopefully no enterprises are running those publicly exposed. If so, be a good idea to fix that because now there's a proof of concept posted about how you can take advantage of it.

There was also another remote code execution flaw in Hyper-V, which also scores the highest severity among all flaws patched this month. It even beats that one. That one was 9.8; this is 9.9. Microsoft's advisory said: "This issue allows a guest VM to force the Hyper-V host's kernel to read from an arbitrary, potentially invalid address. The contents of the address read would not be returned to the guest VM. In most circumstances, this would result in a denial of service of the Hyper-V host" - in other words, a blue screen crashing everything - "due to reading an unmapped address. It is possible to read from a memory-mapped device register corresponding to a hardware device attached to the Hyper-V host which may trigger additional hardware device-specific side effects that

could compromise the Hyper-V host's security." What that really means is we actually do know how this really bad problem could be leveraged to completely compromise Hyper-V security, but we don't want to say that. We just want you to patch it. So anybody who's in any way associated with Hyper-V and needing its protections would be well advised to patch last Tuesday's update.

Let's see. In addition, there was an update that addressed a scripting engine memory corruption flaw in IE, believe it or not. And four more flaws in Microsoft Exchange Server, which continues to dog Microsoft. This makes it the third month in a row Microsoft has continued working to fix that troubled product since the ProxyLogon exploits in March.

Leo: Geez.

Steve: I know, Leo. They just cannot get it right. Well, you know, it's an email server, and they just - it didn't get much attention. And now that it is, they're looking at it going, oh. And you know, this is what we've seen before, too. Remember that when there was that spate of RDP problems, and Microsoft said, oh, maybe we should take a look at RDP. We haven't looked at it for a while. And then they just began spitting out patch after patch after patch as if, you know, they've put the A team on it because suddenly it became important, and those guys are like, who wrote this crap? And they just kept finding fixes for it.

Leo: Yeah, it is, it's like the Eye of Sauron. It moves around, yeah, yeah.

Steve: Exactly.

Leo: Oh, let's pay attention to this now.

Steve: So otherwise the update addresses a large collection of privilege escalation bugs in Windows Container Manager Service, an information disclosure vulnerability in Windows Wireless Networking, and several remote code execution flaws in Microsoft Office, Microsoft SharePoint Server, Skype for Business, Lync, Visual Studio, and Microsoft Media Foundation Core. So in other words, hopefully it's a week downstream, everybody's already updated, and you're like, okay, fine.

Okay. So on to a bit of miscellany. I found a review of the first book of The Frontiers Saga. And it's long, so I'm not going to share it all. But I'll just share the opening because it was fun. And the reason I'm bringing this up at all is that it's so well written. The reviewer is a listener.

So he said: "On a recommendation from Steve Gibson on his Security Now! podcast, I've started reading The Frontiers Saga by self-published author Ryk Brown. This is a review of the first book in the series, called 'Aurora CV-01.'" He says: "The Frontiers Saga is classical science fiction space opera stuff, best summarized as a cross between Ronald D. Moore's 'Battlestar Galactica' and 'Star Trek: The Next Generation.' Sounds a bit run-of-the-mill at first glance, but it raises eyebrows immediately based on the sheer scope of the work." And then he quotes Ryk talking about basically 75 books that he's going to write.

The last paragraph I'll quote. He says: "'Aurora CV-01,' the first book in the franchise, which I've just finished, was originally published 10 years ago. Since then, Brown has

finished two series, meaning 30 books. That's on average three books, of 200 to 300 pages each, a year." He says: "And the guy just keeps on going and going. He's like some sort of anti-George R.R. Martin with his output. That alone impresses me enough to give him a shot. And I must say I have not regretted it."

Okay. That's just the beginning of a much longer review. I made it the shortcut of the week for anyone who hasn't yet been motivated. I would suggest that you read Andy Weir's most recent work, which we know is "Hail Mary." And then, if you're a person who just loves sci-fi, again, I can't recommend it highly enough. The review is at grc.sc/819, this week's episode number.

I just did want to touch on, Leo, because sci-fi is an interest that we share. And I'm a bit bemused, I suppose is the right word, by the whole question of UFOs. I thought it was interesting that "60 Minutes," you know, a serious long-running 60-minute news magazine that airs on CBS on Sunday nights, did a segment on what they refer to as UAPs, Unidentified Aerial Phenomena, and that there's actually an Unidentified Aerial Phenomena Task Force. Wikipedia has an entry describing it. And that there, I mean, that this thing, this entity, this organization, this task force, exists, and it has a budget from Congress and will be submitting a report, I think a month from now, if I remember correctly, about as far as they know what is going on.

I would suggest that, if anyone is interested, because what we saw was some video, it was not brand new video, it's a few years old. But it's real video. On "60 Minutes" they discussed a number of sightings, like quadruply confirmed sightings, two different fighter planes, both people in the cockpit in the front and the back, all saw and recorded on camera and tracked on radar and blah blah blah blah blah. And so, you know, they talk about how, you know, the behavior of these things. And I just wanted to go on record as saying, if you're interested, go find "60 Minutes" from last Sunday. And it's some interesting stuff. I have no explanation for this stuff. Nobody is suggesting that these are extraterrestrial. And frankly, Leo, the more I mature in my understanding of human nature, or maybe entity nature, the more glad I am about the speed of light barrier.

Leo: Yeah. Yeah.

Steve: And the distance we are from anything else. You know, even on this ball of dirt, the oceans kept us apart from each other for a long time, and that was a good thing. As soon as we started being able to sail across the ocean, all hell broke loose.

Leo: Well, look what air travel has brought us, pandemic-wise, you know.

Steve: Yes.

Leo: Yeah. Probably best just to stay home, everybody, please. Even the aliens.

Steve: Yeah, exactly. Just, you know, it's a long-ass trip. Do not - there's nothing here. All we have is bitcoin, and we're not sure about that. So just cool your jets.

Leo: If you're using jets.

Steve: That's right.

Leo: I think it's much more likely there's optical illusions. There's all sorts of things that can cause people to see things. No one's denying that everybody on the plane saw it. So that's not the question. It's just an unidentified thing.

Steve: If you haven't watched this segment, Leo...

Leo: I'll watch it, yeah.

Steve: I really - I would commend you to watch it. It's, I mean, I'm, again, one of the things I've noticed about me is I'm complete - and I found this when I was debugging SpinRite early on, is I'm completely comfortable saying "I don't know." I don't have to have an explanation for stuff.

Leo: Yeah. Yeah, I don't know.

Steve: If there's a bug, I don't know. And that's fine. But that's where you begin to do your research, if you're a researcher. You start with "I don't know," and you start trying to figure things out.

Leo: Yes.

Steve: We had an interesting follow-up two days ago from somebody who posted on April 21st, a listener. He tweeted to me, and he's got a terrific short Twitter, you know, @krv is his Twitter handle. He said originally: "You asked for someone's FLoC ID. Here is mine: 'Your FLoC ID is 5393.'" Then two days ago: "FYI, if you're still interested, my FLoC ID is now 6501." He says: "I'm not sure how often it changes as I haven't been checking it regularly." But yes, presumably weekly. And so I think, you know, it still remains an interesting solution to me.

And two pieces of feedback from our listeners who heard us talk about "Hail Mary" book last week. Zap Anderson said: "Yes, @SGgrc, 'Project Hail Mary' by @andyweirauthor is indeed AWESOME," all caps. He said: "Just binged the Audible book."

Leo: That's 16 hours. That's quite a binge.

Steve: "Just binged the Audible book." And he said: "Narrator and ... other sounds awesome." He said: "It's fudging great," and I don't think he meant fudge. And then Arnold Ochoa, who also has an amazing Twitter handle, @a8a. He said: "@SGgrc If you have the chance, you should give @andyweirauthor's 'Hail Mary' a chance on Audible. No spoilers, but there are things there that can't be in the book. You'll know what I mean once you 'read' it." So anyway, thank you for the feedback, listeners. Everybody I've heard anything from so far has said, oh, wow. And Leo, you should mention that you're going to have Andy on.

Leo: We are. Andy Weir, who I interviewed when "The Martian" came out, I interviewed when "Artemis" came out, so this will be my third time with Andy. I just think he's the greatest. And I would say this book is his best yet. If you liked "The Martian," it's very similar to that. I think you will love "Project Hail Mary." He will be our guest on a special episode of Triangulation. We'll put it out on the Triangulation feed and on the TWiT events feed. This Friday, 3:00 p.m. Pacific, 6:00 p.m. Eastern, that's 22:00 UTC, Friday. Let's see, this is Tuesday, so it would be the 21st of May. And I hope you will listen. And if you're in the TWiT Club, Club TWiT, we will probably fire up the Discord and give some Club TWiT members a chance to ask Andy questions. So I think that'll be fun, too. So please join me.

Steve: Yeah, the trick is that there are some things you really want to ask him having read the book. And so you're thinking maybe about dividing it into a pre-read and then a "danger, spoilers ahead" where, if you haven't read it, you absolutely don't want to finish the podcast until you have. And then you'll be really glad that that second half of the interview is there.

Leo: Exactly. As I listen to it, there are things I'm desperately dying to ask him. But pretty much anything you say about the book is a spoiler. So, I mean, literally, you can't say anything about the book. I'll have to ask him about it. But my guess is we'll do a half hour, 45 minutes with him, saying "no spoilers," and then, okay, if you haven't read the book, pause. Read the book. We'll see you in a few hours

Steve: Or maybe break it into two separate pieces.

Leo: Depending on how much time Andy's willing to give me, that's not a bad idea, as well, yeah. He's great. I love him. His story is fantastic. And he self-published "The Martian," became a huge hit, not only a bestselling novel, but a movie. And I think this new one, man, I can't wait to see the movie.

Steve: And I heard it already was going to be a movie.

Leo: Oh, no doubt that it's optioned. It's just too good, yeah. So you've got to read, well, you're in the middle of something else, I guess. Otherwise you [crosstalk].

Steve: I am. But I will get to a point where the action pauses for me, and I will absolutely jump on it. In fact, I think I already bought it; but I just, you know, it's got itself downloaded, and it's waiting.

Leo: Yeah. You're going to love it, yeah. Frag Attack.

Steve: So as we said at the top, the discoverers of the WiFi KRACK Attack are back. I've been wanting to say that all day. The KRACK Attack, which we of course covered in detail at the time, was a key reinstallation attack that was able to break WPA2 encryption by forcing nonce reuse. The same lead researcher and team have been quite busy behind the scenes. They'll be initially presenting their new set of Frag Attacks. And actually it ought to be capital F, lowercase r, capital A, lowercase g, except that that makes it look a little awkward, because it's both fragmentation and aggregation. So it's obviously

breaking them apart and putting them back together again. And Frag Ag, that doesn't really roll off the tongue.

So, but anyway, Frag Attacks. They're going to be presenting it at the forthcoming USENIX 2021 conference and then later, in much greater detail and depth, during this summer's Black Hat 2021 conference. Which I guess maybe will actually be held in person.

Leo: Ooh.

Steve: I wonder what they're - I haven't heard about that.

Leo: I don't know if we know yet, yeah.

Steve: Yeah. Anyway, these guys, okay. So I'm going to go over these because they're interesting from a theoretical "what could possibly go wrong" standpoint. But this is not the end of WiFi as we know it. This is not a meltdown. This is not, well, actually that's a bad choice of words because Meltdown was not a meltdown. But we're going to be fine. So what they discovered was three fundamental vulnerabilities inherent in the design of the WiFi protocol. Although again, as I said, you've really got to work to make them happen. So these were not implementation errors specific to anyone or more particular devices, but rather mistakes in the design of WiFi itself. And along the way they also discovered a handful of specific WiFi protocol implementation errors where the protocol itself isn't the problem, but the way the code was written to implement it was.

Okay. So here's how they introduced and framed their discoveries. And I tweaked it a little bit just for readability. They said: "We present Frag Attacks, fragmentation and aggregation attacks, which is a collection of new security vulnerabilities that affect WiFi devices. An adversary who is within range of a victim's WiFi network can abuse these vulnerabilities to steal user information or attack devices." Doesn't sound good. They said: "Three of the discovered vulnerabilities are design flaws in the WiFi standard and therefore affect most devices. On top of this, several other vulnerabilities were discovered that are caused by widespread programming mistakes in WiFi products. Experiments indicate that every WiFi product is affected by at least one vulnerability, and that most products are affected by several.

"The discovered vulnerabilities affect all modern security protocols of WiFi, including the latest WPA3 specification. Even the original security protocol of WiFi, WEP" - remember WEP back in the day - "is affected. This means that several of the newly discovered design flaws have been part of WiFi since its release in 1997. Fortunately, the design flaws are difficult to abuse because doing so requires user interaction or is only possible when using uncommon network settings. As a result, in practice the biggest concern are the programming mistakes in WiFi products, since several of them are trivial to exploit.

"The discovery of these vulnerabilities comes as a surprise because the security of WiFi has in fact" - this is them speaking - "has in fact significantly improved over the last years. For instance, previously we discovered the KRACK attacks. The defenses against KRACK were proven secure, and the latest WPA3 security specification has improved. Unfortunately, a feature that could have prevented one of the newly discovered design flaws was not adopted in practice, and the other two design flaws are present in a feature of WiFi that was previously not widely studied." Whoops.

They said: "This shows that it remains important to analyze even the most well-known security protocols. Additionally, it shows that it's essential to regularly test WiFi products for security vulnerabilities, which can, for instance, be done when certifying them." And there's a little jab in the ribs to the Wi-Fi Alliance, you know, also known as the CYA Alliance because they do little except say, oh, it's not our fault.

Anyway, they finish: "To protect users, security updates were prepared during a nine-month-long coordinated disclosure that was supervised by the Wi-Fi Alliance and ICASI. If updates for your device are not yet available, you can mitigate some attacks, but not all, by assuring that websites use HTTPS and by assuring that your devices received all other available updates."

Now, Leo, I was not familiar with the abbreviation "ICASI."

Leo: ICASI.

Steve: Which they're referring to in their opening. So I googled it and looked it up. So it's either the International Culinary Arts and Sciences Institute...

Leo: No, okay, wrong.

Steve: I don't think so. Or Industry Consortium for Advancement of Security on the Internet.

Leo: That sounds right, yeah.

Steve: And that sounds like...

Leo: ICASI.org.

Steve: That's the one.

Leo: Yeah.

Steve: Okay. So they then provide a demonstration showing three examples of an adversary abusing a few of these vulnerabilities. The first uses the aggregation design flaw to intercept sensitive plaintext information, in this instance the target's username and password, if not otherwise encrypted, is available. In other words, they're able to break the WiFi wrapper, the WiFi encryption, getting to the underlying raw data, the so-called, you know, the plaintext within the WiFi packet. But hopefully you're over HTTPS, so you've got TLS tunneling in place, and encryption and authentication anyway, so you're okay. But they show that it's possible to crack the actual encryption offered by WiFi.

Then they demonstrate how an adversary can exploit insecure IoT devices by remotely turning on and off a smart power socket. I'm sure mine is vulnerable, that little cheesy

thing for $5. But it works, even though it's talking to China. And, finally, they demonstrate how the...

Leo: Steve Gibson's lights are on. Steve Gibson's lights are off. Steve Gibson's lights are on. They're off again.

Steve: And we unplugged it because it was annoying. Oh, well. Back to a light switch which we now know you push down when you're in the U.K. to turn things on, rather than up.

Leo: That was a stunning revelation.

Steve: Isn't that, yes.

Leo: Still reeling.

Steve: And finally they demonstrate how the vulnerabilities can be abused as a stepping stone to launch more advanced attacks. And they specifically demonstrate how an adversary can take over a WiFi connected Windows 7 machine inside a local network. So anyway, the various WiFi flaws can be abused in two ways. Given the proper conditions, as I mentioned above, they can be abused to steal sensitive data, breaking the WiFi encryption. And an adversary can also abuse the Wi-Fi flaws to attack devices within a victim's home network.

They felt that the greatest practical risk was likely the ability to abuse the discovered flaws to attack devices in someone's home network. They noted, as I often lament, that many smart home and IoT devices are rarely updated, and that WiFi security is the last line of defense that prevents someone from attacking these devices. Of course, the good news is you can't do that from Russia because you're out of range of WiFi. So thankfully, for any of this stuff to work, you've got to be within radio range of the target's network being attacked. On the other hand, that's possible, if you're a determined attacker, like if you're someone maybe authorized to get access or not. Anyway, unfortunately...

Leo: You mean that black van outside my house, that's not really a TV repairman?

Steve: Yeah, that's got all those weird...

Leo: Weird antennas.

Steve: ...Yagi antennas aimed at your house, yeah.

Leo: I just thought he was a TV repair guy. I didn't know.

Steve: I think they're checking your signal strength, Leo. We're not sure which signal, though. Anyway, so the flaws can be abused to exfiltrate transmitted data. Okay. So

taking a look in more detail at this, we've got, to give our listeners a sense for these things, I mean, I've got it now. Having read through all this, I want to convey that because they're kind of interesting.

So we have plaintext injection vulnerabilities. Several implementation flaws, remember, okay, separate from design flaws, can be abused to easily inject frames into a protected WiFi network. Okay. For example, an adversary can often inject a carefully constructed unencrypted WiFi frame. This can be leveraged into a DNS spoofing attack to trick the client into using a malicious DNS server. And when used against routers, this can also be used to bypass the NAT firewall to allow the adversary to subsequently attack devices on a local WiFi network.

Okay. So how can an adversary construct unencrypted WiFi frames so they're accepted by a vulnerable device? Get a load of this. It turns out that some WiFi devices will simply accept any unencrypted frame that arrives, even when they are connected to a protected WiFi network. In other words, it means that the attacker doesn't have to do anything special. Two of the four home routers that they tested were affected by this vulnerability, and several IoT devices were affected. And some smartphones were affected, as well as were many WiFi dongles on Windows. All of these things, even though you bring up, you have like encryption on the network, and you bring up an encrypted connection, they will incorrectly accept plaintext frames when they are split into several fragments. Turns out the fragment reassembly process sidesteps the check for encryption, and the packets are processed without any encryption as plaintext.

They also found that some devices will accept plaintext aggregated frames that look like handshake messages. So an adversary can exploit this by sending an aggregated frame where the start of the frame resembles a handshake message, but whose second subframe, that is, pieces of frames, individual frames that were aggregated, that second subframe contains the packet that the adversary wants to inject. This, the fact that the front of it looks like a handshake, slips the inbound aggregated frame past the naive WiFi parser's state machine.

Such vulnerable devices first interpret the frame as a handshake. That moves it to a different place. Then the vulnerable devices pass it on. And the subsequent pieces of the aggregated frame are treated as unencrypted and merged right into the conversation. Just, again, weird edge cases, but you could imagine a sufficiently motivated adversary. Somebody really into getting some device on someone's network protected by encryption to misbehave could take advantage of this.

And, finally, several devices process broadcasted fragments as unfragmented frames and will accept broadcast fragments when they are sent unencrypted. So just a mistake in the code of the WiFi stack. An attacker can abuse this to inject packets by encapsulating them in the second fragment of a plaintext broadcast frame, which will be accepted by the router. So, yes, security is difficult.

Those were implementation mistakes. As I noted, we also have a few fundamental design flaws. The first design flaw, that is, as a consequence present in all devices, is the frame aggregation feature. Remember I was just talking about the idea that you'd have an aggregated frame made up of smaller frames. It turns out that frame aggregation is a feature of WiFi. It increases the overall speed and throughput of a network by explicitly allowing the aggregation of multiple small frames into a single larger aggregate. To implement this feature, the header of each frame contains a flag to indicate whether the encrypted transported data contains a single or an aggregated frame.

But unfortunately, this "is aggregated" flag is not authenticated and can be modified by an adversary, leading to a victim being tricked into processing the encrypted transported data in an unintended manner. It can be abused to inject arbitrary network packets by

tricking the victim into connecting to their server and then setting the "is aggregated" flag of specifically selected packets. They said that nearly every device they tested was vulnerable to this attack. They're just, you know, it was a flaw in the design of all of WiFi that does not authenticate the "is aggregated" flag. So you can get up to mischief with it. We've seen these sorts of mistakes throughout the life of this podcast.

It turns out this ability to inject packets can be readily abused to intercept a victim's traffic by making it use, for example, a malicious DNS server. So here's an instance where you would like to have your DNS running over HTTPS to an external anchor, an external resolver, just to prevent anybody from getting up to any hanky-panky with DNS.

They said this design flaw could be fixed by authenticating the "is aggregated" flag in the WiFi standard. And in fact the standard does contain a feature to authenticate the flag. Unfortunately, this defense is not backwards-compatible. That is, if one end of a connection tried to enforce it, and the other end wasn't enforcing it because it requires a slightly different protocol, then you don't have a connection. It'll break, completely break backwards compatibility. So as a consequence of that, in practice, it's never used because only in a deliberately set up instance where somebody exactly knew that both ends of the connection were going to be using this flag, then they could bring this feature on, which nothing else would be compatible with. So in practice it never happens.

There's also something known as the "mixed key" attack. They said this one abuses the deliberate frame fragmentation feature which is also built into WiFi. Frame fragmentation increases the reliability of a connection by deliberately splitting larger frames into smaller fragments. When doing this, every fragment that belongs to the same frame is encrypted using the same key. However, the receivers of these frames are not required to check the keys of these individually fragmented and individually encrypted packets. So, if present, they will dutifully reassemble fragments decrypted using different keys. And this permits an attacker to slip their own packets into the mix.

In practice, this can allow an adversary to exfiltrate selected client data. Unlike the unfixable "is aggregated" flaw above that we just talked about, this one can be fixed in a backwards-compatible manner by only reassembling fragments that were encrypted under the same key, since anything else would always be an attack. But that would require that our WiFi protocol be updated and fixed.

The third and final fundamental design flaw is the - oh, and this is a weirdo, the "fragment cache" attack. Okay. It's still, I mean, it's quite obscure. But still it's there. When a WiFi client disconnects from the network, the device is not required to flush and remove any still non-reassembled fragments. They stay in memory. These researchers provided examples of how this could be used in practice against hotspot-like networks such as something they called "eduroam" and "govroam," and against enterprise networks where users distrust each other.

In those cases, selected data sent by the victim can be exfiltrated. This is achieved by injecting a malicious fragment which will remain in memory in the shared access point's fragment cache. When the victim then connects to that access point and sends a fragmented frame, selected fragments will be combined, reassembled, with the injected fragment which was originally provided by the attacker. So basically you can arrange to leave fragments deliberately in an access point and cause them to be picked up and merged with other users' traffic on its way out of the network.

It turns out, even though it is really obscure, not surprisingly, that one would be trivial to repair in a backwards-compatible manner, simply by requiring that endpoints flush any residual fragments from memory whenever the connection state of any connection changes. I mean, like, yeah, why not? That would be simple to do, at least in theory, but it does require things be updated.

Okay. And we'll wrap this up by coming back to a few remaining implementation vulnerabilities we did not touch on. Some routers, it turns out, will forward handshake frames to another client, even when the sender hasn't finished authenticating. This vulnerability allows an adversary to perform the aggregation attack and inject arbitrary frames without user interaction. Another extremely common implementation flaw they discovered is that receivers do not check whether all fragments belong to the same frame, meaning an adversary can trivially forge frames by mixing the fragments of two different frames. Again, a lot of these are going to be completely resolved as long as you've got HTTPS, that is, your own encryption outside of the encryption provided by WiFi.

And Leo, do you remember, at the beginning of this podcast WiFi wasn't encrypted generally.

Leo: Right.

Steve: Remember most people just, they just like, oh...

Leo: They left it on as a benefit.

Steve: That's right. We want to share it with our neighbors. Oh, passwords, those are pesky things. When our friends come over, they just want to get on the Internet.

Leo: Yeah, no, I always left it on, yeah. I thought it's unneighborly to turn it off.

Steve: Amazing.

Leo: Yeah. We've come a long way. Yeah.

Steve: Things really have changed. Yes, we have. Anyway, they said additionally, against several implementations, it's possible to mix encrypted and plaintext fragments. Unbelievably. And, finally, some devices don't support fragmentation or aggregation, but are still vulnerable to attacks because they process fragmented frames as if they were full frames. Under the right circumstances, this can be abused to inject fragments.

So the researchers pointed out and notified all relevant parties nine months ago of the problems they found so they could and would be fixed, and so that any devices that were being updated would have the benefits of those fixes. So it's very likely that since nine months is lots of time, that things that we use have just been fixed over the course of time. And of course IoT devices are not currently receiving updates to their WiFi stacks, and very few if any can ever be updated. Fortunately, the attacks are all edge cases. They are difficult to implement in practice, and they do all require attackers within radio range of the target.

So Leo, that black van, yeah, that's a problem. But if nothing else, this is one more reason to always place any questionable devices onto their own network. I am seeing that more and more, by the way. I'm seeing other places are recommending network segmentation as the only good solution for dealing with IoT and just stuff you don't want on your internal network of high-value devices.

Leo: Yeah.

Steve: So Frag Attacks, probably fixed.

Leo: Not worth freaking out about.

Steve: Not worth freaking out about.

Leo: But keep an eye on that van on your curb.

Steve: Yeah. I would, when you see the Yagi antenna swinging around to point at you, that's a problem.

Leo: Well, and then there are situations where you have neighbors, like if you're in an apartment complex, you don't know who, you know, if your neighbors decide they want to spy on you or attack you, they're right there, and you can't tell they're on your same network. Same thing in an office building.

Steve: And hacking tools are becoming increasingly available.

Leo: Yeah.

Steve: Once upon a time they were sort of obscure. Now you go on to GitHub.

Leo: Everybody has Wireshark.

Steve: Yeah.

Leo: Yeah. Just download Kali Linux, you're set. You can attack your neighbors. It's great fun. And I think people probably do it just, you know, literally for fun, just because they can.

Steve: Yeah.

Leo: Let's snoop. Let's - you saw the Eufy cameras that people were able to log into.

Steve: Oh, getting the - whose bedroom is that? Oh, lord.

Leo: Eufy, which is Anker's home stuff, has said, well, we've sent out a patch. Now you should unplug your camera, plug it back in, change your credentials, you should be fine.

Steve: Whoopsie.

Leo: Yeah, that's the one thing I really worry about. You know, they get my lights, big deal. But I don't want them to get into the cameras. I really don't. That's why Lisa won't let any cameras in the house.

Steve: I was going to say, Lisa's policy continues to prove to be the correct one.

Leo: If you want to look in my backyard, have at it. Let me know if anything's going on back there. But not my house.

Steve, as always, a fascinating listen, and it's every Tuesday right here on this network. We do Security Now! normally, we were a little delayed today because of the Google announcement, but normally it's about 1:30 Pacific, 4:30 Eastern, 20:30 UTC on a Tuesday afternoon. You can stream the live audio or video if you want to listen live or kind of participate in our chatroom or a Discord server. You can stream that at TWiT.tv/live. And of course as with all our shows now, if you're in Club TWiT, we keep a live audio channel open in the Discord server, giving you a chance to raise your hand and ask questions, that kind of thing.

Steve Gibson has copies of this show that you can download at GRC.com. He's got a couple of unique versions, a 16Kb audio version, which is a little scratchy, but it's the smallest audio version you can get. He's got an even smaller version, that's the human-written transcript, so you can read along as you listen. That's all at GRC.com, along with SpinRite, his bread and butter, world's finest hard drive maintenance and recovery utility. Sorry, mass storage maintenance and recovery utility because it works on everything that spins and doesn't. GRC.com. Lots of free stuff there, too, like ShieldsUP! and all sorts of good stuff.

We have copies of the show, audio and video, at our site, TWiT.tv/sn. There's a YouTube channel dedicated to Security Now!. You'll find a link there, TWiT.tv/sn, to the YouTube channel, plus a bunch of buttons you can press to automatically subscribe in your favorite podcast application. If you do that, you shouldn't have to worry, you're just going to have it on your phone or your device, ready for a listen whenever you're in the mood. However you do it, we don't want you to miss an episode. There's always important information.

Steve, have a wonderful week, and I will see you next week on Security Now!.

Steve: Will do. Bye.