Is Telegram an Encrypted App?

Description: Telegram's founder, owner, and CEO arrested in France. What does that mean? One year after Microsoft began offering free cloud security event logging, how's that going? To no one's surprise, CrowdStrike is losing customers, but how many? Microsoft to meet with CrowdStrike and other vendors to discuss new solutions. Yelp is not happy with Google. Did/does Google put their thumb on the scale? Where do you go to purchase yourself some DDoS? How about sending a Telegram? Chrome exploits are becoming more rare and difficult to find so Google has upped the ante. Believe it or not, Cox Media Group is still promoting their incredibly privacy-invading "Active Listening" capability. How about secretly having foreigners doing all of your work for you? What could possibly go wrong? And Johns Hopkins Cryptographer Matthew Green has become increasingly annoyed by Telegram's claims of being an encrypted messaging platform. So he finally asks the question: Is Telegram an Encrypted App?

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-990.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-990-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here, and of course as always there's lots to talk about. How many customers did CrowdStrike lose, if any; and why Steve says "I'd still be a customer." We'll also talk about Telegram's founder, owner, and CEO arrested in France with what many are saying is an attack on encrypted communications. But Steve's going to do a deep dive on Telegram's, and I'm going to put this in air quotes, "encryption." He says no, it's not really. All that and more coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 990, recorded Tuesday, September 3rd, 2024: Is Telegram an Encrypted App?

It's time for Security Now!, the show where we talk about your security, your privacy, and what's going in the world around us with this cat right here, Mr. Steven "Tiberius" Gibson, the host at GRC.com. Hi, Steve.

Steve Gibson: You, Leo.

Leo: How are you?

Steve: I'm looking at these episode numbers, and it's getting pretty exciting.

Leo: We're inching up. We're inching up.

Steve: Thank goodness I let everyone know a long time ago that it wouldn't be over. Otherwise it would be really sad, you know.

Leo: Yeah, see, aren't you glad now?

Steve: Nine nine zero, nine nine one...

Leo: The countdown?

Steve: Oh, not good.

Leo: It'd be so sad.

Steve: Yeah.

Leo: So now it's a countdown to nothing.

Steve: Yeah. Well, no. Actually, I was telling the truth a long time ago when I said, oh, I'm going to have to rejigger my technology to handle four digits because, you know, back when I wrote it we had one, or then maybe two. But, oh, we're never going to need three, but what the heck, I'll just set it up for three.

Leo: We could do hex.

Steve: No, no, no. We're going to go 999, there'll be a celebration, that's sometime in November, and then we're going to go right on into four digits. And however, I'm really sure we won't need five. That's not going to happen.

Leo: I think you're safe on that.

Steve: I think, yeah.

Leo: Both of us will be just a memory then.

Steve: Okay. So lots of interesting stuff to talk about. As I know you've been talking about, but we haven't talked about it, touched on it here, and it had just happened for last week's podcast, and I didn't know what was going to happen. But Telegram's founder, owner, and CEO has been arrested in France. So we're going to look at what that means. Also, one year after Microsoft began offering free cloud security event logging, how's that going? Also, to no one's surprise, CrowdStrike is losing customers.

But how many? Microsoft, on that topic, is going to meet with CrowdStrike and other vendors to discuss new solutions. We'll talk about that. Also that Yelp is not happy with Google. You know, did or does Google put their thumb on the scale? Yelp thinks so. Where do you go to purchase yourself some DDoS, when that's what you want?

Leo: I'd like a cup of DDoS.

Steve: Yes, how about sending a Telegram? And Chrome exploits are becoming more rare and difficult to find, so Google has upped the ante. And Leo, believe it or not, the Cox Media Group is still promoting their incredibly, I mean, just astonishingly privacy-invading so-called "Active Listening" capability. We're going to revisit that. Also, how about secretly having foreign agents doing all of your work for you? What could possibly go wrong with that? And the reason this podcast is titled "Is Telegram an Encrypted App?" is because that was the title given to the recent posting by our favorite Johns Hopkins cryptographer Matthew Green, who has become increasingly annoyed by Telegram's claims of being an encrypted messaging platform. So he finally asks the question: Is Telegram an Encrypted App? We're going to look at that and answer the question.

Leo: That was a great blog post, actually. I really enjoyed that.

Steve: A little surprising, yes. Yeah, he did a great job.

Leo: Yeah, yeah. And we've been talking, as you mentioned, we've been talking a lot about Pavel Durov's arrest since it happened a week ago.

Steve: Yup.

Leo: And, yeah, it's quite a story. But we will get to that in just a little bit. I am ready with a Picture of the Week.

Steve: Ah. This is a goodie. So I gave this one the caption "When the Universe is suggesting that you should take the stairs, listen."

Leo: Oh, dear.

Steve: Because we have what appears to be a not-that-well-maintained kind of grungy elevator interior, and it's got some instructions over the panel where you push the button for which floor you want to go to. It says: "If elevator does not move, do a small jump. It should move after." Now, again, if you get into an elevator, and you see that signage, the stairs really are looking better.

Leo: Yes. Good thinking, yes.

Steve: So, yes. You know? And I don't know, there's some signage off to the right. There's something about a guy with a mask, it looks like delivery drivers must wear something or other. Oh, and it says "have temperature," blah blah blah, so like have their temperature taken or something. And then down below it says "You M," and then I see "CLOS," and then "ELE." So, like, maybe you must, what, manually close the elevator doors or something?

Leo: Yeah, you must close elevator doors before pressing a button.

Steve: That would be good.

Leo: Unless you want a good view as you...

Steve: Or just jump up and down, and that'll get the elevator going.

Leo: You think that's a joke?

Steve: Oh.

Leo: Do you think it's a joke?

Steve: No, I think it's, like...

Leo: It's stuck a little bit?

Steve: Again, you get in, you see the sign, and you get out. And you just - and so that's why the caption, "When the Universe is suggesting that you should take the stairs, listen."

Leo: Yeah.

Steve: Because, yeah, anyway. Thank you. I will thank endlessly our listeners. We've got some goodies in the queue. So another great Picture of the Week.

Okay. So I gave this week's lead story the title "Telegram Puts End-to-End Privacy in the Crosshairs" because I think that's probably what's ultimately being tested here. At the time, as we said, at the time of last week's podcast, the news was that Pavel Durov, the founder, also owner and CEO of the Telegram instant messaging system, had been detained in France after he flew into and landed in French territory on a private jet. Next, we learned that his status had changed from "detained" to "formally arrested." And then last Wednesday he was released on five million euros bail and is banned from leaving France since he's now facing charges over his responsibility - this is what they're alleging - for the many illegal and in some cases abhorrent things that Telegram's users have been found doing in light of there being no content moderation, mediation, anything within Telegram of any kind. And they're holding Pavel responsible for that.

And of course the reason this is intensely interesting is that, especially to this audience, is that it brings us back to the big and still unanswered question of how the world is ultimately going to deal with end-to-end encrypted messaging, and whether governments are going to allow their citizens to hold truly private electronic conversations without any form of content moderating oversight. And in the present case of Telegram, the charges which French authorities have levied against Pavel include being complicit in running an online platform that allows sharing of CSAM - which as we know is the abbreviation for Child Sexual Abuse Material - also drug trafficking, fraud and money laundering, as well as not cooperating with authorities when required to do so by law.

Now, the French news outlet Le Monde reported that France's police office that tackles violent crimes against children issued a warrant for his arrest. And in a LinkedIn post that was later deleted, that office's Secretary-General said that "At the heart of this case is the lack of moderation and cooperation of the platform," which has nearly one billion users in total - though not all in the EU, much fewer than that - particularly in the fight against, they said, "pedocriminality."

And the EU arm of Politico reported that the specific incident that was cited in the arrest warrant was Telegram's refusal to identify a specific user after being served with a judicial request. Politico wrote, after viewing a document relating to the warrant: "The warrants for Pavel Durov and his brother Nikolai were issued after an undercover investigation into Telegram led by the cybercrime branch of the Paris prosecutor's office, during which a suspect discussed luring underaged girls into sending 'self-produced child pornography,' and then threatened to release it on social media." So, you know, creeps are on Telegram. Okay.

According to the document, the suspect also told the undercover investigators that he had raped a young child. Telegram did not respond to the French authorities' request to identify the suspect. As we've often observed, Telegram is the most combative of all the major social media platforms in their attitude and approach to content moderation and lawful assistance requests. I mean, that's, like, one of the selling points. And, you know, it paints this as a clear benefit in its own FAQ, which explains that its distributed architecture is used to confound court orders. Telegram unabashedly boasts - so here's from their FAQ.

They said: "Telegram uses a distributed infrastructure. Cloud chat data is stored in multiple data centers around the globe that are controlled by different legal entities spread across different jurisdictions. The relevant decryption keys are split into parts and are never kept in the same place as the data they protect. As a result, several court orders from differing jurisdictions are required to force us to give up any data. Thanks to this structure, we can ensure that no single government or block of like-minded countries can intrude on people's privacy and freedom of expression. Telegram can be forced to give up data only if an issue is grave and universal enough to pass the scrutiny of several different legal systems around the world. To this day, we have disclosed," they're saying, "zero bytes of user data to third parties, including governments."

Their terms of service do state that illegal pornographic content is not allowed on its publicly viewable areas. But that doesn't stop people from doing that. Its FAQ says it will only take action on illegal content in these areas, which comprise sticker sets, channels, and bots. However, Telegram assures its users that: "All Telegram chats and group chats are private amongst their participants. We do not process any requests related to them." In other words, within any private groups, which may include up to 200,000 people, anything goes, without any supervision and with an explicit guarantee of technically imposed privacy. So it should be no surprise that many investigations have found child abuse material for sale on Telegram.

However, there are some interesting details here, as an example of an instance where the details matter and where encryption may not mean what its users imagine. This is why today's podcast topic will address the interesting question of whether or not and to what degree Telegram is actually an encrypted app, and exactly what that term means. Our long-time listeners may recall that I have never been impressed with Telegram's encryption from day one because it's a perfect example of what we all know should not be done: Telegram uses a homegrown cipher that a couple of guys just made up.

Leo: His brother. Pavel's brother.

Steve: Right. You know, and it's got some wacky name. I'll get to it later. But it's like the information garbling protocol or something. It's like, what? And literally Matthew says, "WTF?" It's like, he's like, whoa. Anyway, they did this well after the world had learned how to do encryption correctly. So as we've said a long time ago, nobody needs another cipher. Nobody needs another hash. Those building blocks are in place. They've been time and academically and in-the-wild tested. They work. They're solid. So don't just go gluing some together in some weird arrangement and say, you know, we dare you to break it. And of course the fact that they've offered a large cash prize to anyone who could break it does not change the fact that it's not based on any sound, formal design, or tested cryptographic system. So anyway, we're going to take a far closer look at Telegram at the end of today's podcast, since as I said at the top of the show, Johns Hopkins Cryptographer Matthew Green just posted an intriguing piece titled: "Is Telegram really an encrypted messaging app?"

Okay. But be that as it may, Telegram does offer one important feature that makes it unique among all of the private messaging systems. Whereas Telegram, as I noted earlier, can comfortably provide privacy for 200,000 members of a large group, Apple's iMessage groups are limited to 32 participants. Signal groups are limited to 1,000, and WhatsApp's variant of Signal limits group size to 1024. It turns out that implementing true end-to-end encryption across large groups with many participants is not trivial. But what much of the media misses is that, as we'll see, Telegram doesn't actually do that.

So their unique value proposition is to provide large groups with unmoderated communication and certainly some degree of privacy. Telegram describes itself as a "cloud-based messenger" that provides "seamless sync" across devices. But to do that, it needs to have access to the content of those messages. And we know that because Telegram themselves can access the content of conversations. So it certainly could invest in moderation if it chose too. It chooses not to. NBC News reported that child safety groups in the U.S., UK, and Canada all get short shrift from Telegram when they report CSAM on the platform.

And, for example, this is in contrast to an app like Signal, which also espouses and has the technology to actually enforce privacy-first values. Signal's built its app so that its technology implements those values as much as possible while still enforcing privacy. So although Signal collects no content from its users and only minimal metadata about how they use the service, Signal is able to and will respond to law enforcement requests, but only to the extent of providing account creation dates and the date an account last accessed Signal. This means that while Signal is not, in practice, a great deal more helpful than Telegram, at least Signal is not openly combative and can honestly say that it has wholeheartedly cooperated with court orders to the limit of its ability and technology. When Telegram says that, it's not true.

Okay. So what of Pavel Durov? This may just be a shot across the bow. And it might wind up being good for Telegram's business model to see their founder and CEO being detained and tried for his refusal to comply. Since Telegram currently has only 41 million

users in the European Union, this falls short of the 45-million user threshold that would subject it to the EU's Digital Services Act. With Telegram not categorized as a very large online platform, it's not subject to the EU's stricter transparency and content moderation rules. However, the Financial Times recently reported that the EU is now investigating Telegram for misrepresenting the total number of EU users in order to fall below that 45 million user threshold. Yeah, right. I'm shocked. Last February's claim that they only have 41 million users within the EU is going to be carefully examined for its veracity.

Now, the one thing that, like, this gives me the occasion, and I think it's important to observe before we move on, and we'll be coming back to what Matthew Green said in a minute, is that both of today's major mobile platforms, iOS and Android, manage their client apps with an iron grip. They do this to enforce both security and control over these client apps. And we've spent a lot of time through the years talking about all of the ins and outs and mechanisms for this. So, for example, you know, something close to home here, the reason SpinRite boots directly over its user's hardware and brings along its own minimal OS is because it cannot obtain the direct hardware access it requires from within any operating system environment.

But nothing like that exists for our mobile operating systems. None of the various messaging platforms are able to obtain anything approaching direct access to the platform's underlying hardware. So we should always be mindful of the fact that the OS runs the camera, runs the screen, and runs the virtual keyboard; and that access to those resources is granted to the applications that are running. That's why we're able to seamlessly switch among applications without any application being able to prevent that. Apps are powerless clients of their mobile platform OS. So a messaging app such as Signal, WhatsApp, Telegram, or iMessage may be as clever as it wishes with how the content that it communicates is encrypted and decrypted. But everything that is eventually communicated to and from its users passes through the control of the OS, and that OS is always able to "see" everything that's happening in the clear without any form of obfuscation or encryption.

I think we need to hold onto that because it's easy to get focused on the ins and outs and specifics of any given messenger. But our mobile OSes have an iron grip over all of these messaging apps. And what the user sees, the decrypted content coming out of the app and onto the device's UI surface and going in, the OS is the one that has unfettered, unencrypted access to that. So there's a bit of a game of "hot potato" going on here, with no one wanting to take responsibility for the content that's passing through their control before it's encrypted or after it's decrypted. But the truth is that the vendor of the underlying platform - Apple or the supplier of an Android OS - is in the unique position to monitor what's going on before it's turned over to any messaging app, and to similarly inspect what its client apps decrypt before it's presented to the user.

Now, we know, we've talked about this, too, I mean, this is a difficult subject. We know how adamantly the platform vendors want to stay as far away as possible from taking any responsibility for what their users and their client apps do. And I know that we all want to retain the total privacy that we're currently being assured we're receiving. But Pavel Durov's arrest and indictment by French authorities shows us that we should probably regard the privacy we're enjoying today as fleeting, since no government wants to be completely blind to the conduct of its citizenry.

Okay. So to set the stage for some news, recall that five months ago, last April, the U.S. Cyber Safety Review Board released a rather scathing report which squarely placed the blame on Microsoft for the nation state-linked intrusion into Microsoft Exchange Online which led to the theft of about 60,000 U.S. State Department emails that previous summer. The CSRB report stated that the breach "was preventable and should never have occurred."

The report elaborated that a series of operational and strategic decisions by Microsoft pointed to a corporate culture that deprioritized investments in enterprise security and rigorous risk management, despite the central role the company plays in the larger technology ecosystem. The CSRB urged Microsoft to publicly share its plans to make fundamental, security-focused reforms across the company and its suite of products. The board also recommended that all cloud service providers and government partners enact security-focused changes.

Okay. So among the criticism that was heaped upon Microsoft last year was that it was charging, you know, extra money for zero-cost features such as security logging that would have gone a long way, had more of the government entities been using them, to help detect the early states of the various intrusions its users and customers had been experiencing. The tech savvy Senator Ron Wyden said at the time: "Unfortunately, as Microsoft's $15 billion-plus cybersecurity business grows, Microsoft's incentives are not to deliver secure operating systems and cloud software to its customers, but to deliver insecure products and upsell them on cybersecurity add-ons. It should not have taken multiple disastrous hacks of federal systems for Microsoft to make essential security features standard for government customers, but better late than never."

So we're talking about this today now because, one year later, evidence is emerging of the effect, the beneficial effect, of something as simple as free security logging. Last Tuesday, the publication Cybersecurity Dive posted a report titled: "CISA officials credit Microsoft security log expansion for improved threat visibility." They wrote: "Greater access to Microsoft event logs is paying off for U.S. government agencies and critical infrastructure providers, which have gained greater visibility into their network environments, the Cybersecurity and Infrastructure Security Agency said Saturday." You know, CISA.

"Microsoft expanded free access to security logs in 2023 after a state-linked threat actor stole thousands of emails from the State Department after gaining access to Microsoft Exchange Online. Jeff Greene, CISA's executive assistant director for cybersecurity, confirmed via email: 'Yes, Microsoft has expanded access to the logging elements that were used by the State Department to detect the 2023 compromise to a vastly larger set of customers, including all federal agencies and numerous critical infrastructure organizations. These new logs are being used by organizations today to detect threats.' Greene added: 'CISA will continue to work with Microsoft and other companies to ensure that their products are secure by design, and that Microsoft lives up to the commitments it has publicly announced around improving the security of its products following the 2023 compromise.'

"The win for the U.S. government comes as CISA, along with the FBI, National Security Agency, and a group of foreign cybersecurity authorities led by Australia, released a best practices guide for event logging last week. The new guide is part of an effort to combat sophisticated threat activity from state-linked threat groups, such as Volt Typhoon. The group uses living-off-the-land techniques to disguise its threat activities using normal security tools that won't trigger alerts when moved around computer networks.

"Security researchers at ReliaQuest have been tracking a ransomware actor known as Medusa, which is also using living-off-the-land techniques in multiple attacks. Alex Capraro, cyber intelligence analyst at ReliaQuest, said via email: 'By implementing the best practices for event logging and threat detection outlined in this guide, organizations can enhance their ability to identify and mitigate malicious activities, thereby protecting their networks, devices, and data from compromise.'"

So yay, you know, it's unfortunate that Microsoft had to have so many problems and come under so much pressure before it made something that costs it virtually nothing free because it was making money from selling something that it's no longer making

money from. But really, I mean, anyone who's got any experience with IT security understands and has, I'm sure, used logs to find out what's going on. I think the first instance where I saw logging being used to a level that at the time I thought was a little over the top was about 25 years ago, Mark Thompson, my friend whose site is AnalogX.com - Leo and I know Mark, he's been a friend of ours for decades.

Leo: Is he still doing his AnalogX?

Steve: Yeah, he's still busy doing stuff, Leo. You know, Mark made a comment about - I think it was we were talking about something, and he made a comment that he was logging something. And I thought, I mean, it was like logging, like, how long his toothbrush takes to charge or something. I mean, it was, like, what? And but what do know; you know? Turns out that that was useful somehow. And I know that over time I've increased the amount of logging I'm doing. And sure enough, I mean, I guess the point is you don't know what you don't know until you wish you knew.

"And if everything is being logged, then you may have to do some log processing. You know, and I roll logs over monthly and zip them down because the logs tend to compress massively down to things that are much smaller. But, you know, sure enough, I find myself going back and looking through logs to obtain information that I wasn't specifically thinking that I would need. But, you know, if you log it, it's going to be there when you need it. So anyway, the idea, I'm not at all surprised that this is a benefit. And, you know, you could argue 30 years ago that hard drives were expensive, and you didn't want to log everything because, oh, think of all the space it would take. Now, you know, hard drives, data storage is just - it's free. So why not log? And on that note, Leo...

Leo: Log everything. All the time.

Steve: Log everything. Why not take a break to tell us about our sponsor? And then we're going to talk about CrowdStrike and how they're doing with their customers.

Leo: Gladly. Gladly, Steve. All right, Mr. G.

Steve: Okay.

Leo: On we go with the show.

Steve: So far, CrowdStrike reports that it expects to lose around $60 million in net new annual recurring revenue and subscription revenue in the aftermath of its technical outage. Now, I don't have a good sense for what that represents as a percentage of total revenue, but it does not sound like much.

Leo: Yeah.

Steve: Because CrowdStrike is, you know, it's the big player in this EDR, the Endpoint Detection and Response market. So nevertheless, CrowdStrike is endeavoring, as you would expect them to, to retain customers by offering various discounts. Their CEO

George Kurtz denied rumors that the company was losing customers to rivals, but of course that will happen to some degree after the so-called "CrowdStrike outage," which has now been named. Although, you know, as I said, I'm sure I would be staying unless I was in some way otherwise unhappy because the changes they've made since have seemed solid. We know, we talked about last week how George went to the Pwnie Award and accepted like the biggest mistake ever in history award, like in person; whereas other companies like Microsoft have just blown it off. You're not going to get anyone from Microsoft there. So that was impressive. And, I mean...

Leo: A broken bone is always stronger when it heals; right?

Steve: They've really, yeah, I mean, you can have an employee that screws up and, like, over and over and over and refuses to learn a lesson, in which case, okay, fine, we're going to have to let you go. But, you know, it's possible also to learn a lesson. And I'm sure they've, you know, this has really sunk in. George said that he's putting that award in the lobby so that all the employees have to look at it.

Leo: That's a good idea. That's a great idea.

Steve: When they come into work every morning.

Leo: We don't want another one of these; okay?

Steve: Yeah. Yeah. So for what it's worth, both SentinelOne and Palo Alto Networks have claimed that they've been fielding calls from soon-to-be-ex CrowdStrike customers over the past few weeks. Again, I don't doubt that for a moment. But to me, it doesn't seem like that many are leaving. And we actually, I sent the email for this podcast out early today because I started working on it really early yesterday and so got it finished earlier this morning than I normally do, and notified about 8,900 of our listeners of the contents. We have a listener who works at CrowdStrike, and he already sent me some feedback and said, "For what it's worth, we're doing fine." And so, you know, I'm sure they are.

And on that note, interestingly, Microsoft will be meeting privately with a bunch of these guys. Exactly one week from today, on September 10th, Microsoft will host a Windows Endpoint Security Ecosystem Summit, their announcement said, at their Redmond, Washington headquarters. Their announcement said: "Microsoft, CrowdStrike, and other key partners who deliver endpoint security technologies will come together for discussions about improving resiliency and protecting mutual customers' critical infrastructure."

They said: "Our objective is to discuss concrete steps we will all take to improve security and resiliency for our joint customers. The CrowdStrike outage" - this is Microsoft's phraseology - "in July 2024 presents important lessons for us to apply as an ecosystem. Our discussions will focus on improving security and safe deployment practices, designing systems for resiliency and working together as a thriving community of partners" - we're all happy here - "to best serve customers now and in the future."

They finished, saying: "In addition to ecosystem partners, Microsoft will invite government representatives to ensure the highest level of transparency to the community's collaboration to deliver more secure and reliable technology for all. It's

expected that the Windows Endpoint Security Ecosystem Summit will lead to next steps in both short- and long-term actions and initiatives to pursue, with improved security and resilience as our collective goal. We will share further updates on these conversations following the event."

So I would imagine that the government representatives are invited as a means of showing that something is being done to keep anything like this from ever happening again. And in other reporting about this I saw that Microsoft plans, not surprisingly, to discuss new ways of building these EDR products so that they can still get their job done while relying more on safer user-mode code and less on proprietary kernel drivers.

Leo: And that's the key, isn't it. Keep them out of ring zero.

Steve: Yeah.

Leo: Give them an API.

Steve: Yeah. And it's really, well, okay, so it's difficult to do. That is, essentially Microsoft would have to provide hooks all over the place which the various EDR vendors now use. That is, you know, they install a driver. And when the system's booting up, they go and hook a whole bunch of Microsoft's APIs themselves. And by "hook" I mean essentially the idea is that they revector the API service which the OS publishes so that any client running on Windows actually calls into this driver, the proprietary third-party driver, which examines the call, decides what it thinks about it, and then, if it looks okay, forwards it to Windows, the Windows kernel, where it would have normally gone directly to.

So basically it's a comprehensive filter, like, wrapping around the Windows OS. So, you know, Microsoft doesn't want to offer that. I mean, and this is why it's been so limited so far. There are some things, yes, that you can do. You know, AV vendors have some hooks they can use. But nothing like the degree of low-level access that is really necessary to monitor the behavior of things that are trying to use Windows.

So it's going to, I mean, it's an interesting dance. And of course Microsoft is marketing the crap out of their own solution, you know, Windows Defender for Enterprise and everything, because it's like, well, if you just used ours, you wouldn't have had a problem. It's like, right. Nor would we have had the functionality. You know we heard from many users who are using CrowdStrike who said this thing saved our bacon a number of times. So, yeah, we weren't happy that we all had to get up at 1:00 a.m. in the morning and work all day and lost a day of productivity. But, you know, we're sticking with them.

Anyway, it is certainly the case, and we expected, right, that Microsoft would be holding a meeting with the vendors and say, okay, what do we do about this? And of course Microsoft had response and responsibility, too. Many people were saying, why didn't Windows, like, safe boot fix this? Why wasn't it possible to identify the source of the trouble and then say, okay, well, we're going to bring you back up, but you're not going to have your EDR solution enabled until you roll it back somehow. So Microsoft's resilience, you know, the core Windows resilience could have been much higher than it actually turned out to be. So, yeah, lots of things for everybody to fix.

I just wanted to note in passing that Yelp has filed an antitrust lawsuit against Google. It seems, Leo, that Google has reached the size that Microsoft once did back in those days,

and their behavior is being viewed as a little aggressive by an increasing number of entities. In this case, Yelp is alleging that Google has a monopoly over the search market, no surprise there, which it is abusing to promote its own review business. Which of course Yelp is a famous...

Leo: [Crosstalk] Yelp, yeah.

Steve: Yeah, famous reviewer.

Leo: Yelp's been, by the way, whining about this for decades. They went to the EU. That's one of the reasons the EU investigated Google in the first place.

Steve: Right, right.

Leo: So nothing new, and it's interesting they're taking a direct approach now.

Steve: Yes. And it's certainly true that, as we know, controlling search is an incredibly powerful place to be. You know, we view the Internet through what our chosen search engine reveals to us. And I've spoken of her before, my wonderful luddite realtor friend thought that Google WAS the Internet. She, you know, she didn't understand, like when she went to the Google, that she wasn't, like, that it wasn't the Internet.

Leo: It's the Internet.

Steve: Yes, like that's, you know - so, yeah.

Leo: She was actually more insightful than we might realize.

Steve: Yeah. I cried, "Oh, no, Judy, that's not the way - what?" "Just go away, Steve. I know what I'm doing."

Leo: How do I find it if it's not on Google?

Steve: That's right, doesn't exist. Good luck. So anyway, of course there's a reason why SEO, you know, Search Engine Optimization is a booming business, that it matters if you're on the first page of Google's results or the second or where.

Okay. So everyone seems to be piling on Telegram this week. And it's, you know, not as if they probably don't deserve more attention. And in today's Internet threat landscape, that's what's going to happen on any large unmoderated social network platform, which everyone assumes is somehow secure. In this instance, the security firm Falconfeeds has taken a deep look into the flourishing business of DDoS for hire, or more specifically, DDoSaaS as it's formally called: DDoS-as-a-Service. So add the SaaS on the end, DDoSaaS.

In a posting last Thursday titled "DDoS-as-a-Service: The Dominating Phenomenon on Telegram," Jacob Abraham wrote. He said: "In today's digital landscape, Distributed Denial of Service attacks have become one of the most powerful tools in a cybercriminal's arsenal. These attacks, often facilitated by DDoS-as-a-Service platforms, DDoS-for-Hire services, and botnet-for-hire networks, can disrupt online services, extort businesses, and even advance political agendas. At Falconfeeds.io, our latest research reveals a staggering 3,529 DDoS incidents occurred in Europe during just the first half of 2024, making up 60% of the total cyberattacks we analyzed.

"The rise of DDoS-as-a-Service on platforms like Telegram is a significant contributor to this alarming trend. Telegram has emerged as a hotbed for cybercriminals looking to offer DDoS-as-a-Service. On various Telegram channels and groups, vendors openly advertise a range of DDoS attack services at different price points, making it alarmingly easy for even those with minimal technical expertise to hire a DDoS attack. Telegram's encryption and anonymity features create an ideal environment for these illegal activities to flourish unchecked.

"Our research," they wrote, "has identified over 140 Telegram channels and groups actively offering these services, with 80% of them being currently active and trading these services primarily through cryptocurrencies. This trend underscores the growing accessibility and anonymity of DDoS attacks, posing a significant threat to businesses and individuals alike. So-called 'Basic Attacks' are available for as little as $10 per month. And the power and cost scales upward with more 'Sophisticated Attacks' being prolonged, with high-intensity costing as much as thousands of dollars. Price lists are often displayed on Telegram channels, with discounts available for repeat customers or bulk orders." Oh, my god. "This availability and accessibility has turned DDoS into a commodity, available to anyone willing to pay." And again, where are these services to be found? On Telegram.

Leo: Okay. But wait, Steve.

Steve: You no longer even need the dark web.

Leo: Read that whole news story again, replacing Telegram with the Internet and channels with web pages. It's the same story. So I don't understand what the point is. Yeah. You can also get all of that stuff on the Internet. Getting rid of Telegram won't solve that problem.

Steve: Well, I'm not aware of any website that you just go to on the Internet.

Leo: Oh, we've shown them.

Steve: Well, that's the dark web.

Leo: Oh, the dark web.

Steve: Which is very, very difficult to get to. You have to have Tor. You've got to have Onion addresses. I mean...

Leo: So it's making this so easy that that's the problem. Okay.

Steve: Yes. And as we know, ease of access really changes the whole threat landscape.

Leo: Yeah. We'd like to keep attacks away from the unwashed masses. We only want people who know what they're doing to...

Steve: $10, Leo. The bar of entry is really low.

Leo: It's pretty easy, yeah.

Steve: Yeah. Okay. So last Wednesday Google announced that it would be increasing, in some cases by as much as a factor of five, the reward bounties it would be offering for the responsible disclosure, discovery and then disclosure, you know, reporting to them privately of Chrome exploits due to the increased difficulty, which is good news for everyone, of exploiting Chrome. So that's all good news for the world's number one web browser.

Google said, they wrote: "Time flies. Believe it or not, Chrome Browser turns 16 this year." Which, Leo, means you and I have been doing this podcast...

Leo: We're really old.

Steve: ...longer than Chrome has been around. We were three years into this before Chrome happened.

Leo: I should go back and find that episode where you do the story. "And now Google has announced it's going to release its own browser." That would be interesting.

Steve: Yeah. I mean, remember, we were talking about IE6 back at the beginning.

Leo: True. That's a good point, yeah.

Steve: You know, and like Firefox 4 or something.

Leo: We're almost as old as Google itself, to be honest. We've been around a while.

Steve: I do remember when a friend of mine said, hey - because we were all using AltaVista.

Leo: Right.

Steve: That was the best search engine that there was then.

Leo: Right, right.

Steve: And he said, "Hey, some Stanford guys came up with something. Check this out, it's called - it's got a strange name. It's Google." It's like, what?

Leo: I remember when Dvorak would use that as a litmus test to see if you were really a geek. He'd say, "What search engine do you use?" And if you said Excite or AltaVista, he's go, huh.

Steve: Or Yahoo or something.

Leo: Or Yahoo. If you said Google, he'd go, hmm. Doesn't work anymore.

Steve: No.

Leo: No.

Steve: No. My realtor is using Google, so...

Leo: Yes, exactly. It's the Internet.

Steve: Right. Okay. So 16 years old, and their VRP, which is their Vulnerability Rewards Program, to their credit is turning 14. So it only took them two years, Google was two years old when they decided, you know, we should start rewarding people for finding vulnerabilities in Chrome. So that's good.

Google posted: "As Chrome has matured over these years, finding the most impactful and exploitable bugs has become more challenging. At the same time, new features are frequently introduced into Chrome that may result in new issues which we also want to encourage being reported. Therefore, it is time to evolve the Chrome VRP rewards and amounts to provide an improved structure and clearer expectations for security researchers reporting bugs to us and to incentivize high-quality reporting and deeper research for Chrome vulnerabilities, exploring them to their full impact and exploitability potential.

"In this blog post, we'll explain how we've moved away from a single table of reward amounts for non-mitigated bugs, and separated out memory corruption issues from other classes of vulnerabilities. This will allow us to better incentivize more impactful research in each area, and also reward for higher quality and more impactful reporting."

Now, I should mention that reading between the lines what they're sort of saying is we're willing to pay if you're willing to do more work after you find a problem. In other words, a lot of people have been saying, hey, look, I made Chrome crash. Pay out. And now Google is saying, well, okay. If you just make it crash, this is how much you get. But if you're willing to, like, go deeper and do more of our work for us post-crash, then we're

willing to make it worth your time. And that makes sense to me. I mean, that's good because wait till you hear what you can earn if you go all the way here.

So they wrote: "We've remodeled our reward structure for memory corruption vulnerabilities into the following categories." They've got four: "High-quality report with demonstration of remote code execution." They said: "Report clearly demonstrates remote code execution, such as through a functional exploit." And that's the big money. Or "High-quality report demonstrating controlled write, where a report clearly demonstrates attacker controlled writing of arbitrary locations in memory." Third: "High-quality report of memory corruption. Report of demonstrated memory corruption in Chrome that consists of all the characteristics of a high-quality report."

And finally: "Baseline" is their minimum. They said: "A report consisting of a stack trace and proof of concept displaying evidence that memory corruption is triggerable and reachable in Chrome." So, right, different levels, different bar settings that they're asking you to jump over.

And they said: "While the reward amounts for baseline reports of memory corruption will remain consistent, we have increased reward amounts in the other categories," meaning where you're willing to go do more work and give us more, "with the goal of incentivizing deeper research into the full consequences of a given issue. The highest potential reward amount for a single issue is now $250,000."

Leo: Oh, wow.

Steve: A quarter million dollars.

Leo: That's enough to live on for a few months.

Steve: Yes, it is, for "a demonstrated remote code execution in a non-sandboxed process. If the RCE in a non-sandboxed process can be achieved without a renderer compromise, it is eligible for an even higher reward, to include the renderer RCE reward." So you can get them both.

So I've got a link in the show notes. I'm not going to go into any finer detail here. But anyone who's interested in more detail can follow the link. It's to Google's "bug hunters" posting. And I think it's a good move, and good news that since Chrome is becoming more difficult to exploit, the payouts are increasing commensurately. This may also be the first time, and I really give them credit for this, Leo, the first time I've ever anywhere seen a software publisher actually say, they wrote this: "At the same time, new features are frequently introduced into Chrome that may result in new issues which we also want to encourage being reported."

Anyway, anyone who's been following this podcast for more than a few months will think, "Yeah, of course." You know, because we talk about this all the time, like Microsoft won't leave Windows alone, so they're never getting bugs fixed. They're introducing as many every month as they're fixing. So it's just rolling forward.

Leo: Yeah. Yeah. But for them to admit it it's a pretty big deal.

Steve: Yes. Who's actually ever heard any publisher say that? So props to Google for that, yeah. Okay. Yikes. Believe it or not, Leo, when I encountered this next bit of news I thought I was experiencing dj vu. The summary was titled "CMG's Active Listening," and it read: "After media companies and device vendors spent a decade telling customers that microphones baked into their devices are not secretly recording audio, a leaked pitch deck from the Cox Media Group (CMG) is advertising a new service that can show ads to users based on what they've said near microphones. Google kicked CMG from its advertising platform after 404 Media acquired the slide deck and then asked Google to comment."

Okay, now, when I read that it was ringing some bells. I went to GRC's Security Now! page and entered "Cox Media Group" into the search bar in the upper right of all of GRC's pages. The first link and summary that appeared was from our podcast #953. That was the last podcast of last year, dated December 21st of 2023; and that podcast was titled "Active Listening." After the news of what CMG was reportedly doing and bragging about on their own web page, which had the URL ending in "active-listening-an-overview," they took the page down, but not before the Internet Archive's spiders found and archived the page. And that was GRC's shortcut of the week, which is still pointing to the page in question. So grc.sc/953, and it's still every bit as unnerving as it was nine months ago.

The page starts out saying: "Imagine a world where you can read minds. One where you know the second someone in your area is concerned about mold in their closet, where you have access to a list of leads who are unhappy with their current contractor, or know who's struggling to pick the perfect fine dining restaurant to propose to their discerning future fianc. This is a world where no pre-purchase murmurs go unanalyzed, and the whispers of consumers become a tool for you to target, retarget, and conquer your local market. It's not a far-off fantasy, it's Active Listening technology, and it enables you to unlock unmatched advertising efficiency today so you can boast a bigger bottom line tomorrow. Do we need a bigger vehicle? I feel like my lawyer is screwing me. It's time for us to get serious about buying a house. No matter what they're saying, now you can know and act."

And lower down under the "how we do it" they say: "Whether you're a scrappy startup or a Fortune 500, Active Listening makes the unreachable in reach. CMG can customize your campaign to listen for any keywords and targets relevant to your business. Here's how we do it: We flesh out comprehensive buyer personas by uploading past client data into the platform. We identify top-performing keywords relative to the type of customer you're looking for. We set up tracking via pixels placed on your site so we can track your ROI in real-time. AI lets us know when and what to tune into. Our technology detects relevant conversations via smartphones, smart TVs, and other devices. As qualified consumers are detected, a 360 analysis via AI on past behaviors of each potential customer occurs.

"With the audience information gathered, an encrypted evergreen audience list is created. We use the list to target your advertising via many different platforms and tactics, including: Streaming TV, OTT, Streaming Audio, Display Ads, Paid Social Media, YouTube, Google/Bing Search (pay per click). Our technology provides a process that makes it possible to know exactly when someone is in the market for your services in real time, giving you a significant advantage over your competitors. Territories are available in 10- or 20-mile radiuses, but customizations can be made for regional, state, and national coverage."

And then, in their own FAQ, incredibly, they actually ask and answer: "Q: Is Active Listening Legal? A: We know what you're thinking. Is this even legal? The short answer is yes. It is legal for phones and devices to listen to you. And here they actually wrote the following: When a new app download or update prompts consumers with a multi-page terms of use agreement, somewhere in the fine print Active Listening is often included.

Unbelievable. Q: How Does Active Listening Technology work? A: Our technology is on the cutting edge of voice data processing. We can identify buyers based on casual conversations in real time. It may seem like black magic, but it's not. It's AI. The growing ability to access microphone data on devices like smartphones and tablets enables our technology partner to aggregate and analyze voice data during pre-purchase conversations."

So what just happened to bring this back on our radar from nine months ago is that 404 Media, that same group that had previously reported on CMG's web page, which was quickly taken down, obtained the marketing pitch deck that is still, nine months later, being sent by CMG to prospective companies. 404 Media forwarded the deck to Google, who then reportedly kicked CMG off its Partner Program in response. That of course was the right thing for Google to do. But how is it that a massive media group such as CMG is able to, with a straight face, say that consumers are permitting this, making it legal for them, because "somewhere in the fine print" this permission is being given. Unbelievable, Leo.

Leo: Yeah, I feel like, you know, when this story first broke almost a year ago...

Steve: Yeah.

Leo: ...and we talked about it - oops. I don't know what that's doing there. Turn that off. That's our Discord, doing their thing. We kind of thought, well, this is probably an overstatement on the part of Cox Media Group. You know, these guys are salesmen and saying, well, we know what people are talking about probably. I mean, do you think that Amazon is sending the contents of Echo texts to CMG? I don't think so. Or Apple?

Steve: Maybe it's, well, now, we know that Amazon responds to keywords.

Leo: Yeah.

Steve: I mean, at least the enabled keyword. Maybe it's responding to a broader range of specific phrases. I don't, you know, I don't know.

Leo: I don't know, either. But I think it's completely possible to say that these guys are just salespeople overselling what they know because I can't see evidence that they actually, I mean, yeah, they probably can get stuff from Smart TVs. I doubt there's much Samsung won't sell. But I can't imagine that Amazon or Apple or Google [crosstalk].

Steve: How is Apple - and no, there's just no, I mean, maybe Android devices with some app that has like been installed and asked for permission to access your microphone?

Leo: Right. But you know when the microphone's accessed because a light lights up.

Steve: Well, yeah.

Leo: I mean, we all know we're carrying microphones around, but they're absolutely, it's kind of an unwritten law that you don't record everything and then send it to marketers. If they get caught doing that, you know that those companies are going to be history.

Steve: Well, and they're bragging about doing it. So, like, how - I don't know, Leo.

Leo: I honestly think this is Cox Media Group overhyping their capabilities in order to make sales. That's what I think. Because I don't...

Steve: And maybe they're not vulnerable to being held accountable because they're not actually doing it.

Leo: That's exactly my point.

Steve: So if someone says, like, hey, what is this? It's like, oh, well, we're not really doing that, we're just telling people we are.

Leo: Well, and maybe there are, I mean, there are a few devices that they are doing that with. But they're not doing it with the phone in your pocket. They're not doing it with your voice assistant, I'm pretty sure. I mean, if they are, that's a huge scandal. But I think it's much more likely that Cox Media Group's lying, to be honest with you. Not lying. Overstating their capabilities, how about that?

Steve: Yes. Embellishing.

Leo: Embellishing. I mean, what salesperson ever embellishes?

Steve: Yeah. Who's ever heard of that?

Leo: Nobody I know. Would you like me to take a little break here, sir?

Steve: Yes, sir. That'd be good. I'm going to embellish my coffee.

Leo: All right, Steve. You're back. You're on.

Steve: Okay. So last week's serious propeller cap pure computer science nerd fest episode was every bit as much of a hit as I hoped it might be. You know, it's fun thinking about new things, especially for this audience. But I wanted to take a moment to acknowledge some of the feedback I received from a number of our more technical listeners who correctly observed that the three layers of Bloom filtering I described last week could not always be guaranteed to be sufficient. Those observations were correct. My goal was to clearly establish the concepts involved; to talk about Bloom filter

applications where the filter's inherent tendency to produce false positives would and would not represent any actual trouble; and then, in cases where no false positives could be tolerated, to introduce the idea of successive layers of Bloom filters, where the next successive layer of the cascade would capture and be trained on the set of false positives which had been generated by the previous layer.

So those who noted that the third layer might also produce some false positives were 100% correct. And a fully realized implementation of this system actually takes the form of a variable depth cascade where successively smaller layers continue to be added and trained until no misbehavior is observed when the entire corpus of unexpired certificates is fed down through the entire cascade. Eventually, there will be nothing to train the next layer on, since not a single false positive will have managed to make its way all the way down through the cascade. And I guess, you know, in retrospect, I could have explained that last week. But as it was, I felt like it was already a lot for our listeners to take in.

And also for the record, I used one megabit as the number of bits in the first Bloom filter level, which would be addressed by 20 bits taken from any candidate certificate's hash, purely for the sake of illustration since that made it much easier to describe and visualize. The actual size of the first filter and of each successive filter, as well as the number of Bloom layer bits that will be set by the addition of each certificate, are all well understood and are determined by a bunch of very fancy math. But, you know, that was technically irrelevant to our understanding of the overall concept of probabilistic Bloom filtering, and getting that across was the goal of last week's. So anyway, definitely big props to our listeners who said, "Uh, Steve, you do realize that three layers might not always do the job; right?"

And, you know, speaking of listeners and their feedback, I got an interesting piece of feedback. We were talking a couple weeks ago about the security company who discovered that they had inadvertently hired an actively hostile employee based in North Korea who'd gone to extreme measures to spoof their identity and set up a fake domestic operating location. What happened to one of our listeners is a little different, but I think it's just worth sharing it.

He wrote: "Hi, Steve. I was interested in the story from SN-985 about North Korean hackers posing as U.S. workers and getting hired by American tech companies. I'm currently between jobs, and I got an email from someone claiming to be from Malaysia who found my profile on a job board. This person is proposing a" - and he has in air quotes - "a 'collaboration' wherein I get hired for a remote American tech job, then he impersonates me and does all the work. I send 85% of the paycheck to him, pocketing the other 15% for myself." He said, "I don't think anyone's ever approached me to ask for my participation in something so blatantly illegal before. Though if I'm being honest I was momentarily tempted, since it would be easy money for me and he'd still be making more this way than he could working in his own country. Sounds like a win-win, apart from the whole fraud thing and serious criminal and reputational liability to me."

He said: "Anyway, I never responded to the messages, so I can only speculate. But I wonder if this is actually how the situation with KnowBe4 happened. I have no reason to believe the sender of the email used his real name, or that he's based in Malaysia. It might be more plausible that this message is part of the sort of large campaign that uses an 'IT mule laptop farm' as described in the story. His Gmail address is generic and formulaic enough that I suspect there are many other identities being controlled by the same party. The message itself is so carefully wordsmithed that it doesn't strike me as a personal note from a fellow dev. I also received a follow-up message a week later, which felt more automated than not."

He said: "Regardless, I thought you might be interested to see it since the public reads about the aftermath of these stories, but their onset usually happens behind closed

doors. Forwarding the full message here in case you'd like to read it on-air. Thanks, signed Parker."

Okay. So interesting and intriguing, indeed. Here's the solicitation email that Parker received. The subject was "Open to a collaboration?" And it says: "Hi, Parker. I hope you're doing well and don't mind me reaching out. I'm Lucas, a full-stack developer from Malaysia. I found your profile on..." - and this was on usebraintrust.com/talent. He said: "...and wanted to propose a collaboration. I don't currently have any projects that need your help, but our collaboration could be either technical or non-technical.

"For the non-technical aspect, I'd like your help with entrepreneurial factors for my development work. If we end up getting jobs together and working on them, it would be a technical collaboration. To keep it short, I'm looking to get well-paid jobs with companies or clients in the U.S. While this is feasible from Malaysia, they tend to prefer hiring developers from similar time zones. Unfortunately, I'm in GMT+8, while the United States is in PT to ET. Especially for full-time jobs at companies, they typically don't hire developers outside of the U.S. So I believe the best way to get U.S. jobs is to 'impersonate' someone who resides in the U.S. It might sound risky, but it won't be risky as long as we keep this 100% confidential. Besides, I don't mean that I want your identity information."

Leo: No.

Steve: He says: "Have you heard of Upwork.com or Toptal? They're the largest freelancing job markets in the world, where most individual clients in the U.S. look for developers for their projects. There's no easy way to get well-paid jobs, and Upwork or Toptal has a lot of competitive freelancers. However, I'm very confident that I can get great jobs to make decent money.

"Here's how it would work: First, you open an Upwork or Toptal account and log into it on your secondary laptop. I connect to your secondary laptop via AnyDesk app, and I search for jobs. You receive money into your bank account once I finish jobs with clients. You take your commission and send me the remaining. This would be a non-technical collaboration, and I would suggest a split of 15-20% for you and 80-85 for me. For full-time jobs at U.S. companies, which obviously makes us way more money than freelancing jobs, I would apply for jobs on LinkedIn, and you would crack the interviews. However, I'd say this is the advanced step of the collaboration, which should be based on a strong foundation of trust between us.

"Here's how that would work: I apply for company jobs on LinkedIn using your LinkedIn account and get you scheduled with interviews. You crack the interviews and get job offers. I perform day-to-day work on those jobs while you attend the scrum meetings." He says: "(I can join the meetings if team members usually turn off their cameras.)"

Leo: If you've ever done scrum, that's more work than doing the coding.

Steve: Exactly.

Leo: I've got to say I would want more money for that.

Steve: Yeah, I had the same thought, Leo. And finally he says: "You get paid into your bank account bi-weekly or monthly, and you send me my portion after deducting your commission. This would be a mixture of technical and non-technical collaboration, and I would suggest a split of 20-25% for you, 75-80 for me. Please reply to this email if you want to schedule a call to discuss this further or if you have any other opinion for the collaboration. Best, Lucas."

Leo: It feels like it could be real. I mean, I'm sure there is a group of people in other countries like Malaysia who can't get work.

Steve: I imagine it. But I'll tell you, Leo, my own credibility filter snapped on when I read a sentence like: "For full-time jobs at U.S. companies, which obviously makes us way more money than freelancing jobs, I would apply for jobs on LinkedIn, and you would crack the interviews." That sentence, and the rest of the note for that matter, does not strike me as having been written by a non-native English speaker. You know, maybe with AI generated, okay. But in any case, Parker's sense of right and wrong kept him from responding, since this problem of North Korean infiltrators worming their way into Western jobs is clearly very real. With a solicitation as slick and polished, it occurred to me that this might have been some sort of sting operation designed to catch Westerners who would be willing to expose their employers to potential hostile exploitation.

Leo: Right. Actually, in Malaysia many of them speak English, and they speak a British English. So "crack" actually might have been exactly how he would have said it.

Steve: Yeah.

Leo: But I don't - but, see, I don't - yeah. I mean, I wouldn't, if I were Parker, I would not respond, of course.

Steve: Right. Well, and this whole, you know, set up a secondary laptop and then he'll log into the laptop, which means he'll have a domestic IP address...

Leo: Yeah, not good.

Steve: ...and is looping through the laptop from wherever.

Leo: Yeah, yeah. The one thing I would have liked him to do is take the call and just see who's on the other side. Right?

Steve: Like how it goes, sort of explore it further.

Leo: Yeah. But if it were me, I would not...

Steve: Well, no, no, no.

Leo: Shine it on.

Steve: I mean, it just feels - it feels sketchy, you know, to say the least.

Leo: Wow. What an interesting email.

Steve: Okay. So we're going to talk about what Matthew Green, his take on Telegram. Maybe we ought to go a ways before we take our last break.

Leo: Sure.

Steve: Or do you want to...

Leo: Yeah, yeah, it's up to you.

Steve: So we'll get sort of halfway in, and then we'll take our last break.

Leo: Okay.

Steve: Okay. So Matthew wrote: "This blog is reserved for more serious things." Right? And like he's normally talking about the details of subtle problems found in post-quantum hashing algorithms and things. I mean, you know, Matthew isn't bothering to talk about abuse of commercial messaging.

Leo: He's kind of the king of cryptographers from Johns Hopkins. I mean, this guy is very, very - he's the guy, if he says it, I believe it, I guess is the bottom line.

Steve: He knows what he's talking about, yes.

Leo: He knows what he's talking about.

Steve: So he says: "This blog is reserved for more serious things, and ordinarily I wouldn't spend time on questions like the above." Because his blog is titled "Is Telegram an Encrypted App." He says: "But much as I'd like to spend my time writing about exciting topics, sometimes the world requires a bit of what Brad Delong calls 'Intellectual Garbage Pickup,' namely correcting wrong, or mostly wrong, ideas that spread unchecked across the Internet.

"This post is inspired by the recent and concerning news that Telegram's CEO Pavel Durov has been arrested by French authorities for its failure to sufficiently moderate content. While I don't know the details, the use of criminal charges to coerce social media companies is a pretty worrying escalation, and I hope there's more to the story. But this arrest is not what I want to talk about today. What I do want to talk about is one

specific detail of the reporting. Specifically, the fact that nearly every news report about the arrest refers to Telegram as an 'encrypted messaging app.'

"This phrase," Matthew writes, "drives me nuts because in a very limited technical sense it's not wrong. Yet in every sense that matters, it fundamentally misrepresents what Telegram is and how it works in practice. And this misrepresentation is bad for both journalists and particularly for Telegram's users, many of whom could be badly hurt as a result.

"So does Telegram have encryption or doesn't it? Many systems use encryption," he writes, "in some way or another. However, when we talk about encryption in the context of modern private messaging services, the word typically has a very specific meaning. It refers to the use of default end-to-end encryption to protect users' message content. When used in an industry-standard way, this feature ensures that every message will be encrypted using encryption keys that are only known to the communicating parties, and not to the service provider.

"From your perspective as a user, an 'encrypted messenger' ensures that each time you start a conversation, your messages will only be readable by the folks you intend to speak with. If the operator of a messaging service tries to review the content of your messages, all they'll see is useless encrypted junk. That same guarantee holds for anyone who might hack into the provider's servers, and also, for better or for worse, to law enforcement agencies that serve providers with a subpoena. Telegram clearly fails to meet this stronger definition for a simple reason: it does not end-to-end encrypt conversations by default.

"If you want to use end-to-end encryption in Telegram, you must manually activate an optional end-to-end encryption feature called 'Secret Chats' for every single private conversation you want to have. The feature is explicitly not turned on for the vast majority of conversations, and is only available for one-on-one conversations, and never for group chats with more than two people in them. As a kind of a weird bonus," he says, "activating end-to-end encryption in Telegram is oddly difficult for non-expert users to actually do.

"For one thing, the button that activates Telegram's encryption feature is not visible from the main conversation pane, or from the home screen. To find it in the iOS app," he says, "I had to click at least four times once to access the user's profile, once to make a hidden menu pop up showing me the options, and a final time to 'confirm' that I wanted to use encryption. And even after this I was not able to actually have an encrypted conversation, since Secret Chats only works if your conversation partner happens to be online when you do this. Overall," he writes, "this is quite different from the experience of starting a new encrypted chat in an industry-standard modern messaging application, which simply requires you to open a new chat window."

Okay, now, I need to interrupt for a moment to clarify and explain something that's probably not clear. There's a world of difference between a messaging app providing true end-to-end encryption, and merely having encrypted communications. Matthew doesn't bother to draw attention to this distinction because he lives in the world of encryption where the phrase "end-to-end encryption" has a very specific meaning. But it's easy to miss this important distinction.

The reason iMessage imposes a 32-member limit on group messaging, which I mentioned earlier, and Signal and WhatsApp both impose around 1K limits, is that these services, which Matthew describes as "industry-standard modern messaging applications," are all actually encrypting every party's message, end-to-end, individually to every other party. Telegram is incapable of doing this ever. It has no ability to do this under any circumstances.

So while it's true that Telegram's individual connections are always encrypted, it's only when two - and only two - parties are simultaneously online and Telegram's users opt to enable end-to-end encryption for that single, that two-party dialog, that any truly unobservable conversation ever takes place over Telegram. All larger group chats are being decrypted by Telegram's servers for re-encryption and sending to other Telegram users. Remember that Matt mentioned that industry-standard modern messaging applications never get the keys that are being used by end-users to exchange messages. Telegram has all of the keys. So obviously this is a crucial distinction.

Okay. Returning to Matthew's explanation, he says: "While it may seem like I'm being picky, the difference in adoption between default end-to-end encryption and this experience" - that is, having to do four clicks and digging down and hit menus and turning it on only when the other guy is online, he says - "is likely very significant. The practical impact is that the vast majority of one-on-one Telegram conversations - and literally every single group chat - are visible on Telegram's servers, which can see and record the content of all messages sent between users. That may or may not be a problem for every Telegram user, but it's certainly not something we'd advertise as particularly well encrypted." He said: "(If you're interested in the details, as well as a little bit of further criticism of Telegram's actual encryption protocols, I'll get into what we know about that further below.)"

He says: "So does default encryption really matter? Maybe yes, maybe no. There are two different ways to think about this. One is that Telegram's lack of default encryption is just fine for many people. The reality is that many users don't choose Telegram for encrypted private messaging at all. For plenty of people, Telegram is used more like a social media network than a private messenger."

Leo: And by the way, when we talked about this ages ago, that was exactly the conclusion we came to.

Steve: Right.

Leo: Was that Telegram is encrypted enough, or is not encrypted at all, but that's good enough. I think that was actually the phrase you said, "good enough messaging."

Steve: Right. Right.

Leo: Yeah. And so people, as long as you know that, and they don't advertise otherwise, that's fine. But unfortunately they imply that it is encrypted.

Steve: Yes. And even to the point where Pavel, I don't think I have it in the show notes, but Pavel has actively attacked Signal and WhatsApp...

Leo: Oh, yeah.

Steve: ...deriding their encryption.

Leo: He says, "Oh, the government has backdoors into those guys." Well, the government doesn't need a backdoor. It's Signal. Geez Louise.

Steve: Yeah. So he said, he was talking about how they use it as a social media network more than a private messenger.

Leo: Right.

Steve: And he said: "Getting more specific, Telegram has two popular features that makes it ideal for this use-case. One of those is the ability to create and subscribe to 'channels,' each of which works like a broadcast network where one person, or a small number of people, can push content out to millions of readers. When you're broadcasting messages to thousands of strangers in public, maintaining the secrecy of your chat content isn't important."

Leo: No.

Steve: And he says: "Telegram also supports large group chats that can include thousands of users. These groups can be made open for the general public to join, or they can be set up as invite-only." He said: "While I've never personally wanted to share a group chat with thousands of people, I'm told that many people enjoy this feature. In the large and public instantiation, it also doesn't really matter that Telegram group chats are unencrypted. After all, who cares about confidentiality if you're talking in the public square?"

He says: "But Telegram is not limited to just those features, and many users who join for them will also do other things. Imagine you're in a 'public square' having a group conversation. In that setting there may be no expectation of strong privacy, and so end-to-end encryption doesn't really matter to you. But let's say that you and five friends step out of the square to have a side conversation. Does that conversation deserve strong privacy? It doesn't really matter what you want, because Telegram won't provide it, at least not with encryption that protects you from sharing your content with Telegram's servers.

"Similarly, imagine you use Telegram for its social media-like features, meaning that you mainly consume content rather than producing it. But one day your friend, who also uses Telegram for similar reasons, notices you're on the platform and decides she wants to send you a private message. Are you concerned about privacy now? And are you each going to manually turn on the 'Secret Chat' feature, even though it requires four explicit clicks through hidden menus, and even though it will prevent you from communicating immediately if one of you is offline?

"My strong suspicion," he writes, "is that many people who join Telegram for its social media features also end up using it to communicate privately. And I think Telegram knows this, and tends to advertise itself as a 'secure messenger,' and talk about the platform's encryption features precisely because they know it makes people feel more comfortable. But in practice, I also suspect that very few of those users are actually using Telegram's encryption. Many of those users may not even realize they have to turn encryption on manually, and think they're already using it.

"And this brings me to my next point: Telegram knows its encryption is difficult to turn on, and they continue to promote their product as a secure messenger. Telegram's

encryption has been subject to heavy criticism since at least 2016, and possibly earlier, for many of the reasons I outlined in this post. In fact, many of these criticisms were made by experts, including myself, in years-old conversations with Pavel Durov on Twitter."

And Leo, I'm going to inject something next, but let's take our final break.

Leo: Okay.

Steve: And then we're going to get into what Matthew thinks about the actual technology that Telegram has deployed.

Leo: Stay tuned for Steve's injection. Okay, Steve. Time for my injection.

Steve: Okay. It was an interjection, but yes.

Leo: Oh. Not an injection, an interjection. Much better.

Steve: I'm going to interject here.

Leo: Okay.

Steve: To note that back in the morning of March 29th, 2015, after Matthew first sat down to take a serious long look at Telegram's encryption protocol and its system, his Tweet linked to Telegram's page. I've got the link in the show notes for anyone who's interested. And the Telegram page is titled "Creating an Authorization Key." So he tweets the link, and then he says: "Like seriously. What the F is even going on here?" Okay, so this is a top cryptographer who understands this stuff, who looks at Telegram's technical document on creating an authorization key and is scratching his head.

Okay. So he writes: "Although the interaction with Durov" - now he's speaking of the interactions that the security community, including himself, had sometime later, actually in 2016, the next year. He said: "Although the interaction with Durov could sometimes be harsh," he said, "I still mostly assumed good faith from Telegram back in those days. I believed that Telegram was busy growing their network and that in time they would improve the quality and usability of the platform's end-to-end encryption." And remember, when he says that, he means exactly that, end-to-end. And he said, which is to say, the platform never has the keys, only the endpoints know the keys that are being used to encrypt and decrypt their conversation. That's the key. Telegram only offers that if you jump through hoops, and it's never on by default. There is no on because of like the hoops you have to jump through.

So he said: "I believed that Telegram was busy growing their network and that in time they would improve the quality and usability of the platform's end-to-end encryption. For example, by activating it as a default or providing support for group chats, and making it possible to start encrypted chats with offline users." You know, those are all things we take for granted, right, in all the other state-of-the-art platforms. They all do all of that. He said: "I assumed that while Telegram might be a follower rather than a leader, it would eventually reach feature parity with the encryption protocols offered by Signal and

WhatsApp. Of course, a second possibility was that Telegram would abandon encryption entirely and just focus on being a social media platform.

"What's actually happened," he wrote, "is a lot more confusing to me." And of course he's being generous. He said: "Instead of improving the usability of Telegram's end-to-end encryption, the owners of Telegram have more or less kept their encryption user experience unchanged since 2016. While there have been a few upgrades to the underlying encryption algorithms used by the platform, the user-facing experience of Secret Chats in 2024 is almost identical to the one you'd have seen eight years ago. This, despite the fact that the number of Telegram users has grown by seven to nine times during the same time period.

"At the same time, Telegram's CEO and sole owner Pavel Durov has continued to aggressively market Telegram as a 'secure messenger.' Most recently he issued a scathing" - oh, I do have it in the show notes - "a scathing criticism of Signal and WhatsApp on his personal Telegram channel, implying that those systems were backdoored by the U.S. government, and only Telegram's independent encryption protocols were really trustworthy." Well, you might argue the government couldn't understand them, so maybe. Anyway, he says: "While this might be a reasonable nerd-argument if it was taking place between two platforms that both supported default end-to-end encryption, Telegram really has no legs to stand on in this particular discussion. Indeed, it no longer feels amusing to see the Telegram organization urging people away from default-encrypted messengers, while refusing to implement essential features that would widely encrypt their own users' messages. In fact, it's starting to feel a bit malicious.

"So what about the boring encryption details? Since this is a cryptography blog I'd be remiss if I didn't spend at least a little bit of time on the boring encryption protocols. I'd also be missing a good opportunity to let my mouth gape open in amazement, which is pretty much what happens every time I look at the internals of Telegram's encryption. I'm going to handle this in one paragraph to reduce the pain, and you can feel free to skip past it if you're not interested."

Okay, now, I am going to interrupt Matthew again to note that he has laced his description, which I'm about to share, with asterisks. And later he explains that: "Every place I put an '*' in the paragraph is a point where expert cryptographers would, in the context of something like a professional security audit, raise their hands and ask a lot of questions." Okay. So I'll just - I'll say the asterisks as I'm sharing this, and now you know that every time there's an asterisk, this is Matthew saying, uh, what?

Okay. So he writes: "According to what I think is the latest encryption spec, Telegram's Secret Chats feature is based on a custom protocol called MTProto 2.0. This system uses 2048-bit* finite-field Diffie-Hellman key agreement, with group parameters (I think)," he says, "chosen by the server.* Since the Diffie-Hellman protocol is only executed interactively, this is why Secret Chats cannot be set up when one user is offline.* MITM protection is handled by the end-users, who must compare key fingerprints. There are some weird random nonces provided by the server, which I don't fully understand the purpose of* and that in the past used to actively make the key exchange totally insecure against a malicious server, but this has long since been fixed.* The resulting keys are then used to power" - here it comes - "the most amazing, non-standard authenticated encryption mode ever invented, something called 'Infinite Garble Extension' (IGE), based on AES and with SHA2 handling authentication.*"

Leo: You said "Infinite Garble"?

Steve: Infinite Garble Extension, IGE.

Leo: Honestly, the more I've been thinking about this, the more I think this is actually malicious, that this is not ignorance. They know exactly what they're doing is what I think.

Steve: Yeah, yeah. And that is the point that Matthew's come to is that they know what's going on. Pavel knows this is not actually encrypted. And I'm sure he's telling governments, oh, we can't get in. We can't moderate. This is super secure. No. So anyway, he says, Matthew says: "I'm not going to go further than this. Suffice it to say that Telegram's encryption is unusual." And I love that he said "the most amazing nonstandard authenticated encryption mode ever invented, something called Infinite Garble Extension." Right.

Anyway, he said: "If you ask me to guess whether the protocol and implementation of Telegram Secret Chats is secure, I would say quite possibly. To be honest, though, it doesn't matter how secure something is if people are not actually using it.

"So," he says, "is there anything else to know? Yes, unfortunately. Even though end-to-end encryption is one of the best tools we've developed to prevent data compromise, it is hardly the end of the story. One of the biggest privacy problems in messaging is the availability of loads of meta-data essentially data about who uses the service, who they talk to, and when they do that talking. That data is not typically protected by end-to-end encryption. Even in applications that are broadcast-only, such as Telegram's channels, there is plenty of useful metadata available about who is listening to a broadcast. That information alone is valuable to people, as evidenced by the enormous amounts of money that traditional broadcasters spend to collect it.

"Right now all of that information likely exists on Telegram's servers, where it's available to anyone who wants to collect it. I'm not specifically calling out Telegram for this, since the same problem exists with virtually every other social media network and private messenger. But it should be mentioned, just to avoid leaving you with the conclusion that encryption is all we need."

Okay. So there are many useful wonderful bits among what Matthew wrote. One is that while Telegram's crypto is bizarre, on its face it's not obviously insecure. But neither has it ever been shown to be secure. Mostly, it's just bizarre. Or as Matthew put it, what the "F"? The most important thing for Telegram's users to appreciate is that what Matthew referred to as today's industry-standard encrypted messaging apps provide always-on end-to-end encryption by default, while extending that true end-to-end encryption no matter how many individuals are participating in chat groups. And you know, Leo, I didn't think of this when I was putting this down on paper yesterday. But Telegram is actually riding on the coattails of the other messaging apps.

Leo: Oh, yeah. Oh, we do it, too. We're end-to-end. See?

Steve: Yeah.

Leo: Yeah.

Steve: Because Apple and Signal and WhatsApp have established the idea that everything is secure because they actually are.

Leo: Right.

Steve: Telegram's just saying yeah, we are, too.

Leo: Yeah, us, too.

Steve: Yeah, you know, we do that. That's what messaging is, encrypted. Yeah. So also remember that last time we talked about iMessage and saw that not only had Apple implemented true multi-party end-to-end encrypted messaging, but that iMessage is also offering true forward secrecy by periodically and continuously rolling its conversation keys. iMessage and Signal offer technology that Telegram has never had and, as Matthew noted, shows no sign of obtaining or even wanting.

Leo: It's pretty clear they don't. They don't want it, yeah.

Steve: Right. Well, and look. They've gone up by a factor of seven to nine, I mean, it's super popular. Why complicate that with additional technology? It's like they don't need more encryption. They're able just to claim it. And of course, Telegram's popularity may not really be about true security; right? It's more about subscribing to its channels with a weaker assumption that, well, "Things are secure here," only because Telegram also has the unearned reputation of being a secure messaging system.

So anyway, you know, they're unable to offer what the other guys offer with much smaller groups. And it's a benefit that Telegram is able to have these massive hundreds of thousands subscriber broadcasts. They cannot make it end-to-end encrypted. So they don't. Yet they're getting the benefit of doing so.

Anyway, Matthew began, as we know, by posing the question: "Is Telegram an Encrypted App?" The most generous answer would be that, while it can be forced to provide state-of-the-art end-to-end encryption between two online parties, it certainly is not "as encrypted" as the general public, its users, and the press have all come to assume. More than anything else its ability to broadcast to very large groups has turned it into a social media platform with an air of undeserved security and privacy. So thank you, Matthew Green, for laying it out.

Leo: There you have it. Yeah. I think that's - I read the piece, too. I'm glad you brought it back because it was very interesting, and I thought a pretty big takedown of it. Unfortunately, the people who most need to read it will not, never know.

Steve: This is just for our listeners.

Leo: Yeah. And even our listeners already know this because we've covered this subject.

Steve: Yeah.

Leo: Before. I like Telegram. Actually, I shouldn't maybe mention this, but right now we're streaming on seven streams, as you know - YouTube and Twitch, LinkedIn, Facebook, Twitter, Discord, and Kick. And I think we're going to replace Kick with Telegram.

Steve: Telegram.

Leo: Because I, you know, in fact I loved - maybe eight years ago when it really took off, I said, I want everybody to use this. But we talked about this, and it was as you said, good enough. It's not encrypted. But most of the time you don't expect that. The standards have changed now, thanks to Apple and Google, using RCS in Google's case, Apple uses RCS encryption.

Steve: And Leo, the podcast, your network podcasts don't need encryption.

Leo: Right. We don't want them to be encrypted. We want everybody to see them.

Steve: Yeah.

Leo: Yeah. So I think Telegram, I don't know, you can't - I don't know. We'll see. You know what's cool, though? We have 764 people watching on those seven platforms right now. And I think that's a great way to introduce ourselves to a new audience.