*Episode 35: Three Buddy Problem*

# North Korea's biggest ever crypto heist: $1.4B stolen from Bybit

**LISTEN:**
https://securityconversations.com/episode/north-koreas-biggest-ever-crypto-heist-1-4b-stolen-from-bybit/

**Cast:**

- Juan Andres Guerrero-Saade
- Costin Raiu
- Ryan Naraine


COSTIN (00:01.112)
So was watching Joe Rogan's latest episode and he has this advertisement for Zero Day on Netflix. Did you guys see that?

JAGS (00:05.977)
Ha ha ha!

JAGS (00:10.425)
What are you doing watching Joe Rogan, bro? I'm worried about

Ryan Naraine (00:10.933)
this is new Netflix show.

COSTIN (00:13.358)
It's a new show, new show. And I was like, why, how come that we are not sponsored by Netflix? I mean, we are a better choice for Zero Day Anything than Joe Rogan.

JAGS (00:22.979)
Is it good though? Like I wanna watch this thing.

COSTIN (00:25.259)
I like them.

Ryan Naraine (00:25.456)

In all seriousness, hear the casting is great and everyone in security is talking about it. A lot of NSA hacking everything apart.

COSTIN (00:28.384)
Robert De Niro

There's like NSA hacking people's signal, like left and right. There's a commission that basically, it can bend any law. Like they can do whatever they want.

JAGS (00:32.247)
And I say, I love this country, bro. That's right.

JAGS (00:44.825)
That's cool. Sounds realistic. I'm about it.

Ryan Naraine (00:47.79)
Hello everyone, this is the ThreeBuddy Problem, a podcast on the Security Conversations Network. I'm here with my buddies, Kostin and Juanito. Big week, big week of news this week. I want to start right off the top with this cryptocurrency exchange Bybit, apparently a Dubai-based.

COSTIN (00:55.917)
morning.

JAGS (00:56.899)
Morning.

Insanity.

JAGS (01:04.569)
Okay, what the fuck is going on? And I say that because like I felt so proud of myself that I like prepared, I read all the articles, all the shit, I was gonna be so ready. And then you guys just pop off with like the live investigation magic money bullshit. the hell's going on, man?

Ryan Naraine (01:18.595)
Magic money!

Costin this is your turn to shine buddy, your magic money people. Magic money people in the news. No in all seriousness this is being billed as the biggest crypto heist in history. 1.4 billion. In history, 1.4 billion dollars stolen from this Bybit cryptocurrency exchange and directly tied to Lazarus which is a North Korean threat actor. So Costin right off the top, can you kind of level set what we know as of right now?

COSTIN (01:31.712)
It's the biggest heist crypto or not. Yeah, yeah.

COSTIN (01:50.99)
Well, just to set the stage, first of all, Bybit is the world's, think, largest, third largest crypto exchange. So I think it's right before after Binance, which is probably the world's largest. And this is a company, I think they originally started in Singapore, but they moved to Dubai, which has become kind of the the Mecca for

cryptocurrency stuff because there's no KYC. It's pretty easy for someone, for instance, to start a company in Dubai, open a bank account. Then they create an account in an exchange there. They deposit the funds. They swap the funds to dollars. They move the dollars into their bank account. And next to the cryptocurrency exchange, there's a bank where they cash everything with like minimal, minimal commission fees. So like almost nothing.

Ryan Naraine (02:46.48)
Have you heard about this by bit before today? It's a known in your world? Okay.

COSTIN (02:48.97)
I admit I have not. I admit I haven't. I've heard of the ones that had all sorts of troubles with the law. for instance, yeah, the CEO of Binance, CZ, he was in jail in the United States for a while. The founders of a number of other cryptocurrency exchanges, they're sanctioned. KuCoin, for instance, they're sanctioned.

Ryan Naraine (02:56.836)
That's when we hear about them.

COSTIN (03:15.864)
pretty much, you that's when you hear about them. But to be honest, I haven't heard of Ben Zhou or Zhou before. What can I tell you for sure is that I was impressed about how he handled this incident, which again, he's the CEO of of Bybee, correct, Ben Zhou.

Ryan Naraine (03:29.828)
He's the CEO of Bybit, right? Benjoo.

And he confirmed, he confirmed the hack. What, what, did he say and what? Yeah.

COSTIN (03:38.388)
It seems he did it. in a way, he's the one who, let's say, clicked or approved the transaction, which turned out to be something else because most of these transactions and the way that hackers sometimes steal the funds is they kind of require user interaction, especially when you have to move the money from the cold wallets into the hot wallets. And in case people don't know, typically

big exchanges, keep all their money, funds in a vault, like the gold that Fort Knox, if there's any left. And every now and then they just move the funds from the vault into the kind of the real

world. But otherwise, money are just safely stored there. And the nice thing about crypto, by the way, is that you can prove that those money actually exist, unlike the gold that may or may not be.

cryptocurrencies can be proven like on the blockchain this is like our deposits these are our funds you can watch like sometimes you can even watch it in like with popcorn you can watch it in real time so what happened here is that he thought that he was moving some of the money from the vault into the hot wallets which is the wallets connected to the internet with the bots with everything

JAGS (04:34.701)
Wow.

JAGS (04:41.047)
You can even watch people heist it, like completely, just make it disappear. It's great.

JAGS (04:50.295)
emotions.

COSTIN (05:01.39)
and he approved the transactions with something called SAFE which by the way it used a harder token he said that he used a ledger I think to approve the transaction which is again kind of impressive because this is not let's say like a stupid silly mistake no this was like a sophisticated thing in which their multi SIG called wallet was

compromised and that means that every single person that had to sign that transaction and typically is not just one but when it's a multi-seag wallet several people have to sign it so I sign you sign one signs and if all three of us we sign it only then the transaction goes so the Lazarus guys they managed to fool everyone they are in the company all and of them if you want

Ryan Naraine (05:56.475)
This is a technological hack.

COSTIN (05:59.146)
It's I think a super technological, but also there must be a lot of social engineering involved because when he said when he signed the transactions, he said he saw a totally different amount. He thought that he was moving like a few million dollars in funds, not billions. And obviously he didn't realize that the money were going to the hackers address. So now there's

speculation mostly about how this was achieved some people claim that the Lazarus guys they managed to compromise everyone like infect their computers with malware through different kind of investment applications which is quite typical for them they trick people into running Python code off of GitHub and you think maybe if you get some Python code and you look at the code and there's nothing malicious in there

Maybe it's just talking to an API to get the latest exchange rates. But then I think they exploited vulnerability into one of these things. This is one of the theories. And that is exactly what gave them remote code execution on the machines. Maybe at least one in the beginning and then they move laterally to all the people who are doing the multi-sig wallet thing.

Ryan Naraine (07:23.738)
Juanito, this is typical TTPs for Lazarus Group. just quickly before we get to Juan, Costin, how can you shed some light on the quality of the attribution here? How do we know exactly that it's Lazarus Group? It feels like this happened overnight and everyone's already pointing to North Koreans. Is there strong evidence there or is it shaky?

COSTIN (07:33.902)
Mm-hmm.

COSTIN (07:38.606)
Mm.

COSTIN (07:43.01)
I would say it's good. It's a kind of good evidence that we saw with WannaCry back in the days. If you remember, it was Ben Nemo who posted something on Twitter back then linking an early version of WannaCry with the Lazarus group. So maybe this is kind of similar in the sense that before running the heists, the Lazarus guys sometimes they test those wallets to make sure that actually they work. So like one of the

most stupid things in crypto is that you get a new wallet and you move all your money to the new wallet and turns out that the new wallet is broken somehow and you lost everything. It happens more often than you can imagine. Then there's people sending money to the zero address like to nowhere. And yeah, it's so easy to lose money, which is why people test. And in this case, it's connected, I think, to the Lazarus Group in multiple ways.

And here when we say it's connected, it's connected to cases that the FBI said in the past were connected to the Lazarus group. So it's not just things that people say, random people say, yeah, that was Lazarus. But the FBI themselves, for instance, they link some of the hacks such as the Ronin hack, which was before this, which was, I think, the largest cryptocurrency heist in history. was 600 plus million dollars.

And that one is linked by the FBI to Lazarus. Now the methods, the TTPs are also similar to Lazarus. So pretty much everything in this story actually screams Lazarus. And I think also it's interesting to say that the researcher who made the connection first, he cashed a bounty from Arkham. Arkham being a platform for cryptocurrency blockchain attribution.

style investigations if you want and he got a bounty of $30,000 for being the first who linked the Lazarus Group to this which is now again the largest cryptocurrency and not just cryptocurrency

heist in history. By the way we should also mention Lazarus previously they were trying to steal $1 billion from the Bangladesh National Bank right the Bangladesh Bank heist.

COSTIN (10:10.038)
which is what made them famous. And I saw like another very cool case in history, which was when Saddam Hussein was trying to flee Iraq, he instructed his son to go to the bank and cash $1 billion, just to draw $1 billion in cash, which is considered to be the biggest heist in history, Saddam Hussein and his son trying to cash $1 billion.

Ryan Naraine (10:36.74)
So this 1.4

JAGS (10:37.585)
How do you physically move a billion dollars? Bank notes, I guess? You would need central bank notes, I guess. Because there are bigger denomination bills for banks.

COSTIN (10:40.244)
look i i was wondering i

yeah mm-hmm good point yeah sure to move them between the banks right or if you go purely in cash I guess a million dollars is what like a few kilograms no idea I've never seen a million dollars no it's less than a few kilograms

Ryan Naraine (10:50.81)
catch man

JAGS (11:01.369)
No, no, no, it's like a million dollars is like 17 pounds in cash.

Ryan Naraine (11:07.696)
1e2

COSTIN (11:07.726)
17 pounds what's that?

JAGS (11:10.081)
Like, like, like eight, seven, I'm not good at math.

COSTIN (11:11.502)
4 kilograms.

COSTIN (11:16.526)
It's a few kilograms. It's a few kilograms. So that would be like tons. It would be like tons.

Ryan Naraine (11:16.592)
I don't know where we went off the rails. One into I want to circle back. I want to circle back to this Lazarus thing. did we, how did we move? How did we move from North Korea doesn't have internet access to North Koreans being like the most elite teams of crypto hackers capable of picking off $1.46 billion and

JAGS (11:25.889)
Why are you circling back, man? Why? Why?

COSTIN (11:34.19)
to 1.4 billion dollars.

Ryan Naraine (11:43.471)
having an entire system in place and a structure in place to launder it and to eventually kind of move it around. Are we falling for our own propaganda that there's no internet access there or have they really invested? Like help me understand how you view that ecosystem.

JAGS (11:58.437)
Those things are not mutually exclusive, right? Like those people may very well be eating cardboard and not have access to the internet. And they still have like an elite team of hackers, which in part, like we know they're like affiliated with North Korea, but previous reporting usually puts them as not, it's not physically like the hackers, the operators themselves are not physically within North Korea. You hear a lot about like China, Thailand, maybe Russia and like

There's this sort of notion of like pay your own way, right? Like a lot of the the heist thing is also sort of like supporting your study abroad Initiative that the North Korean government has been kind enough to bestow upon you But I am and we we've definitely talked about this very early in the podcast. I am always kind of fascinated and and humbled a little bit by the Lazarus group

writ large. And I say that because when we worked as part of Operation Blockbuster, Jaime Velasco and I did some research, then Kosen and I did some research, and we contributed our bit to the endeavor. The notion was not of a hyper sophisticated group. It was more pulling the threads of a bunch of separate attacks, things that

malware families that had never been correlated, et cetera, and showing that like, hey guys, like there's actually this giant iceberg that we now call Lazarus. So that's what OpBlockbuster gave us. But that was very much an accomplishment fixed in its time, which I believe was like around 2015, 2016. Since then, what you see is a

an evolution, a growth, a development, a diversification, an ecosystem building, an investment on the part of the North Koreans of saying, they started to take it seriously as it actually succeeded and it showed itself as a revenue generator and not just some soft Intel thing or somebody's ability to fuck up somebody's day in South Korea by ransoming them or deleting all their data.

JAGS (14:17.753)
Once it became recognized as a revenue generator, what you see is an investment that I failed to predict, that I definitely would not have read. I assumed the North Koreans would be, they were shitty when I last checked in on them, and I assumed they would have stayed shitty. Even when we saw the beginnings of these operations becoming nation-state bank heists, essentially. Nation-state

Sponsored robberies. I still didn't realize that We would see in the North Korean hacking teams what we expected to see in the ransomware groups But didn't which is when you get a fuck ton of resources you can level up and Like I don't know if that means buying exploits developing exploits training having more operators Increasing your operational tempo increasing your remit it probably all of those and more but

I don't know that we've seen the ransomware groups reinvest their ill-gotten gains into improving their ops and getting zero days to that level. Whereas with the North Koreans, I'm not saying that it's through reinvestment, but the quote unquote Lazarus group of today, because today, I don't think the Lazarus group exists as the Lazarus group. You're using it as a big-ass umbrella term for what are now a bunch of groups.

but.

The Lazarus group of today, I don't think we could have dreamed of comparing them to 2015, 2016.

Ryan Naraine (15:59.909)
Costain, you agree with him that we've largely overlooked and kind of

JAGS (16:07.097)
No, wait, wait, wait. We haven't largely overlooked. largely overlooked. Like, Kostin was the one who opened my eyes, right? Like, Kostin was the one who like, oh, these guys are like improving faster than anybody else. He said it on the podcast. I want to say it's like episode like two or three. And that was for me a realization that, you know, I'm not saying everybody else, like Song Sue and Vitali and a bunch of other people have like known this shit. I'm just late to late to know.

Ryan Naraine (16:12.314)
No, and I'm asking the question is...

Ryan Naraine (16:31.63)
Right, no, no, no, the people in the trenches understand this stuff. I'm talking about in a general sense, we have this propaganda in our heads that there's no internet there, it's a backward society with no internet and no one has access to anything and we start to see this kind of sophisticated hacks over and over and over again. We see this kind of deliberate detailed

strategy around fake IT workers. You talked about using Python scripts on GitHub. You talk about like the long game, like playing the long game, working on infecting these.

COSTIN (16:40.792)
Mm-hmm.

Ryan Naraine (17:00.568)
employees at these crypto banks and exchanges and so on and slowly you start to see the pieces coming together. And what I wanted to ask one, you believe in general we've kind of overlooked it and like what happens next with this? Like help someone like me who doesn't understand this world. What happens when money gets put into a wallet? It needs to be laundered and cleaned and moved through exchanges and some exchanges are blocking it and there's a risk that you can get the money frozen and seized and like.

COSTIN (17:14.893)
Mm-hmm.

Ryan Naraine (17:29.934)
Like, me understand, it $1.4 billion gone forever? Is there chances that this money gets back? What happens next?

COSTIN (17:35.019)
Mm-hmm.

First of all, I think that it's very bad to overlook what North Korea can do because let's keep it in mind that North Korea is a nation who has nuclear weapons. They have people fighting in Ukraine on the Russian side. They say, know, initially they were totally unexperienced, but now they're learning and getting better and better and better.

Like two of the, you know that there's two kinds of taekwondo in the world. There's the World Taekwondo Federation and the International Taekwondo Federation, which are basically first is the South Koreans and the other one is the North Koreans. WTF, correct. So they renamed it recently to WT, no F, because people were very confused. But like my diploma here, this is a WT, formerly F.

JAGS (18:14.489)
WTF.

Ryan Naraine (18:23.152)
Yeah.

JAGS (18:23.203)
This is the GRU GU shit.

COSTIN (18:30.892)
diploma. like, yeah.

JAGS (18:32.698)
You need to show it, man. It's out of screen. You gotta bring it into...

COSTIN (18:35.95)
But if you look at North Korea, there in the Olympics, I was looking at the Olympics with Simone Biles, right? And like in the top 10, there were North Korean athletes and for a country that, you know, they're living in communism and people think that the situation there is very bad. I think that they are overperforming and they have power to be reckoned with. So definitely do not overlook what they can do.

For me personally, the realization came when I saw them exploiting this race condition in a Solidity compiler, which was kind of impressive in my opinion, just to steal again, steal more cryptocurrencies, but that kind of work. Yeah, that's a cutting edge. All right. So that's one thing. I was also thinking that back by the way.

JAGS (19:22.083)
That's the one we talked about. That was the one that you used to like open my eyes, right?

Ryan Naraine (19:24.016)
Correct.

COSTIN (19:33.558)
It's very easy to think that communist countries are incompetent or incapable because everything is so fake and everyone's clapping for the supreme leader. But in reality, the hardship, it creates some very tough motherfuckers, if you want. Like back in the days, you know, I grew up in Romania in communism and Romania was like right there in the top in the Math Olympics. We had like some of the best people in mathematics.

Some of my teachers, math teachers, they immigrated and now they're teaching at MIT and other prestigious universities in the States. So the hardship, I think, know, hardship builds very tough people and they can be very, very dangerous on many aspects. Now what happens to the money? This is, I think, when the fun part begins because...

JAGS (20:11.821)
Lex Friedman taught Kostin I think early on.

COSTIN (20:31.776)
In cryptocurrency, laundering is everything. you steal cryptocurrencies, laundering the funds is everything because all the big exchanges, they have blacklists. So the moment they see money coming from any of these stolen or somehow associated with these stolen funds, they will

immediately block it. So now the Lazarus guys have historically been super, super adept at laundering funds with the

Bangladesh bank heist they were trying to launder that through casinos if you remember in Macau Correct Nowadays what happens with these cryptocurrencies? So what was impressive again in the past was that they're bridging it between different chains So let's say if they steal this etherium as we have here They are converting the etherium into another chain like Solana or polygon

Ryan Naraine (21:06.934)
yeah

COSTIN (21:28.302)
And during this conversion, the kind of the addresses, if you want, they get lost. even if you, let's say, have the input and the output, sometimes they try to exploit that. So in one case, for instance, one of these bridges that would swap one thing into another, it allowed you to specify the source address. And they were using an address associated with Vitali.

Buterin, which is the founder of Ethereum, just to bypass all these kind of know your customer checks. So they're very good. Now, like I said, the fun begins because some cryptocurrencies have already started cryptocurrency exchanges or bridges. They've started seizing the funds. So for instance, some of the stolen coins, they were this mental staked Ethereum. So like the

Interesting thing about Ethereum, yes, Ethereum you can stake it. Like if you have some Ethereum you can stake it and then you get interest, which is about 3 % I think per year. And there's all these protocols which allow you to stake Ethereum and essentially pocket free money, free magic money in your pocket like every couple of days.

Ryan Naraine (22:50.21)
At some stage in this, in this laundering process, does it ever become undetectable completely? Or is it always, do we have technology at some point that can do this tracing all the way to the end? Because it helped me understand how it becomes cold hard cash.

COSTIN (23:02.606)
Yeah, yeah, so most of the laundering, how does the laundering work? It works, let's say somebody digs a hole and there's 20 of us that we want to launder and everybody throws their pocket change into this hole and then we wait for a while and then we go and everybody takes back whatever they put in that hole.

But maybe I take your money, take Juan's money, Juan takes my money and you don't know exactly what came from where.

Ryan Naraine (23:34.49)
Why are we leaving it in a hole for a certain amount of time? What's the equivalent there?

COSTIN (23:37.844)
Well, because we want enough people to come and throw their pocket money into the hole as well, right? And we want like, yeah, we want the hole to be like full of money from America, from Latin America, from Lebanon, from Syria, from Russia, China. These are the mixers, correct? These are the mixers. So in reality, like even the...

Ryan Naraine (23:45.924)
This is just muddying the hole.

Ryan Naraine (23:56.859)
So what are these holes called? These are the mixers. Huh.

Ryan Naraine (24:04.442)
Don't laugh Juanito. This is like, so, so really, so, so, so there are these mixers, these, these, these, that's an exchange.

JAGS (24:05.891)
Guys, what the fuck?

COSTIN (24:08.014)
You

JAGS (24:08.983)
Magic money bullshit.

COSTIN (24:12.6)
There are. Yeah. And I think there's some famous kids are tornado. Tornado was one of the mixers that they were using in the past. And actually tornadoes founders, I think they got arrested because of this, particularly because Lazarus was trying to launder and they successfully laundered hundreds of millions of dollars through the tornado protocol.

So they went to jail, think one of the guys was recently a Russian programmer was recently released from jail and possibly under Trump, you know, he'll he'll just walk away. But there's a lot of these mixers in particular, the one which is making the news at the moment is an exchange called EXCH, which to me it looks it's a Russian decentralized exchange. Now,

The guys from Bybit actually reached out to EXJs and said hey whenever the money are coming in from these stolen funds can you please seize them? And this guy said no fucking way you bastards we're not gonna stop anything because do remember the last time when some of our users were trying to cash out on your exchange and you seized our funds so we're not gonna help you so it's a lot of drama this is like

JAGS (25:31.073)

Ryan Naraine (25:33.551)
my gosh.

COSTIN (25:37.012)
If you're wondering what's happening in this world, there's a lot of drama, even more than in InfoSec. And the other one is ChainFlip, which is an interesting platform from the guys who developed Session. If you're familiar with the Session Messenger, it's another like Tor-like cryptocurrency-powered secure encrypted communications platform that will soon be super illegal in the UK.

And they developed this thing called ChainFlip as well. And they were already swapping some of the amounts on ChainFlip and people reached out to ChainFlip and said, hey, can you please hold the money? And the ChainFlip guys were saying like, well, we are very new. We don't even have a mechanism to stop it. they just, I think they paused everything, all the pools. They paused the pools so they can actually implement some kind of filtering. So if you ask me.

It's gonna be a kind of a cat and mouse game with laundering the money for the next at least two years if not even more because like traditionally the Lazarus guys they launder a bit in the beginning sometimes and then everyone you know is super fresh and super aware and they can't launder anything anymore so then they're gonna just let you know the the coins just sit there in the hole for a while and

then after one year like if someone is still looking they're gonna start swapping them on new platforms preferably because these kind of new exchanges appear all the time so they're just gonna wait for new exchanges to appear that have no blacklist and swap some of them there and always they'll like try so they'll take some money put it into 50 wallets and then those 50 they're gonna try it on on a number of different

decentralized exchanges and some of them will be seized, some will work. I think in the end they do lose some of the funds. Like in this case, for instance, Mantle managed to seize a part of the money, like a few million dollars. So they're going to lose. They're not going to get $1.4 billion in cash in China in Binance. So probably they're going to initially get

COSTIN (28:00.866)
Maybe a few million dollars, tens of million dollars and...

Ryan Naraine (28:04.176)
The bait isn't gonna get their money back either.

COSTIN (28:06.702)
I have no chance now. I think there's zero probability that Bybit are going to get their money back. They put together a bounty of 10%, which is $140 million to whoever helps them recover the money. So whenever, let's say somebody gives them back a million, they'll give 10 % of that.

If you, Ryan, can bring them back a million, they'll give you $100,000, which is typical in this business.

Ryan Naraine (28:41.808)
How did we get left behind so far? That this all sounds like real magic to us.

COSTIN (28:48.41)
You didn't invest in the Tanase projects when I told you.

JAGS (28:48.569)
We got old.

We got old somehow. No, I think it takes a certain, like, there's a certain amount of literacy to understand the space, but there's also like a necessary suspension of disbelief that if you're not open to it, it makes it very hard to look at this thing in its own language, if it makes sense.

Ryan Naraine (29:21.05)
Yeah.

JAGS (29:21.241)
Right, which is also not necessarily a bad thing, right? Like, there's amazing researchers like Jackie Coven that, you know, can do some magic in this sort of like crypto analysis, like a cryptocurrency analysis, like chain analysis type work. But at the same time, like I do think it's healthy to also keep a

an outsider looking in perspective that you can tap into to say things like what you were just saying now, right? Like, okay, so the mixers are the whole, and we're putting the thing in here. And like every once in a while, you feel like a total fucking boomer putting it that way. But it also keeps some of it straight, where I think a lot of the crypto world would prefer that it be a little more muddy, a little more forgiving, a little more like San Francisco, like, you

Ryan Naraine (30:15.76)
Cryptic, yeah.

JAGS (30:16.633)
Valley magic and like, believe me, bro, like I'm this like Messiah for currency and everybody wants to get rich and we're in a period of mania when it comes to markets. So of course we're going to end up here. What I am genuinely fascinated by is I'm just curious like what all of this money, what institutional money is going into these fucking

cryptocurrency, not just exchanges, but other types of coins, these bridges, these things, because like these people aren't breaking into some random bridge and being like, fuck, there's only five Bitcoin here because like no one's really using this bridge. Every time they walk into

some random shitty, like half baked project nobody had ever heard of to move like this one bullshit shit coin into some other

bridge that will then allow people to play video games that if they play for long enough, they make, you know, another type of shit coin that is then completely untradeable, but they can spend it in order to get on a different currency so that they can then reap the rewards of all their work. And then like maybe they can convert that into like a sub offshoot that of a theory.

Ryan Naraine (31:30.042)
Because...

JAGS (31:38.413)
that's been like broken in the tree. So half of the people believe in it. The other people think it's not real. But from that, you can exchange it to like real Ethereum and then you can stake it so that the money doesn't become real, but you get more magic money. then like, but you know, before you even get to sell it, like the price cratered because some idiot said something on television or like, dude, that's how this shit works. Like it's complete. like it.

Ryan Naraine (31:50.352)
That's how you end up in prison.

Ryan Naraine (31:58.801)
Question, how high is he?

Ryan Naraine (32:03.536)
It's true.

COSTIN (32:04.928)
Look, this is a lifestyle. I know people, mean, I tell you, I got into kind of blockchain forensics and investigation late because I had friends and colleagues back at work who were into Ethereum when Ethereum was, I don't know, $20 a piece. And I was like, how do you have time? How do you have time to

to stay all the time, stay connected, see what's happening, read and try to understand all these new solutions and new algorithms and new ideas and bots and trading bots and so on. And it's a lifestyle, it's a job per se, if you want. Absolutely. I mean, look, even the president of Argentina got involved into this whole...

Ryan Naraine (32:49.626)
Crypto Bro don't come easy bro.

Ryan Naraine (32:56.701)
Yes, tell me what happened there. I saw something about like some rug pull.

COSTIN (33:01.422)
So he actually pitched one of these meme coins called Libra and I don't know if he had any kind of stakes in it or he just wanted to do a favor to someone or he just thought that it's cute or whatever but he did say like yeah this is cool and people started buying it and the owners of that they just did a rug pull and

Ryan Naraine (33:21.392)
He wants to be Bukalili.

COSTIN (33:29.354)
everyone lost their money and now he's under investigation in his own country. The president is under investigation for this fraud because essentially it's when you do a rock pull it's fraud. You defraud all your investors that's what it is. And yeah it's not just you and me or our colleagues but as the president of Argentina I the president of the United States has his own meme coins and yeah.

non-meme coins if you want and this is it like that's how it is nowadays and either all this thing will be banned or it will explode and be the end of civilization

Ryan Naraine (34:13.456)
Costin, you had mentioned the Roninbridge hack, the coin check hack of 2018, which was 530 million, Mount Gox hack, 470 million, this one, right? These are significant events, but what happens is they just kind of just get lost in the wayside, another one gone and

COSTIN (34:17.365)
Mm-hmm.

JAGS (34:22.777)
Holy fuck.

I forgot, mouncocks.

Ryan Naraine (34:34.65)
the dust. this what we're seeing here or do you think this one big 1.46 billion number of course it's going to be on the front page of every newspaper and it's going to be on CNN and mainstream media is going to be running with this big giant. There may be movies about it but is it just going to be another Mt. Gox run in coin check in the dustbin or do think this is going to trigger some sort of like what happens next? What happens next? mean the North Koreans are literally picking off

COSTIN (34:46.892)
In case there'll be movies about it. At some point they'll make movies.

COSTIN (35:00.066)

Yeah, so

Ryan Naraine (35:03.31)
doing this wealth transfer to fund, like you mentioned, a nuclear program. I mean, that's how the FBI is connecting these things. Like what happens next?

COSTIN (35:09.838)
So just for you to understand like this there's a kind of a catch here which is that in this world $1 billion is nothing so this cryptocurrency exchanges they swap like 30 billion every single day so I don't know the

JAGS (35:22.603)
inflation.

JAGS (35:28.185)
Okay, okay, but that's where you see it, dude. Like that's where it becomes clear. But it's not just the lifestyle. Like look, a billion, I know that we're all doing quite well here, but a billion isn't pocket change to anybody on this podcast or listening to this podcast. All 50, no, no, no, not on this planet, just on this podcast. Like a billion is not pocket change to just about anybody.

Ryan Naraine (35:32.378)
That's the lifestyle.

Ryan Naraine (35:46.882)
on this planet.

COSTIN (35:47.66)
Wait, what?

Ryan Naraine (35:51.664)
You

JAGS (35:55.065)
It is pocket changed to very specific types of organizations and they are the kinds of organizations that in the past have rushed to not just exploit but also create dark markets in order to be able to take advantage of arbitrage techniques like high frequency trading.

When I say that I'm very curious at the fact that like you join any, like you hack into any bullshit DeFi bridge project with four people in it and a discord and you find $5 billion sitting around, I don't like, that is not, they might claim that that is wide adoption, but it's not really wide adoption.

It's not like the people's money put together to look like a bustling economy. I mean, let's keep in mind that there are not really day to day economies being fueled by any of this shit. So what the

fuck are the investment bankers, the hedge funds, like the high frequency traders doing right now in these places where they're not being watched?

with these arbitrage opportunities that are like almost like so multi-dimensional as to be of an impossible complexity to fully understand, right? Like it's chains of things that connect currencies that are traded in different chains that can be bridged between different types of currencies at different times that can be withdrawn or contributed to for a bunch of like random.

exchanges and different countries with no clear regulatory framework, especially not across the board. The dimensions of opportunities there are for arbitrage are insane, which means there's like a mania of like ridiculous wealth generation that's happening inside of this black box of cryptocurrency bullshit. And like we're talking about heists, but like

JAGS (38:09.273)
If someone was regularly withdrawing $3 billion from the local economy and never bringing it back, you would feel that in a real economy. the fact that whomever is putting this money into these places doesn't seem to be feeling the effect of its loss is like a fascinating symptom of some bizarre

Ryan Naraine (38:20.336)
Okay, in a short order,

JAGS (38:39.057)
sickness in a market that we're going to get out of like a who's that who's the Michael whatever that writes the like financial books like the Big Short Michael it's going to be a Michael Lewis book at any fucking minute but like just think about someone is having a couple of billions stolen from them regularly and they're not missing a beat you're not hearing about

Ryan Naraine (38:47.696)
Michael Lewis,

JAGS (39:06.507)
like hedge funds filing bankruptcies or anything like that. So there is some serious bullshit, like mega scale bullshit happening in this space.

Ryan Naraine (39:17.136)
Bustin, we're wrong though, right? Because it's not bullshit.

COSTIN (39:21.154)
Look, all money are just numbers on paper, that's it. Like, besides gold, all the money are just virtual. So a lot of, I think, of the wealth in this sphere is virtual. In theory, the virtual wealth is directly proportional to the demand. So let's say the more people somehow hear about these things.

Even this story alone by itself, it will create more wealth than the billion and a half that was stolen, in my opinion. Because more people will hear about it. Everything will be fine. Long term, there's no such thing as bad publicity. There'll be a... Well, the stock market is a Ponzi scheme. Everything is a Ponzi scheme, if you want. I know, I know. Mr. America, I know, I know.

Ryan Naraine (39:59.249)
So that's the definition of a Ponzi scheme.

JAGS (40:07.193)
Bye!

Ryan Naraine (40:09.316)
You

JAGS (40:09.785)
Uhhhh

COSTIN (40:13.998)
But look, the stock market is the same thing. In my opinion, it's the same thing as the stock market. They said the stock market is maybe more regulation and more taxes.

Ryan Naraine (40:25.379)
You

JAGS (40:26.041)
Look, the whole point of the market and the reason that regulation is generally welcomed or used to be welcomed in the stock market is that the whole point of it is that you like all these gambling addicts can come and speculate as much as they want, but the scales are fair, quote unquote, right? Like more or less fair. Like it's not so rigged.

that it's impossible for one of us mere mortals to like, you know, put in, you know, one of us in theory could bet, you know, put our last $10,000 on some, some bullshit company. And the next day you find out that you are now like a hundred millionaire and you withdraw at the right time and your life has changed. Like that is possible because

Ryan Naraine (40:56.208)
Listen to yourself.

COSTIN (40:57.283)
Hehehe.

Ryan Naraine (41:07.807)
some Nvidia shares.

JAGS (41:20.569)
There is such a thing as like, no, no, no, no, no, no, that is not a Ponzi scheme. That is a space where you can.

COSTIN (41:20.718)
That's a ponzi scheme. Yes it is.

COSTIN (41:26.971)
You know how that works? At some point the market will crash, everything will like burn in fire, there'll be a reset. Yeah, and the cycle starts again.

Ryan Naraine (41:32.139)
Reset

you

JAGS (41:36.505)
But what you're talking about is like not all wealth redistribution is a Ponzi scheme a Ponzi scheme is a very specific type of wealth redistribution that That's it's pons. It's a Ponzi scheme with health care. No, no, I I'm dead serious like there is an important difference here because even from an economics perspective, right the more we decouple

Ryan Naraine (41:46.384)
That's socialism.

COSTIN (41:48.27)
You

JAGS (42:04.353)
Like the wealth that has been generated over the past 20 years in like stratospheric, insane, unforeseeable numbers has come from the creation of financial instruments that are kind of bullshit, like, or largely bullshit or almost entirely bullshit.

But it's like CDOs and tranches of this kind of stuff, like all the stuff in the big short, right? Like all the things in 2008 that like caused a global collapse out of like, no, no, my point here is at least that was tied to some physical indicators, like some real world economic indicators of like success or failure. Like it was reverberating.

Ryan Naraine (42:36.142)
You're making Kostin's point in all of this.

JAGS (42:57.425)

in parts of the economy that you could see and touch and feel. Right now, it's like there's a war in Mount Olympus. And like the trillionaires are slinging mud at each other. And like, we can't even see what's happening because it's not immediately tied to like...

people's ability to buy apartments or stay in their homes or buy eggs or whatever the fuck it is we're into these days. But that also means that when, you let these people go to critical mass, which is what they do every time, right? Like we have like some mega financial cataclysm every like 40 years or something, 30 years. I'm curious what it'll look like to have, when they talk about the

quote unquote crypto bubble bursting. I want to know what happens when you have like a trillion dollars of institutional wealth that by some technicality fluke or whatever gets like shunted entirely in one direction and the whole ship fucking capsizes sideways without having any fucking idea of what just happened.

Ryan Naraine (44:13.038)
But this crypto world isn't going away. In fact, it's getting wider and wider more accepted here. US government embracing it. So I mean, I feel like we. Yeah, we need to get our we need to get our education up and have Mr. Costin continue to do some of these classes for us.

JAGS (44:20.067)
That's what should be scary about it.

COSTIN (44:28.536)
Look, I don't pretend that I know what's going on and I'm definitely not an expert in this field, but for me it's incredibly interesting. It's super.

Ryan Naraine (44:36.58)
and don't have wallets or coins sitting around anywhere. Make it very clear please that you don't have like a...

COSTIN (44:42.67)
I have, but like with some modest amounts, like I said, we were playing like we have a group of people who just we try to learn more. We try to understand more and friends of ours, they're like developing their own blockchains if you want. And we put like, I don't know, I put like a hundred dollars. I asked you if you want to put a hundred dollars just for fun to understand how it works. If you lose it, you lose it. Like it's a stake in Chicago, right?

And if you don't lose it, then you'll learn maybe something new, how that whole staking works in the blockchain, not in Chicago, and how to know a bit more about when the whole market will collapse. Because I mean, eventually it will collapse for sure. There'll be a default, the same as when a country defaults, it will happen. Things will get reset and you start from zero. If you ask me at the moment,

One thing which worries me a lot is the US national debt which keeps growing and growing and I don't think that we're gonna see a default pretty pretty soon on this topic but I think the potential for inflation is there and I don't like I don't have like a lot of investments into cryptocurrencies but bonds and stocks you guys seem pretty worried to me.

Ryan Naraine (46:08.292)
Let me change the subject before you bomb out the audience. He's bombing out the audience. are just clicking out to this podcast, being like, I don't need to listen to this. Bomber shit. Juanito, you're a district con. We're late publishing this podcast because you are a district con. One of the things I looked at the agenda, it looks like an amazing, pretty packed agenda. But something that popped out, obviously for me and for the people on this podcast that we love is this iOS Ode.

JAGS (46:09.89)
Ha

Everyone's checking their 401ks right now and shit like... Yeah, this is a bum-fucking bummer, bro.

JAGS (46:27.523)
Yeah.

Ryan Naraine (46:38.032)
And there was Bill Marsak from Citizen Lab and a Microsoft researcher, Christine Fosat-Chika. Is that how he's heard him? Discussing Quadream. Did you catch the talk? Can you give the people a live report from this? What? This is the reason we're late.

JAGS (46:53.537)
No, no, can't give I cannot give anybody anything. I I can't give you guys shit. like and I I know we delayed the podcast because of this. Look, man, I tried. I got dressed. I woke up early. I got my coffee. I made it there. I'm dead. There are pictures. There are there's proof. I saw Dave Vitell. He's one of our 50 listeners. Dave Vitell saw me.

COSTIN (47:00.898)
That's why we sent you there.

Ryan Naraine (47:05.392)
What happened?

Ryan Naraine (47:10.032)
Gusted that we believe him.

COSTIN (47:14.126)
I have the image in my mind, Juan waking up, dressing up, putting up the fancy shoes.

Ryan Naraine (47:19.908)
Go ahead, go ahead.

JAGS (47:22.477)
The shoes were fancy. And I get there and everyone's just standing around the lobby in the dark. like the entire, the power for the entire city block had gone out. like super unfortunate and like this had happened like the night before and they were reassuring the organizers that no, no, it's gonna come back by.

You know, by 9 a.m. the next day, it's like one o'clock in the afternoon, there's still no power. So the power did not return until about an hour before or like around when the conference ended, suspiciously enough, like on the second day, like at the end, end, end of the conference. It, which was a shame. It.

Ryan Naraine (48:09.476)
Doesn't this happen at Cyberwarcon every year as well?

JAGS (48:12.355)
DC is a cursed city for conferences. don't know what it is, but yeah, cyber war con, cyber war cut. think someone said they saw John Holquist with a fake mustache and a pair of pliers just running around the hotel. No. Well, the, what ended up happening, mean, to the organizers and to the speakers and every, and all the participants like.

Ryan Naraine (48:17.604)
You sure it's not sabotage? Conspiracy Ryan is asking.

Ryan Naraine (48:23.699)
Hehehehe

Ryan Naraine (48:29.488)
So what happened? The conference started late?

JAGS (48:38.709)
Eventually, it definitely delayed the con, like almost, I want to say like an hour and a half for two hours. But eventually they started doing the talks in like a stuffy cramped underground room with no AC and like one projector and like a battery pack and like, it was just like scrappy as all hell, which is awesome. Like it's great that they do it. like, mean, I can't imagine General Nakasone giving a talk.

In the dark, you know with a flashlight like it's like a goosebump story But I'm afraid I ended up missing I'm ended up missing basically all the talks I'm right now ripping the live stream off the internet so that I can watch it on the plane

Ryan Naraine (49:21.818)
So it is on YouTube, there is a live stream available on YouTube. Is it open to everyone?

JAGS (49:26.157)
I mean, it's on YouTube. It was open. I'm guessing there's people at home that watched more of the talks than I did being there. At the same time, it's it's raw feed and it doesn't look like it's all of it. So, you know, it's whatever we can scrap from it. But there were some amazing looking talks. like I'm like the one that I was excited about was actually Hal Vars closing keynote, like lock note for the first day. And yeah, yeah.

Ryan Naraine (49:52.696)
memory safety stuff. saw him post his slides here.

JAGS (49:55.833)
And I look what I'll say about this just to, I don't want to make this Rincon sound like a failure at all. It actually wasn't like a really nice conference, like a really good vibe. No one was upset. Everybody was, yeah, there were, there must've been a couple hundred folks. And, but everyone was like having good conversations, super good natured.

Ryan Naraine (50:11.44)
Big? How big? 200, 300 people?

JAGS (50:21.699)
people trying to help other folks that are like in the federal government and just lost their job or they're about like they feel like they're about to lose their jobs. So a lot of like comradery. And then I did get to participate on day two in they had an AI policy round table and it was off the record, know, Chatham house stuff. Dude, honestly, I normally would have expected it to be extremely shitty because

Ryan Naraine (50:39.77)
Sounds super exciting.

JAGS (50:47.703)
when you have something like that where you're like, don't know who these 20, 30 people in the room are going to be, the conversation tends to, well, it was actually nice because somebody handpicked the people. So what you had were like congressional staffers and like people from big companies that actually like had a vest. Like I learned a lot about some like open source initiatives and stuff in the EU that I didn't know about. And like we were genuinely, it was a good conversation. You had Halvar.

Ryan Naraine (50:52.368)
Go ahead, pitch me why this was exciting.

JAGS (51:16.503)

You had Will Pierce from Dreadnode and like Martin Wendigensen, just, you know, folks that I'm already like very familiar with, but like we weren't even the most active participants in the tables. It was actually really insightful and it kind of threw me into writing a paper about this whole AI thing. I'm in the process of editing it. Like I really, I left that.

For the first time in a long time, I left that AI policy roundtable and I crossed the street to a coffee shop and I sat down with my laptop for an hour and a half and tried to bang something out just so that I wouldn't lose the thread of the things that I've been thinking about during that. So I found it a very rewarding conference despite the power outage.

Ryan Naraine (52:03.546)
we have a crypto correspondent and we'll have an AI correspondent and cost you a while.

JAGS (52:07.629)
What's your thing, bro? What's your niche?

COSTIN (52:08.174)
My question was how was the karaoke? That's why you went to DC, right?

JAGS (52:12.185)
I would never, I wouldn't be caught dead. I have this, in Spanish we say.

COSTIN (52:17.55)
to tell you a secret, Juan is like the master of karaoke. He's fantastic, especially in Spanish.

JAGS (52:22.937)
Fuck you guys. Fuck you guys. In Spanish we say pena ajena. can have vicarious embarrassment. Which I think is what the kids call cringe these days. My sense of vicarious embarrassment is extremely delicate. I can't watch people sing. I can't watch singing shows. You're not gonna catch me dead at this karaoke.

COSTIN (52:30.786)
Painter?

COSTIN (52:39.598)
Mm.

Ryan Naraine (52:49.68)
You had one job at District Con my friend. had one job. Mr. Costian. While Mr. Juan was missing talks at District Con, we heard from Apple. We heard from Apple in a direct follow up to something we discussed in detail. was the top story in episode 33 of our show, which was this Joe Men scoop. The leak out of Apple that the UK government was demanding.

JAGS (52:53.975)

Hahaha!

COSTIN (52:56.224)
Ice cream?

JAGS (52:57.75)
I s-

COSTIN (53:04.324)
no.

Ryan Naraine (53:17.024)
access to iCloud encrypted backups in a of a virtual backdoor. Apple announced just this week, I think it was on Friday, that they can no longer offer this advanced data protection in the United Kingdom to new users and current UK users will eventually need to disable this security feature. Something we predicted that this was the only obvious move for them. What does this mean? Does this help level set that this it's

COSTIN (53:18.69)
Big door.

Ryan Naraine (53:45.218)
only affects people in the UK, is there a risk that this filters out and affects the rest of us?

COSTIN (53:51.15)
Well, first of all, I saw there's a lot of people, you know, hating Apple for this. I say, Apple is evil. And look what they're doing. Like to me, this is like amazing. In my opinion, Apple did an amazing thing here because, well, basically they refused to build a back door in a silent manner that would give

Ryan Naraine (54:00.666)
They had no choice, right?

COSTIN (54:16.43)
government access to your encrypted data. That would have been so much worse. And actually there's a lot of people who are asking the question, you know, to the void and there's no answer. Like what about Google? Like Google, is it encrypted? Like if it's encrypted, does the UK government have a backdoor to that? And there's no answer. So to me,

I think this is a huge success story in the sense that Apple refused to build a backdoor in the encryption. The encryption is solid. They prefer to disable it instead of just creating a backdoor. And the other thing which I think is a huge success story is that this means that encryption works. Like if you use encryption, it really works. You are protected. People who want to get access to your data, they can't because the encryption is solid.

For Apple, this is like a double success story in my opinion, and it means that your data, which if it is encrypted with this advanced data protection technology, then it means that it is much safer than other solutions. I think I saw, I apologize if I'm mistaken, was JD Vance saying that this could have been the case in the United States as well.

So I wouldn't be like so quick to rejoice from the geographical point of view. I'm afraid that now that this has been a success, kind of a success story in the UK, this may happen in other countries as well. What is I think also important here is that Apple said that we are gonna stop offering this to new users and in time.

Existing users who have it enabled will also have to disable it or we will disable it for them So my advice here would be if you don't have this enabled and you live in a free country then enable it That's probably the best advice try to enable this as soon as possible while it still lasts Because you never know what happens

JAGS (56:19.353)
Honestly, I loved the part where Apple has to come up with some way to help people turn off the... Well, but no, mean, like they couldn't just turn it off, which I think is really telling, right? Like they're saying like, hey, we're going to come up with some guidance for those of you that already had it on because we can't remotely undo this. And I think that too is an amazing, you know, it speaks...

Ryan Naraine (56:28.962)
security privacy.

COSTIN (56:46.03)
Fantastic.

JAGS (56:49.269)
assuming it's not all incredibly overblown theater, which I...

Ryan Naraine (56:53.37)
You can ship an update to turn that off. mean, they've shipped updates to turn things on and off. This Apple intelligence is now on, yeah. I don't know, I don't know.

JAGS (56:58.041)
I don't know. I don't know. No, no, I don't think that we can properly speak to that, right? Like the kind of stuff like that you see in Yvonne Christic's Black Hat Talk from a few years back, like that kind of architecture, they are at least, again, if they're doing what they say they're doing, which I honestly have no reason to believe that they aren't, they're putting a lot of engineering and like extremely sophisticated mental power.

Ryan Naraine (57:03.629)

Agree, agree.

JAGS (57:27.423)
into taking those abilities away from themselves. And that's the only way you will never be compelled is if you literally have, do not have the power to do so. the fact that Apple spends so much money and time and energy trying to do that is something that like, there's a reason they are the fucking like luxury brand for security. That is what you want. If you are wealthy living in the first world,

you should have Apple devices for the sake of that security, at least iOS devices. So like, you do have to give them that credit because they are putting the fucking work into it and Google, once again, shines by its absence.

Ryan Naraine (58:09.312)
And then that's where I wanted to flag right here, conspiracy cost in flagged it right at the top there, which is a piece in Joe Men's story. I'll read a paragraph from Joe Men's original story on the UK officials demanding this backdoor. It says Google would be a bigger target for UK officials because it has made the backups for Android encrypted by default since 2018. Google spokesman Ed Fernandez declined to say whether any government had sought the backdoor, but implied none had been implemented.

Google can't access Android end-to-end encrypted backup data even with the legal order. We haven't heard from Google still through all of this. What do we think has happened there? The UK government just miraculously doesn't know that Google do this? Or there's something happening there that we haven't learned?

COSTIN (58:51.246)
Yeah, but the language, the language there says Google, even Google cannot access, but they are not saying that whatever government cannot access. So maybe this can be built in a manner that whatever government can, but Google cannot. So always when it comes to this kind of press releases, I think the language is super, super important. And that's how you you cut through all the bullshit and you understand what's happening when you're very careful about what you're saying.

JAGS (59:13.911)
yeah.

Ryan Naraine (59:16.26)
You have to parse it,

COSTIN (59:21.562)
And like, let's say when you ask, did the UK government ask you to build a similar backdoor and you answer that my company cannot access the data. I mean, that's, think an interesting observation. No.

JAGS (59:32.665)
Because it's not an answer, right? It's not an answer because it's a pivot to this is our comfortable and extremely legally vetted language for answering this. And like we've all done media training before, right? Everyone here has done media training at some point. It's all, you you stay on message, you deliver it your way. You wanna make sure the sound bite, the clip is exactly what you were meant to be saying.

Ryan Naraine (59:34.308)
Yeah. It's the pivot,

COSTIN (59:47.022)
Of course.

JAGS (59:59.359)
you don't let them steer you. ask you like, so what's the weather like in Berlin? And you go, our product is the fastest, bestest way to do whatever. And they go, so what are you wearing today? You go, our product is the bestest, fastest thing, whatever.

COSTIN (01:00:14.926)
Or like what was that with the drones in New Jersey? then the answer comes. That was all authorized research the drones were doing. And like everyone's, if it's authorized, it's fine. And everyone else is like, wait, what kind of research? What kind of research were they doing? There were like thousands of them doing what research?

JAGS (01:00:31.545)
Okay

Ryan Naraine (01:00:32.365)
It's a...

JAGS (01:00:35.469)
Yeah, what the fuck are you guys doing?

Is that the end of the, is that what that story came down to? I, I, I'm telling you, man, I, have figured out how to like somehow stay away from, yeah, just let all this shit just pass right. And like, I'm ducking and every once in a while, like I, catch myself slipping. I catch a stray and I'm like, wait, what did they do? And I'm like, no, no, stop, stop it. It's just fucking pretend it's, it's not happening.

Ryan Naraine (01:00:44.164)
Nobody knows.

Just let that shit pass over.

Ryan Naraine (01:00:55.962)
You gotcha straight.

COSTIN (01:01:03.874)
When did you have drones flying above your house doing research?

Ryan Naraine (01:01:03.952)
Let me get this train back on the tracks.

JAGS (01:01:05.89)
Yeah.

JAGS (01:01:10.455)
I mean, I'm not at a wedding, so I'm not that concerned. It's fine.

Ryan Naraine (01:01:15.62)
Let me get this train back on track. Two things, is this something that people in the UK should worry about only? Does this affect the rest of us? Are you expecting cost in another European nation, an Asian nation, somewhere else to say, turn it off for us too.

COSTIN (01:01:31.48)
Look, I was thinking if I'm in the UK and I still want to profit from this thing, can I just change my region to Ireland and pretend I'm Irish and get the encryption or is it like not very politically correct and like a totally no-no to do in the UK?

Ryan Naraine (01:01:45.848)
I don't know what you're saying.

JAGS (01:01:47.853)
Well, it's not that easy to do, right? Like the, is notoriously rigid with stuff like that. Cause they tie your payment verification, your credit card, your whatever. like, you know, I'm not saying it's not doable, but like.

Ryan Naraine (01:02:03.12)
Do we expect circum, it's, do we expect circumvention to pop up at some point where people are able to keep it but not, you get a different back door that way.

COSTIN (01:02:09.592)
Can set your country to China?

JAGS (01:02:12.409)
No, I, this is not the kind of, so this is not the kind of product that you just like replace. Like this is the kind of thing that is a beautiful add-on to an ecosystem and only the ecosystem

maintainer is in a position to provide that, which is again, why I give Apple a lot of credit for the way that they do things because only they can do them for their people.

COSTIN (01:02:14.968)
You get different,

JAGS (01:02:38.713)
But no, I don't see this as something that you end up circumventing like you can go try to like come up with a bunch of like Crafty cool ways to protect yourself, but you cannot do the protecting That Apple is the only position party to do

Ryan Naraine (01:02:55.618)
Apple has made a point of promoting private cloud compute, this PCC thing for their Apple intelligence for the handoff of device computing. Do we expect that to also be in the crosshairs at some point in the future if that's where some of the magic computing happens for our AI searches and our AI interests? And Apple is building a system where that's kind of off limits and the security there is like a vault. I mean, it...

Should we connect those things at all? No?

JAGS (01:03:28.537)
No, well, again, it depends entirely on the implementation. that's, I'm sounding like a broken record today, but like, that's why you want to give Apple credit because I don't know what the implementation of TCC is going to be. And it's possible that they don't know what the implementation of TCC is going to be. I, yeah, sorry, PCC private cloud compute.

Ryan Naraine (01:03:48.708)
PCC

JAGS (01:03:56.855)
They may not know what the implementation to PCC is going to be just yet, but I would imagine it's in their greatest possible interest to genuinely make this thing semi-anonymized or ephemeral in some way, and they can't reach the data because the query itself is in an enclave. That kind of magical, ultra-high-end security engineering, the legit crypto analysts who didn't go work at the fort.

that that's the kind of thing we should be excited for. And I would expect Apple to do it. at the same time, there is a Faustian bargain that could be made there, which is Apple is winning on some capacity for like this whole hardware, that enables running language models locally. And they want to lean into that more.

But if Siri keeps sucking this much, if Apple intelligence keeps being this shitty, well, I'm wondering if there's gonna be like a desperation point where they kind of embrace that they do need to actually pay more attention to what the queries are and how they're being used and

what the responses are from OpenAI. And if there's a way for them to distill without distilling what OpenAI is doing so that they can improve their own like small

Ryan Naraine (01:04:58.02)
Nobody will care, hopefully.

JAGS (01:05:21.249)
models and stuff like that. There's definitely some incentives here that could get dicey if Apple starts to feel like they're somehow missing the boat on the AI revolution because their shit sucks. Their software is going to shit. I don't know what is happening to macOS and iOS, but the amount of little bugs, failures in notification stuff, AirPods de-stinking, dude.

Ryan Naraine (01:05:42.084)
Photos crashing, camera was crashing, everything, yeah.

JAGS (01:05:45.049)
Things are getting like reindexed by spotlight at random and certain like after certain OS updates and then getting stuck CPU is getting pegged over some stupid daemon I'm genuinely I genuinely believe they broke something in the Bluetooth stack about like three versions ago That's causing issues with all kinds of devices including their own like I don't know if you notice how many times your air pods like will crash and like reconnect

Something is wrong and these motherfuckers don't even have a ticketing system. So I don't know what, like I'll go on Twitter.

Ryan Naraine (01:06:18.832)
This is the same guy who just spent the last segment telling everyone to buy iPhones to protect themselves.

JAGS (01:06:25.813)
I do Apple goes through these periods where they're like software. It's like you can feel like it's almost like an afterthought like somebody rushed the software at the last minute.

Ryan Naraine (01:06:33.808)
Just buy more.

Ryan Naraine (01:06:37.562)
Buy the new version, it'll fix all of the old problems.

COSTIN (01:06:39.502)
I'm also a big Apple fan, you know me. The only thing which is kind of not okay in my book, you know, like in my book I have like different names like Juan, okay, Ryan, okay, Baldi, super okay, Apple, not okay. You know why? Because they...

Ryan Naraine (01:06:56.368)
Will he get super?

JAGS (01:06:58.721)
Not okay.

COSTIN (01:07:02.07)
I applied for a security researcher's device and they rejected me. They said like, I'm not good enough for the security device. Like I don't have enough zero days. I don't have like enough credentials to own one of those. I was, but I was not probably Apple's CRC top 100. And I was thinking like, you know,

Ryan Naraine (01:07:10.02)
You're not okay.

JAGS (01:07:10.147)
I don't know, bro.

JAGS (01:07:15.875)
Weren't you MSRC top 100 at some point? the end.

Ryan Naraine (01:07:26.256)
Let me.

COSTIN (01:07:28.558)
That's a very kind of short-sighted approach thinking that you give these devices to people who develop zero days I think they should give them to people who have the potential to uncover other kind of things security vulnerabilities so use them to fine-tune models for malware detection or make the operating system more resilient so You once it and yeah like in my book Apple not okay

Ryan Naraine (01:07:49.38)
Make your pitch, make your pitch, Ivan is listening.

JAGS (01:07:52.14)
If not.

JAGS (01:07:56.226)
Not okay.

Ryan Naraine (01:07:57.261)
Ivan, hook my guy up. Defenders can find these things too. I'm being serious. And I want to pivot very quickly too, and I don't want to spend too much time on it. Iverify, is an iOS app, they spun out a startup to...

sell an iOS app that enables the public to scan devices looking for advanced threats. We got a press release out of them saying that in May they launched the app and they found some Pegasus infections and then they had some media coverage and 18,000 new users scanned devices and uncovered 11 new Pegasus cases in December 2024 just a couple of months ago.

And their argument is that the infection rate is approximately 1.5 for every 1000 devices. Like, do any of us use iVerify? What is this iVerify? And do we trust this data at all cost?

COSTIN (01:08:50.36)
Well, look, mean, I verify they've been around for a while. think originally Dan Guido was one of the founders. Then he kind of separated it from Trail of Pits because maybe some people were questioning given the kind of offensive work that he's doing. Is it good for this application to be associated with someone doing that kind of work or not? Nevertheless, now it's an independent company. So I know actually a lot of people are

running iVerify. I have iVerify on some of my iPhones as well and I even I saw people who actually found things on their phones with iVerify. There was one guy on X that I saw recently, a Romanian guy who posted a screenshot of iVerify flagging something like public indicators of compromise have been found on the the device. So for sure it finds stuff. I don't know if it finds a

the really advanced things because of the architecture of the iOS or the inability of one sandbox application to scan others. But I think what it does is looking for signs kind of in TMP, private var TMP folders, or if the device is jailbroken, you can test for that. So looking for these kind of infection signs, which in my opinion,

There should be more applications doing that. It's not that difficult actually to do such an app. And I think in the past there were a few others, similar apps and one of them from Stefan Esler, if I'm not mistaken, was pulled out of the app store. They removed him from there for some reason. And now I verify I think it's a top app.

of this kind that allows you at least to do some checks of your device. And they also have another thing which is interesting, the more advanced checks when you first you need to trigger a SysDiag on the device and then you upload the SysDiag to them. So in the SysDiag there will be a lot more forensics evidence. And me personally, I do a SysDiag every couple of weeks. I save it in a backup. whenever

COSTIN (01:11:09.96)
I read about some new Quadrim style malware, I tried to look at all my previous czdox and backups to see if it was infected, which is something that I recommend to everyone. So yeah, would say they're a very serious company. I know they got into... It's true. This is Yeah. Where? Where? In which countries?

Ryan Naraine (01:11:28.176)

Yeah, but this is all marketing cost and there's no technical details. This is, there's, it's like we uncovered 11 new Pegasus cases and everyone should just believe this. Like where, what, where are the IOX? Why are we paying attention to this one? And two, two, they, do they have the capability to flag something that this was definitely Pegasus? Like, like, unless you can show your work, we are going by some marketing lines in a press release.

COSTIN (01:11:39.156)
Yeah, yeah, yeah, ehh...

COSTIN (01:11:47.32)
True. I fully agree. And also what attracted my attention here is they say that the new detections involved business executives. So this in my mind, at least it means that they know who those guys are. Yeah, they know who they are. So there's maybe a privacy implication here as well, if you want. Maybe they got in touch with them and they found out they were business executives.

Ryan Naraine (01:12:04.592)
who their users are.

COSTIN (01:12:16.574)
It's strange, it's unusual and I know I wanted to say they got into some kind of a fight with the Grafino S guys if I'm not mistaken over this hype There is a beef, yeah, there's drama. Always there is a drama. It doesn't matter what it is like chess, cryptocurrencies, secure. That's always a bit of drama

Ryan Naraine (01:12:28.154)
Who did I verify guys? There's beef.

JAGS (01:12:32.665)
I'm too anxious to breathe.

Ryan Naraine (01:12:39.982)
Yeah, I was tempted to just delete this press release because I thought you can come out and say, yeah, we saw 11 new Pegasus infections. It's a line in a press release. get a couple of news headlines, more people download it, more people scan and they see this thing that they could somehow maybe connect in a lab to Pegasus, but they're not showing their work. Like, how do we know that this is true?

COSTIN (01:12:42.797)
Mmm.

COSTIN (01:12:58.286)
I would be curious if they uncovered anything else besides Pegasus. I mean, Pegasus is like so 2023 if you want. What about the new things that have been in the news? Like graphite. What

about that thing? Do they have the capability to catch it? I think that unfortunately a sandboxed application can only do that much.

Probably they're missing a lot of infections. So they say the infection rate is 1.5 per 1000. Maybe if you add the other platforms out there, it's not just Pegasus obviously, but there's many others. I think the infection rate could very easily reach somewhere in the range of 1%. And to me, if Apple was listening like you suggested, I think that they should pay more attention to that.

Like I said before, how about having a remote SysLog? Very simple feature that has almost no impact on the device, the ability to redirect the SysLog to a remote device. And all those, these kinds of things, they can be leveraged for telemetry and for detection and it would help people to know if they were victims, if they were targeted and so on.

Ryan Naraine (01:14:15.024)
Why can't Apple do that? What's the big holdup? Is there some IP disclosure issue? Is there just, there's no malware on my platform? They're like, stop, you guys go away, look the other way. What is going on?

JAGS (01:14:28.049)
I think it's more of the latter. I think that there's definitely a sense in which they would rather not know a whole lot of things. Because there's... Well... I don't know. I don't know. And they've misused it every single time. Yeah, and that's part of the problem. That's why I'm saying that it kind of seems like it's more that they would rather not know.

Ryan Naraine (01:14:34.256)
They have a threat intel team that is capable and has this direct knowledge of what's going on though. I mean, we have shared information with these folks before.

They know it though, they're aware though, they're not dense.

JAGS (01:14:56.621)
does seem to me that they would rather not know the true scale of issues, the true, they don't seem to want to know the specifics about like the stories of the individual customers and why it's relevant to them that they're getting popped. And they also don't seem to want to know the overview of why, like the true scale of the issues in hand, right? Like this, verify thing, like obviously it's not going to be a,

a good sampling of all iOS devices, that's impossible for iVerify. It is not impossible for Apple at all, not even a little bit. So if iVerify, which is not getting a random sampling of iOS at all, it's people who are willing to try this. So clearly they seem to think something's wrong or somebody's trying to check their device or something. And you're still getting this like one in 1,000, one and a half, like one and a half iPhones and 1,000 iPhones infected.

That really, the reason that perspective is important is that what, that's what keeps people in Cupertino with this ability to wave away that this is not that big a deal. It's not that much of a problem. We're doing our best to like manage it, but this is still like a rounding error, a remainder of the problem that's like very, very small and not a big deal and don't worry about it. Like, and we're just gonna keep, yeah.

Ryan Naraine (01:16:22.006)
extremely targeted to specific individuals.

JAGS (01:16:25.067)
And they don't fucking matter at all. Don't worry about it, bro. Like there's something, you know, I do think, I do think that's a factor. And frankly, I was surprised that this Iverify thing could do anything at all because Apple has gone through extreme lengths to neuter the ability of any user land software and applications from doing any real forensics or any kind of evaluations or even any kind of like genuine like EDR.

on these devices as far as we can tell. And I mean, maybe the iVerify guys have something better because they do have like an MDM and EDR thing that we haven't tested. But it's important to note that the mechanism in this app is, we're going to create a crash dump of a SysDiagnose routine. And then you're going to follow along and click these four buttons. And that's going to upload this crash dump.

and we're gonna analyze it on the cloud and then let you know if you need to do more stuff. So like, it's not like this iOS app, like it's doing something special. It's just walking you through the only mechanism available to them. And I mean that, like, I don't think I verify it is lacking in the developers that could do this. Apple has made it impossible to do this.

So why the fuck aren't they, doing it themselves and B, providing a genuine sense of transparency as to the scale of macOS and iOS infections and their failures, shortcomings and implicit paternalistic decisions they've made on our behalf where they basically say that they're the ones that get to decide how safe we need to be and how much we need to know.

Ryan Naraine (01:18:13.2)
Alright, can we pivot quickly off of Apple? want to touch a couple of quick stories before we go. One is this, we got a new report out of Inversec OS. Li Nalao, known online on Twitter as Inversec OS, has a new report out on how the NSA, through the equation group, allegedly hacked into China's Polytechnical University.

We've spoken in the past about the absence of good data out of China in terms of their visibility Costing has made the point that this and this stuff is already happening. It's just probably not being shared publicly It might be she being shared privately there. Have you guys had a look at this report? What is the quality of the the reporting here? Costing what can you tell us?

COSTIN (01:18:58.318)

I was still thinking that you said inverse sec OS. I was thinking, could it be inverse cos? Like cosine? Like the function? The cosine? Inverse cosine? I don't know. So which is kind of a mathematical angle to the equation group. Which is the irony of that.

Ryan Naraine (01:19:07.17)
Inverse cost.

JAGS (01:19:10.9)
yeah, that would make sense.

Ryan Naraine (01:19:11.162)
possible.

Ryan Naraine (01:19:14.901)
I-N-V-E-R-S-E-C-O-S, yeah.

there you go.

COSTIN (01:19:22.51)
But I did look at the report. There's a hash by the way, like three hashes for the same thing. A very old second date implant sample shared by the shadow brokers. So like nothing new, unfortunately. I was reading through the report and like there were some points in there for which I was thinking like, where did this come from? Like there's some new information in there.

which I personally, can't immediately source it. Like which one of these many, like many Chinese reports. So for instance, they say they're like the, NSA uses some front companies, like, and it gives the name of those companies. And then it gives the name of somebody working in one of those companies. And I was thinking that where did that come from? I don't think I remember seeing it. Maybe I am just wrong here. Maybe somebody who.

Ryan Naraine (01:19:55.92)
Give me an example.

COSTIN (01:20:18.094)
listens to us can find the original report where the names of those companies are mentioned. So, I don't know if you...

JAGS (01:20:25.529)
I remember the company names were from the same one where they figure out Rob Joyce worked at the NSA. I think that was the one.

COSTIN (01:20:35.374)
So like the Jackson Smith Consultants and the Mueller Diversified System. And Amanda Ramirez. Who is Amanda Ramirez? who is that? Interesting.

Ryan Naraine (01:20:48.42)
He's just messing with us.

JAGS (01:20:49.559)
This man is just fucking like trying to light fires left and right.

JAGS (01:20:56.521)
I remember seeing some of that stuff. It was definitely out. You remember the, there was a report, was like a couple of years ago, I wanna say. I'm pretty sure it's the same one where, like I said, they figured out that Rob Joyce worked there, but maybe I'm wrong. But I definitely remember looking into the Jackson Smith Consultants and Mueller Diversified Systems.

And like we talked about some of it around some of the anonymizer infrastructure that equation group used back in the day and like servers in Columbia and like all this stuff. Like some of it.

Ryan Naraine (01:21:28.602)
What did we learn from this report? This new report here, did we learn anything new?

COSTIN (01:21:32.728)
Well, like immediately what I learned and like this is not immediately obvious is that it's a mix of things that have happened over many years. So if you want, this is not for many different sources and not necessarily new, not something that happened yesterday. So, I mean, one of the top incidents they talk about here is something which allegedly happened two years ago, I think. And well, three years, 2022.

Ryan Naraine (01:21:44.528)
from many different sources.

COSTIN (01:22:02.318)
And if you want, it's not necessarily a report about some new discovery, but more like going through all these different reports that got published during the last years, extracting some of the beats, putting them all together and kind of extrapolating the methodology, the tool sets, the names of these things from different reports and their activity times, putting it into one single source.

And this

Ryan Naraine (01:22:33.338)
This university was a known victim of... or that's also new.

COSTIN (01:22:37.834)
So well, like the Chinese every now and then they put out like these small things, small alerts with no details except that we caught the Americans in our networks and they are evil and they

were stealing stuff. So it's not just us stealing stuff, but we are not actually stealing stuff. But it's not just us. It's the Americans as well for the record. So they do this from time to time. And when they do it, like there's no proof. Typically, they don't

publish any proof, any IOX, any TTPs in detail but then like some report comes from one of the companies like for instance Pango when they published about this BVP 47 toolset or Chi An Shin I think it may be yeah right correct

JAGS (01:23:24.567)
Is that the best report? think that may be out of all of them. I think the VVP 47 is the best one.

COSTIN (01:23:30.958)
from Pangu Labs, which by the way is intrinsically connected to some of other stories that maybe we have time to talk about. But like, if again, to summarize what's new in here and what was new for me is that someone and props for that went through all these Chinese bits and pieces that got published during the last years extracted the most interesting details sometimes

JAGS (01:23:37.817)
Maybe.

COSTIN (01:23:59.564)
translating the Chinese with maybe more than just tools. Perhaps she can actually understand Chinese Mandarin natively and that allowed the extraction of more information than usual. That's my... I would say it's interesting to read. Yeah, for some of the code names, I mean, some are like super well known.

Ryan Naraine (01:24:16.506)
You recommended folks read this report?

COSTIN (01:24:26.382)
As I was looking actually a bit just to see what's been published so for this particular Implant that they mentioned I realized that nobody has actually done a thorough analysis of what was in the the first shadow brokers dump So the first one was the strangest because it was mostly router tools and router malware So very few people actually had the knowledge to to look

at those and understand how they work, what they are, ROM images, flash tools and so on. And I think, I would recommend taking a look for sure. hope that she or they do even a follow up on this, because I suspect that there'll be an increase in the amount of public threat intelligence from these Chinese companies. Like I was saying last year.

It's good to keep an eye just to understand the capabilities of Chinese retinal companies. A lot is known about the West, but very little is known about their capabilities.

Ryan Naraine (01:25:32.56)

Want it all? Closing thoughts on this paper?

JAGS (01:25:37.825)
I'm surprised at how many people have like kind of brought it up to me and like were commenting on it because

Ryan Naraine (01:25:43.92)
Come on NSA equation group talking into China, we're hearing some words from Chinese side, of course it'll make you raise your eyebrows.

JAGS (01:25:48.205)
Well...

It also made me realize how little some folks have engaged with the existing equation group literature because to me this felt like, and I'm not putting the researcher down at all. This is like, I like the write-up. I enjoyed it. I read it twice. No disrespect whatsoever. No, seriously, no disrespect whatsoever. it definitely feels like kind of like a big

Ryan Naraine (01:26:09.776)
No disrespect, here it comes. Okay.

JAGS (01:26:19.841)
like a book report sort of summarizing like this is what's being claimed in these different places. And as such, it works well because we had all seen these pieces, like these reports when they came out at some point. Yeah, but you don't really kind of like put it together and really sort of suss out like what's going on. At the same time, I think that a lot of people sat out

Ryan Naraine (01:26:34.456)
in various pockets somewhere,

JAGS (01:26:47.029)
really engaging with the equation group findings when they happened and the same thing happened with the shadow broker stuff. And if we are cured of this fucking fever of like over classification and like, and acting, well, I say sat out for a good fucking reason. The clearance stuff was like over convenient, like bullshit.

Ryan Naraine (01:27:00.58)
That's what you mean by sat out, they couldn't look at it because of clearance issues and stuff?

JAGS (01:27:13.513)
And I don't think that people should give themselves that much of an excuse or a pass for ignorance because that's what it really turned into. And that's what we're talking about now. Like, I mean, I agree, but it was like an excuse for ignorance. And if it's fine, fine, fine. It's been like.

Ryan Naraine (01:27:21.53)
That's laziness though.

JAGS (01:27:35.961)
10 years?

Ryan Naraine (01:27:37.904)
There's a lot still to revisit there, right?

COSTIN (01:27:38.181)
yeah, 10 years, correct.

JAGS (01:27:39.019)
It's been 10 years. Do yourself a favor. Go through all that stuff in Notebook LM. Have like a nice weekend and like realize how much stuff is out there, how much you haven't understood about your own intelligence machinery and how much your adversaries have understood about your intelligence machinery while you were fucking burying your head in the sand just to like, you know, for cutesy poly screening bullshit. But I say that again because this is making me realize that to the point where

We've been discussing internally like, well, you what should we do with the podcast? Right? Like, do we really just want to keep doing the news? There's things that people appreciate. And it, I immediately was like, you know what guys, like we need to do some like deep dive on all the equation research that we've like, that we worked on before sort of like the, the, yeah. How do we get here? What happened? You remember that story? Like all this private research that never really got shared beyond.

Ryan Naraine (01:28:25.626)
Yeah, like the trails that ended up that didn't, yeah, that didn't.

JAGS (01:28:36.631)
Like we worked a lot, like I jumped later on. I wasn't there for the discovery of things proper beyond like seeing that this was coming and like getting to live tweet it. like the, but then got to work on like subsequent components that I now realize have never been discussed publicly. We worked on the triage of like the shadow broker stuff in the very beginning.

right, actually, and wrote that blog about like, hey, like this, here's the inverse, like crypto constant that keeps connecting things from shadow brokers back to equation group. And like had arguments with academics at the time who said that that wasn't, that couldn't be accurate because they've never had to hunt anything for themselves. And then all of that was so present in my world, because like that led to WannaCry, that led to NotPetya, that like, was an insane period of time.

And I'm now looking back at this and being like, fuck, I don't think, I think a lot of people really, like to us it was this action movie that was all consuming. And then I look even in circles out here and I'm like, I think these people have never heard these fucking stories. So I do think if there's a big takeaway from this is I think this Inverse Cause blog, I hope, basically makes it palatable and desirable for us to.

Ryan Naraine (01:29:42.608)
Yeah.

Ryan Naraine (01:29:56.891)
just go revisit some of the loose ends.

JAGS (01:29:58.195)
just revisit that, at least as the first thing that we revisit.

Ryan Naraine (01:30:02.938)
You guys mentioned Pangu team in the earlier segment. I want to pivot quickly to a new report out of our friend, Yohinu Beninkasa. He spoke at LabsCon this year. A new report out connecting. he was out there.

JAGS (01:30:13.613)
He was here for district con man. was on the China like jump the wall event and came to dinner with us last night. He's a good dude.

COSTIN (01:30:15.948)
Mmm.

Ryan Naraine (01:30:21.38)
He's got a paper out saying the Pangu team, a prominent Chinese white hat group known for developing iOS jailbreaking tools has been linked to iSoon, the company involved in espionage attacks and activities for Chinese government leaks. So we've known about these iSoon leaks. I think we discussed it on a previous episode. He is connecting the leadership of Pangu team to the iSoon folks. What is the implication here, Costin?

COSTIN (01:30:46.882)
Well, what attracted my attention, by the way, back in the days when Pango released that report that we were talking about the BVP 47 report, which by the way, it was something atypical for them because if you look, I think that's maybe the only or maybe one of the very few reports they ever released. So there must have been some reason why they released that particular one. And I would

probably expect them to have more reports on that side. Now, what I was thinking here is that, of course, Pango, they've been super famous for many, years for these jail breaks and obviously

very skilled people in exploit development. And it makes sense for someone like that to get together at some point to find a way to monetize their skills and their expertise with the iOS.

jail breaks and exploitation. So to me, it makes sense. We know that the Chinese have a huge ecosystem of companies and trust relationships and cooperation based on personal relationships, which is very important there in the culture. You know, we're going to work with friends and the friends are going to work with their friends. And in the end, like we are all in a kind of a trust circle.

So there's a lot of cooperation like that happening and it makes, if you want, it makes sense for the skilled people to be engaged in a bit more than just jailbreaking. Now, if you ask me, I think that the same situation probably true for Western companies. There's a lot of money to be made in this field of exploit development. Even nowadays, I think people still need

iOS exploits, Android exploits and mobile phone exploits in general and if you ask me specifically about the implications here, I think it kind of confirms, it serves as a confirmation about these cooperations that are going on and yeah, you would expect these renowned hackers who won hacking competitions like PwnFest, the TianFu Cup

COSTIN (01:33:12.472)
to be somehow connected to this world.

Ryan Naraine (01:33:15.192)
Is the connection that Eugene is making solid enough?

JAGS (01:33:19.597)
yeah, I I trust Eugenio. We've discussed some of the reporting that he and Dakota Carey have put together, some of the talks they've done before. They're doing excellent work. So I have no reason to doubt the connection, more so considering that it seems to be further gains from analyzing this ISUN leak. So this is going to come out. What I think is

Ryan Naraine (01:33:40.784)
you

JAGS (01:33:46.935)
I think it's kind of interesting to consider how differently we take these glimpses, how differently we take them from the way our European counterparts might see it versus the way that I hear it discussed in the US. I think for the Europeans and the folks that are sort of used to watching this, doing intelligence a little bit.

more sanely, this is kind of like a discussion of the particulars, right? Like, it's like, hey, this particular company with these individuals and that particular company with those individuals, we can now document have been working together in this and that way. And there may be

interesting ramifications of that if you go back to this and that. Yeah. Yeah. At this, you know, at this time and in this way.

Ryan Naraine (01:34:38.81)
they were having these very specific discussions around vulnerability acquisition. Like you can actually see it in the.

JAGS (01:34:46.649)
But the discussion that I've gotten around this in the US is a lot more kind of like this marveling, ooh, of like, we can see behind this veil to what our enemies, our adversaries look like. you're like, they have big companies talk to each other and they sell each other stuff and they...

Ryan Naraine (01:35:12.25)
Same things we do here.

JAGS (01:35:14.499)
But like, in a way, same things we do it in a way, no. Like that's honestly it. It's like, think we are, we have this like, we've developed this like weird alien mechanism for how things work in the US. Like in Five Eyes, but more than anything in the US. Cause like when you say the same thing happens in the US, I don't know, man. I don't know that Raytheon and like booze.

like have emails back and forth about like the girls in the research team next door and like because it's like two mega fucking trillion dollar corporations that are doing it here and that comes with all the red tape and all the bullshit that comes along with that and over there it's like a couple of companies of skilled people that have been doing this for several years. Those exist here too, right? Like for sure, but

Ryan Naraine (01:36:05.136)
Do you want to tell me you can't find the equivalent of an ice soon and a pangu team here in the US? Doing this kind of collaboration.

JAGS (01:36:13.353)
I don't want to answer flippantly. I think we could find similar organizations, like similar companies within certain aspects of it. But I don't think you up until now, maybe by the time this podcast is released, it will be different. But up until now, you didn't really have, you don't really get to have the like

cowboy do everything companies. They hack, they source, they do the vulnerability research, they decide who they go after, they share stuff with each other, they call each other up, hey bro, I was doing this for these guys. No, we're not in the skiff, right? This isn't some insane fucking over-bureaucratized process. You're just shooting an email, like, hey man, they would love a vuln for this thing. I guess they're going after those gamblers, ha ha. That's not happening here.

in that way, but also I don't think that that's necessarily a good thing for us. Like we have put 17 layers of bureaucracy and 4,000 pages of paperwork in the middle of every operation, every component, every team that does one thing and analyzes another to the point where like when we watch other people do it in the most

common sense way that every other place on earth thinks is like, yeah, that's how business is done. We're like, no, we don't pretend we're like, wow. What must this say about their lifestyle and like military, like culture? What must this say about their inscrutable soul, Asian soul, so impenetrable, so hard to understand? The fuck, man.

Ryan Naraine (01:37:39.642)
We pretend we do it like...

Ryan Naraine (01:37:46.32)
Cause then he's put a lot of whitewash on this stuff eh.

Ryan Naraine (01:37:58.501)
Mr. Free For All over here.

JAGS (01:38:02.827)
Anyways, that's on a Eugenio. Eugenio's work is good. Just weird receptions, man.

COSTIN (01:38:03.338)
I don't know I was... yeah I was just looking at this Enduril post on X If you have seen it The lowercase one Like the ones all lowercase like Sam Altman style

Ryan Naraine (01:38:13.978)
Which one? There was like, so there were two, there were two I saw. All over KC.

JAGS (01:38:18.871)
I need to go get my andriol jacket, man.

Ryan Naraine (01:38:23.664)
Hi, can we talk quickly? We got news out of Cisco Talos around Salt Typhoon. One of the things they're making clear is that, listen, the Salt Typhoon people are rummaging through these telco networks using old vulnerabilities that have been patched for a long time, stolen login credentials, living off the land techniques. There's nothing magical or sophisticated about ODA usage here at all according to Cisco Talos visibility.

JAGS (01:38:34.115)
off.

Ryan Naraine (01:38:50.522)

They conformed two things, two things we got confirmation from Cisco is that CVE 2018.01.71 is a remote code execution vulnerability. And one of their smart install feature was actually compromised in this. And they're saying we have no information that these other three or four CVEs that the government is talking about is actually thing, but they're still again, old patch things. What did we learn from Cisco Talos here? Anything, anything groundbreaking at all? What do you know cause Juanito.

JAGS (01:39:20.301)
I'm gonna get in trouble on this one. I have a feeling because I don't get the feeling that Talos wrote this.

Ryan Naraine (01:39:34.334)
Ooh, ooh, ooh.

COSTIN (01:39:34.584)
Mm. Mm-hmm.

JAGS (01:39:36.569)
Go look at that shit. It looks like fucking product guidance. You need to go hard in this and that. And for customers who enabled the this and the that and whatever, they can expect a patch and a fucking brownie in their mailbox tomorrow. And you're like, what the fuck? This is not a research report. What is this shit about? Like we've got, we know one Ode is real, but the other ones we don't think are true. And you're like, bro, you maintain these fucking devices. What do you mean that you don't know they're true?

Does that mean you haven't seen them? You haven't evaluated them? That the government make them up? Like, what the fuck are you talking about? And honestly, the rest of it is like generic guidance about things we'd already heard about, but that don't really speak to the operational limit, like issues here that make it so that even your guidance is not really all that solid. Because like your...

you're doing this bullshit thing of like, well, this is how this concerns my appliance that I make. And no, no, no, no, no, no, no, no, no, no, no, no, no, no, no, no, no, no, no, no, no, no, no, no,

Ryan Naraine (01:40:39.514)
Well, it's their visibility, and in all fairness we're hearing- Okay. Okay, go ahead.

JAGS (01:40:59.789)
B, that would explain why you're saying four O-days, but you only know about one and the other ones, just gonna, like, you're not telling us that they weren't real O-days or that you analyzed them and they're actually N-days or that they were exploits, but they didn't work. You're not giving us some guidance that says we looked into this and we're telling you that, like, authoritatively, only one of them was an O-day.

They're saying one of them is an Ode, the other ones are a rumor because we haven't looked at them or like nobody shared them with us.

Ryan Naraine (01:41:30.426)
They're explicitly saying that no new Cisco vulnerabilities were discovered during this campaign. While there have been some reports of assault abuse, these three are known Cisco vulnerabilities. We have not identified any evidence to confirm these claims. Again, this reads to me as like, here's our visibility. We don't have the evidence.

JAGS (01:41:47.469)
But your visibility is A, one IR's worth of visibility because I'm sorry, these are.

Ryan Naraine (01:41:56.014)
Is it possible that they're in the same conundrum that we are where we don't have a device to inspect? We can't definitively.

JAGS (01:42:03.851)
No, no, how do they're Cisco devices?

Ryan Naraine (01:42:06.926)
No, mean, meaning they don't have telemetry from the victim.

COSTIN (01:42:07.147)
No telemetry.

JAGS (01:42:12.793)
I don't think this is a telemetrical thing. I don't even know what kind of telemetry they can and can't collect. I don't know what they can and can't do remotely because, I mean, there's zero transparency about any of that stuff. But I honestly, I haven't asked because I don't want to put anyone in a difficult situation. But like, this doesn't read like a Talos report to me. This looks like a fucking Cisco knowledge base article about how you can cover your ass.

about the Cisco part of your network, because the other part here that's saying like, it doesn't, it cannot, it does not matter in the way that they're discussing it, because what I want to remind you is that there are, all of these networks have multiple types of appliances on them. So giving you hardening guidance about how you can go about

Ryan Naraine (01:42:46.736)
Could it also be true though? It could have also been.

JAGS (01:43:10.657)
Like they almost make it sound like these people are so silly. It's just credential, like just the using of valid credentials. And you go, yes, but the credentials are harvestable from the network

and the network has multiple types of appliances, not just Cisco. So even if I do all of your bullshit hardening for the Cisco thing,

Ryan Naraine (01:43:34.618)
Credentials are still exposed and being ripped off here.

JAGS (01:43:35.661)
The credentials are still going to be exposed in the network where there are other footholds that you're not talking about. So this is like very much a myopic CYA release. I, and I resent if I'm right, then I resent that they tried to use the Talos mantle because this doesn't sound like a Talos report.

Ryan Naraine (01:43:57.029)
Yeah. I see where I see the point you're making.

Ryan Naraine (01:44:04.238)
Hmm, Costin, you read this report. There was one line here that I want to flag for you. says that Redacto also pivoted from a compromised device operated by one telecom to target the device in another telecom. And then there's no technical details or no description of what that is. It tells you also that whoever wrote this, whether it's Talos or whichever lawyer kind of put this thing together, they threw that in there because they have this visibility. Like, what do you, what do you make of that line?

COSTIN (01:44:32.078)
Well, I think it's common and it happens that some of these telecoms are connected to each other for either like, you know, swapping customer information, especially when it comes to telcos, subscriber information, all those kind of things. So that's not necessarily surprising. I was somehow thinking that I saw this before, but I can't quite say exactly where I have seen it before.

The other line, by the way, which attracted my attention were just two things which I find surprising about this report. The first one is that yet another report without IOX. Like there's two IPs in there, but I understand they're like legitimate IPs. So, exactly.

JAGS (01:45:16.281)
Then what the fuck was that?

Ryan Naraine (01:45:16.814)
quite unlike unlike Talos as well. Talos is known for for for shipping Ix, right?

JAGS (01:45:22.605)
Well, not just for shipping IOX, but then you get this weird, like, update where they suddenly go, these, like, first it was like, these are salt typhoon IPs, and then they have to update the blog, and it's like, never mind, these are legitimate IPs, and you're like, the kind of, the fuck is this?

COSTIN (01:45:34.104)
That's ours. Yeah. And then the best part, like for me, the most I don't want to say the only the only interesting, the most interesting part of the report is when they talk about this thing called jumbled path. And I was thinking, this is something new. I don't think I've seen jumbled path being mentioned before. This is like a new malware name for me. It seems to be some kind of a custom tool written in Golang.

Ryan Naraine (01:45:36.952)
No, smart install abuse not associated with salt.

COSTIN (01:46:03.288)
And I was like, awesome, where is it? Like, share the hash man, like, be like, come on, we need some IOCs. I'm still surprised that people are still too secretive when it comes to salt iPhone. Where's the hashes? Like, does it really hurt that much to share a hash for jumble path or the Yarrow?

JAGS (01:46:22.489)
Let me ask you something. And this is what be even worse. What if this isn't salt typhoon? What if this is just a different Chinese threat actor, different random threat actor that's hitting Cisco appliances? Because like at this level of analysis, we've watched other people.

COSTIN (01:46:38.083)
possible.

JAGS (01:46:49.835)
Like that recorded future report was bullshit. We've like, we've seen a lot of ambulance chasing on the salt Typhoon train. And I am asking if you remove the name Talos from this blog, would you trust or even believe that this is salt Typhoon and not just we saw a thing hitting an appliance with a back door.

that did the stuff and it sounds salty.

Ryan Naraine (01:47:17.242)
This is the problem with show your work, right?

COSTIN (01:47:17.71)
I trust I trust I trust is salt typhoon you know why because no IOCs that's that's a proof if it was something else there'd be IOCs

Ryan Naraine (01:47:23.152)
There's the proof.

JAGS (01:47:25.113)

This is very much a trust me, bro. it's not. that's why I feel like really indignant on the suspicion that this isn't Talos. Because trust me, bro, this is the equivalent of like, you know, if those bullshit blogs about Ukraine coming out of Microsoft had been branded Mystic.

Ryan Naraine (01:47:40.41)
Fair enough.

Ryan Naraine (01:47:52.1)
Right, right, right. You mean the Cyber Peace Institute blogs.

JAGS (01:47:53.309)
Which would have been, would have, yeah. I mean, look, I bitched about the digital crime unit and all that crap, but like, at least they had the decency to not like drag the name of their like genuinely believed research team through the mud for like some cover your ass shit.

Ryan Naraine (01:48:11.738)
Yeah, we're not throwing mud on Cisco Talos at all. Shout out to the guys over at Cisco Talos. But the biggest takeaway here, if you could walk away with one thing here, is that listen, these telcos are literally sitting on unpatched vulnerabilities. User credentials are everywhere. It's a complete and utter mess there, and there's no level of sophistication needed for Salt Typhoon to be successful. I feel like that general gist comes over in this blog post that it's a fair takeaway.

JAGS (01:48:15.117)
No.

Ryan Naraine (01:48:40.816)
I want to talk quickly about Russian APT, a new report out of Mandiant. Our friend Dan Black with a report on Russian APTs abusing this link devices feature in Signal. So Signal allows you to scan a QR code and run the messenger on your phone and on your desktop concurrently. It's a feature we all use, I'm pretty sure. He has found evidence of a couple of unks, sandworms,

targeting individuals of interest in Russian intelligence services, Ukrainian military personnel, government officials and so on with this trick and this technique. Is that something significant cost in? Does this mean we should all stop using Signal if we are...

COSTIN (01:49:22.67)
No, I mean, look, to me, it all makes sense. And we've seen Russian APT groups getting interested in compromising Ukrainian encrypted communications because they have no other ways to snoop on what the Ukrainians are talking about. And we've seen cases where encrypted signal chats are being used to discuss like real stuff on the battlefield.

This is being used on the battlefield for real, for military purposes, sometimes through GSM networks, but also like in other cases through Elon Musk space internet. So it's not a surprise

that they are targeting that. was thinking that there's an interesting parallel between this story and the one with Apple removing the advanced encryption in the UK.

because in essence the question was like why would the UK government need Apple to remove that encryption because basically there's no good way of breaking signal communications but by default and if you don't know what you are doing all your signal messages actually get backed up in your iCloud unless you go in there and you manually disable like through one of the menus and

Well, if you're the UK government, you can try to ask for those backups which will contain the messages. If you're the Russian government, you don't have that luxury. So you need to develop all these tricky, sneaky methodologies if you want to steal the signal SQLite3 encrypted databases from the computers of the victims to target their accounts with QR codes. Of course, all of that

It's essentially just how to say guerrilla warfare I mean something that they have to do in order to snoop on those encrypted communications and what I really liked about this blog is that it didn't focus on just one thing in one group leveraging this Sneaky new method with the malicious QR codes, but it goes through all the different groups which have very different methodologies by the way they

COSTIN (01:51:46.082)
either do phishing kits to steal the signal credentials or disk QR codes or stealing of the databases for instance Turla does that they like to do that so I like that very much for me it was a very interesting blog with multiple IOKs for the different actors mentioned there so props for a very nice one

Ryan Naraine (01:52:06.426)
But it also pinpointed a pretty significant weakness in this signal mechanism. think a signal actually fixed something here based on this reporting because signal is updated up to include safeguards such as user verification prompts after linking new devices and requiring authentication for adding new devices, which suggests that in the past you could just scan a QR code and.

COSTIN (01:52:14.552)
Mm. Mm.

Ryan Naraine (01:52:29.774)
It runs in the background, there's no like triple checking that. Wait, that's the right QR code. Wait, I'm in a restaurant, I'm expecting a menu. Like, weird. Right.

COSTIN (01:52:31.968)
Yeah, that's like no, it's terrible. It's terrible and somehow this, by the way, reminds me of the story we discussed the last time with pretty much more or less the same, but with Microsoft

Entra, per favor, por favor story. Yeah, yeah, coming, coming. Like when there's like this method where code can be sent to an account. I thought that...

JAGS (01:52:36.639)
Right, right.

Ryan Naraine (01:52:50.192)
Come in Ian, come on Ian!

COSTIN (01:53:00.408)
There can be some parallels in there. It's interesting that the Russian tractors are moving towards these methods where they listen to the site. They link their interception infrastructure through essentially abusing features in the communication protocols applications. And then they just sit to the side, get a copy of everything and they don't have to do zero days malware like iOS.

Ryan Naraine (01:53:02.446)
Yeah, yeah, yeah.

Ryan Naraine (01:53:16.813)
Mm-hmm.

Ryan Naraine (01:53:25.732)
Yeah, you don't have to break encryption or do any of this stuff.

JAGS (01:53:28.873)
I think it's also an interesting corollary that they are doing this, meaning that they don't have a mobile capability that's actually properly scaling and sitting on those devices. Because like, no, no. I mean, look, it's always preferable, right? Like to have full device access and know what else they're using and know if there's other coms and be able to like do analysis and spiral out from there, et cetera. So like the fact that they're not.

Ryan Naraine (01:53:41.178)
Or they don't have to. Or they don't need.

JAGS (01:53:57.633)
Like, yeah, yeah, sure, sneaky, but you would never choose this as your first option, meaning that to some degree that first option is not available, which I think is very interesting too. But I'll...

Ryan Naraine (01:54:12.176)
Pretty interesting.

COSTIN (01:54:12.353)

I remember talking to one of, think it was somebody working for one of the cyber mercenary companies at a conference. Not my friends, not my friends, just people I meet. It's like people who want to, you know, just come and take photos with me. Yeah. For some reason. And then if you want to have a photo with them, they like super

Ryan Naraine (01:54:23.162)
Look at you! You and your friends!

JAGS (01:54:24.141)
Yeah, he keeps interesting friends. Yeah.

JAGS (01:54:33.593)
Yeah. People who want to take photos. Yeah, do you get those? I, uh, yeah.

JAGS (01:54:42.221)
Yeah, exactly. I blue hat, blue hat is real as always. Yeah.

COSTIN (01:54:42.528)
I was like asking in that particular case I knew they had zero days but at the same time they were doing some like low-end phishing and I cannot say I wouldn't say yes

Ryan Naraine (01:54:54.766)
Was it at Blue Hat Israel?

JAGS (01:54:58.135)
I cannot say. He's famous everywhere. He's famous.

Ryan Naraine (01:55:00.693)
Yes, he cannot say yes. Go ahead, go ahead.

COSTIN (01:55:03.82)
Maybe Romania or Bulgaria. And yeah, it was like, what you guys have zero days, right? You have like all this wifi exploitation. You have zero click, I message thing is, what do you do fishing? Like he said, like, listen, sometimes it's good to have some low end capabilities that get caught and everyone is happy. Like, yeah, we caught those guys. This is all they have. It causes some kind of.

Ryan Naraine (01:55:29.796)
Big blog post, big report,

COSTIN (01:55:31.95)
Yeah, they're happy. Everyone's happy essentially, and we can still use our zero days and nobody's thinking about searching or finding those. So I would, I would expect like these super sophisticated groups, especially the GRU affiliated ones to do to have some kind of iOS

exploitation capabilities. And we've seen them like APT 29, for instance, in the past, they were targeting people with iOS zero days over LinkedIn.

Ryan Naraine (01:55:39.492)
Misdirection.

COSTIN (01:56:02.03)
to steal their cookies and to read their messages. So I would expect them to have such capabilities, but they save them for the most valuable targets like the the crop of the crop if you want and for everyone else it's good to have some malware that steals your SQLite 3 databases or uses these methods and sometimes you'd be surprised at these simple basic techniques

JAGS (01:56:18.221)
Yeah.

COSTIN (01:56:27.0)
can bring more value and can bring more information than the super advanced zero click chains.

Ryan Naraine (01:56:34.896)
Shout out to Dan Black for some good work, good research, sharing his work. And let's end the show on a more lighter note with a story that we'll all understand. The last time we heard from Satya Nadella on Twitter, it was about this Windows recall thing that turned out to be a disaster. This time around, we get a big Satya thread on Microsoft announcing a breakthrough in quantum computing. I say this is a pretty easy thing. It's named Mahorana.

COSTIN (01:56:43.468)
Yes?

COSTIN (01:57:02.378)
My orana. My oran. My oran.

JAGS (01:57:03.991)
you're on the

Ryan Naraine (01:57:04.612)
Cost in, unpack and simplify this for us. What are we looking at here? Microsoft created an entirely new state of matter. Why is this the biggest thing ever?

COSTIN (01:57:13.326)
Look This is like one of those tricky things when you ask something and the reply is about something else So like what are you wearing our company? Just launched a new pair of shoes and like no that was not the question like what's what kind of hat are you wearing? Yeah, our

shoes are the best so like if you want to just you know to be to nitpick things I don't think that they announced or

Ryan Naraine (01:57:15.216)
You

Ryan Naraine (01:57:25.456)
You

JAGS (01:57:27.009)
Hahaha!

Ryan Naraine (01:57:33.712)
You

COSTIN (01:57:42.254)
created a new state of matter. think that's wrong. That is wrong. I call it. No, they didn't. Look, there's four states of matter, There's four states like solid, liquid, gas and plasma. Four. That's it. Now, well, again, if you want to nitpick things, but there's physicists out there who would say, well, this is a, with maybe a Russian accent.

JAGS (01:57:44.855)
Really? Microsoft didn't create a new state of matter? Are you serious? Are you saying they're lying to us? They didn't change the physics of our universe last week?

Ryan Naraine (01:57:45.572)
That's what the man said.

COSTIN (01:58:09.58)
This is a new, entirely new quantum state of matter which is very different from state of matter. Quantum, not quantum. That's different. And I think, by the way, there's like some amazing Russian physicists on YouTube talking about the universe and all that. I was just, I am, right?

Ryan Naraine (01:58:27.78)
You see this rabbit hole? He's going to

JAGS (01:58:29.421)
Dude, this is fascinating. I'm here for this shit. Let's go.

COSTIN (01:58:33.1)
But like look, it's not a new state of matter, but for sure it's something new again, a quantum state of matter. what they say, and I thought that the name they chose for this chip, which is Majorana, it's an Italian name. It's of a guy called Ettore Majorana. And I was wondering what

kind of name is Majorana like for Italians. But then I realized Romanian people who are like brothers with the Italians, we have this name as well, Majorana.

So yeah, it makes sense. It sounds Italian. right. And Ettore Majorana is a famous guy who disappeared under some super mysterious circumstances. He bought a ticket from something like Naples to Venice and then he vanished during the trip. Only to some people say that he appeared later in Argentina. Other people said he appeared in Venezuela. So it's like a mystery. His disappearance remains a mystery if you want, but he was a

JAGS (01:59:22.233)
fuck

COSTIN (01:59:29.56)
brilliant physicists who came up with this idea of Majorana particles which they're not like the typical particles you know like you know from school protons, neutrons so these are kind of let's say pseudo particles, fake particles or cluster of particles it's like saying the three of us together we are a problem but it's not like three different problems we are just one problem

So this is what it is essentially, it's like a cluster of particles when taken together they behave differently. And most quantum computers so far, they leverage different techniques to create these qubits and they all suffer from the same problem which is decoherence. They break down after a while. So the qubits break down and that means that you can't correct the RSA encryption with them.

So what Microsoft did here, like if you want differently, they leverage these fake three-body problem particles to create a more stable infrastructure that could allow them theoretically in the future to develop the 1 million qubits super quantum computer. So there is for sure some progress. So there's a significant breakthrough here. I would say they haven't

like really created the new state of matter. So it's not like inside this chip there's some glowing sparkles which are neither matter, liquid, nah, nah, it's actually more boring than that. But what is kind of crazy here, if you ask me, is that they do say that the information is not kind of stored locally with this particle. So what that means

JAGS (02:01:02.039)
an infinity stone of some sort.

Ryan Naraine (02:01:05.072)
So you're calling out Satya.

COSTIN (02:01:21.038)
probably relates to the Nobel Prize in Physics from 2023 which was actually granted for proving that the universe is not locally real. So I was still thinking about that when I was reading this.

What does it mean? like the information is not locally stored. Where is it stored? They are not storing it in the chip. Can you imagine that? It is somewhere else.

JAGS (02:01:23.011)
Cloud particles.

Ryan Naraine (02:01:42.264)
you this was a soft topic.

JAGS (02:01:45.067)
in the hyper cloud.

COSTIN (02:01:48.606)
We can't say for sure where the information gets stored, but the whole point here is that because the information is not locally stored, it is more stable. So it cannot be influenced by temperature variations and other things. So it may be in a different universe, maybe can be in a different time zone possible. Maybe it's in like three hours behind or three hours ahead. And that's why it's more coherent.

JAGS (02:02:10.04)
What the fuck is happening over there with you guys?

Ryan Naraine (02:02:11.344)
Juanito, Juanito, could you close with some shout outs please?

JAGS (02:02:16.761)
I mean, I think this is like, it's amazing that Microsoft can recreate the universe on a whim just a couple of weeks after some Nvidia statement makes the entire quantum computer market drop like 13 % or whatever, right? Like it's cool. It's like, no, no, no, it's not that far away. Come back here. Interesting time.

Ryan Naraine (02:02:19.098)
Get

COSTIN (02:02:43.032)
Well, and can I say the fact that they immediately went, they didn't say that this will allow us to do the 1000 qubits. This, they didn't say this is going to allow us build the 5000 qubits. like if you want to break RSA, people say maybe you'll need about 5000 qubits, something like that. And RSA can be broken with, you know, all the error. The more qubits you have, the better, but they, they went like straight for the one

million qubits. So to me, this was also a bit fishy, like, but it sounds better. Sounds much better. But like, but to the bottom of things, like at the moment, this chip, has, you know how many?

Eight qubits. That's it. So they say we're going to get to one million, but for now we have about eight, which these eight, they allow us to factor all the numbers from one to 10. So good job.

Ryan Naraine (02:03:17.52)
Very good. Yeah, I understand all of

Ryan Naraine (02:03:32.624)
We got eight.

JAGS (02:03:33.849)
Good enough.

Ryan Naraine (02:03:41.06)
Juanito, close the show for me, please. You got some shout outs?

JAGS (02:03:45.797)
I did, I don't remember anymore. I'm like marveling at Satya, master of the universe. Well, okay, unfortunate stuff with the power at DistrictCon, but I am excited to get to watch some of these videos actually on the plane to reverse conference, which I will be doing an iOS training. So to bring all this stuff kind of together, doing iOS Mac, the Jiska's iOS Mac OS reversing training. So I'm excited.

for that and here's hoping no emergencies like pull me away from any of it. But excited for this new con as we've talked about it multiple times. The other thing I've been thinking about is with this Russia signal post that you brought up and Dan's great work.

JAGS (02:04:40.281)
If things are going to play out the way that was described in the Munich Security Forum,

then I think everybody better get ready to double back to giving a shit about Russia again. I think we, on some level from Western centric and American centric standpoints, we have started to look at Russia as a diminished threat, as a contained problem.

with this incredibly effective shield of the Ukrainians, you know, fighting tooth and nail and coordinated sanctions packages and all that stuff. And if that's all about to change in some capacity, unless we see some like serious continuity, all I'm flagging is for everybody who moved on and

is now almost entirely focused on China or like local, you know, ransomware or whatever it is. Don't get too cozy not paying attention to Russia because it's going to become incredibly relevant, at least to Western Europe. So more so than it already has. Not to mention Africa and the Middle East and so on. But interesting times.

Ryan Naraine (02:06:10.426)

Kostin, you got some shoutouts?

COSTIN (02:06:12.462)
sure thing interesting times just the other day over here in the Constitution Square there are people with the American flag in one hand with the Russian flag in another hand and with the Romanian hand in the third hand all the same and like what's what's going on in this world we don't know shout outs to our good friend Mr. Will Bushido token who submitted the fantastic story we didn't have time to cover on

JAGS (02:06:28.417)
All AI people.

COSTIN (02:06:41.646)
Taiwan government wanting to ban Fortinet, allegedly because of their links with China.

Ryan Naraine (02:06:50.224)
Yeah, apparently the Fortinet CEO and his brother are Chinese citizens who created that company many, years ago. mean, there's like some loose connections. The Zoom CEO also has like links to China that Taiwan is flagging. It's like, hey, this is Chinese related problems that we should start looking at. We can get to it in the other episode.

COSTIN (02:06:59.886)
Hmm. Hmm.

suspicious, yeah?

COSTIN (02:07:11.33)
Very interesting, So shout out to Will, of course, and to pretty much all the other people who are okay in my book, except for those who are not okay.

COSTIN (02:07:23.906)
They know who they are.

Ryan Naraine (02:07:24.08)
I will be at ReverseCon in Orlando with Juanito there. If we have any listeners there that want to grab a cup of coffee, grab a beer, come and find me. We'll say hello. And with that, thank you everyone. Thank you gentlemen. We'll catch you again next week.

JAGS (02:07:40.665)
Take care.

COSTIN (02:07:41.624)
Bye bye.