Episode 47: The Three Buddy Problem

Russia hacks Ukraine war supply lines, Signal blocks Windows screenshots, BadSuccessor vuln disclosure debate

WATCH & LISTEN:

YouTube: https://bit.ly/TBP-YT
Spotify: https://bit.ly/3DH5wEO
Apple: https://bit.ly/3budprob

Cast:

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

JAGS (00:00.354)
Pizdec

Ryan Naraine (00:01.284)
Good morning everyone. This is episode 47 of the Three-Body Problem. I'm back with my buddies Juanito and Costin. Costin checking in from Romania where they just finished their election season. Can you give us a quick wrap up? I understand a mathematician from the Math Olympiad is one of your winners. Give us a quick recap of what's going on.

c (00:21.663)
Yeah, so the very famous mathematician, Niku Shordan, who actually is one of the very few people who won the Math Olympics with the gold medal twice. And he did so with the perfect

score and only 25 people in history have managed to achieve the same is going to be and is the new president of Romania through the power of blockchain, through the power of our

Ryan Naraine (00:42.116)
Congratulations. What does that mean through the power of blockchain? Because I saw that they published the results on the blockchain.

c (00:46.957)
We were like kidding and joking that we need the blockchain right to record all the votes and you need to vote with your ID card that has a chip inside and what do you know like in Romania it's already almost reality so all the votes were recorded in a blockchain that anyone can download inspect and it guarantees that the winner is the one that we want the winner to be something like this

Ryan Naraine (01:10.798)
That's what the blockchain says.

c (01:13.516)
I'm kidding of course. But it's funny to see how things happen in reality and that this blockchain was actually implemented through a governmental directive. There was a governmental directive which said that all the votes need to be registered in a blockchain, which I only found about after the election finished. So to me it was a bit like surprise. Yeah, but somehow it worked out guys, it worked out.

JAGS (01:13.646)
and

JAGS (01:35.662)
They kept it secret so you wouldn't fuck with it, you know?

c (01:43.808)
We have a new president. Someone said of course that after you guys canceled the elections last year, you didn't expect for the other guy to win, of course. But I mean, of course.

JAGS (01:56.834)
I think we were all worried he was gonna win. Right? Like, I was very surprised when you were like, the the math Olympiad guy won. And we're like, nice.

c (01:59.379)
Everyone was. Everyone was.

c (02:07.264)
which is just, yeah, it's unexpected, but everyone's like, let's see. We're gonna see how a mathematician fares with managing a country. Like, how will that go?

JAGS (02:17.922)
Man, if he fucks this up, we'll never grab another educated person ever again. Ever.

Ryan Naraine (02:23.524)
Juanito, why aren't we putting our votes on the blockchain in all seriousness? this like a pathway to some sort of verification, some sort of elections integrity issue? Why aren't we leading in this?

JAGS (02:35.918)
I

JAGS (02:39.49)
Because there's no money to be made in it. No, I don't know, man. So our issues in the US, as far as I understand them, have very little to do whether the record is immutable and verifiable. That's an obvious problem with any election. But our issues are much lower down the chain of gerrymandering and ID.

Ryan Naraine (03:09.87)
Same things we talked about last week, vote or ID compliance.

JAGS (03:10.03)
Yeah, ID compliance issues and like, you get an ID in the first place and like all that kind of nonsense. which is not to say that this element doesn't matter, but it goes hand in hand with like a bunch of other stuff. And I don't know, man. Like I think this is an area where the U S is most efficient. Mostly because of like the federal versus like state level division.

c (03:11.647)
Mm-hmm, I've already.

Ryan Naraine (03:36.836)
Did you say most efficient or deficient? Okay, I didn't hear it clearly.

c (03:38.877)
Deficient I hope it was. Deficient.

JAGS (03:39.636)
Deficient most D most massively D deficient, deficient. There's Yeah, it's a disaster, right? Like you have this like, federal, supposedly federal process being run by 50 different states at different levels of organization and different standards with different whatever and then you have local governments implementing that below that standard. It's impossible. Like how do you

c (03:43.496)
Efficient? De-efficient.

JAGS (04:08.492)
Unless you standardize the whole stack, like what are you doing? So our issues are organizational.

c (04:13.539)
Just for the record, I think it's funny to say that the observers sent by the US government afterwards, they give like a statement and they say, wow, elections in Romania are really advanced. We have a lot to learn from this thing, which to me was impressive on one hand, but you have to know one thing that voting stations, closed at nine and basically by 12 we knew

JAGS (04:30.625)
Really?

c (04:43.269)
the president was. Like, counting the votes took about three hours, something like that. That's all it took.

JAGS (04:49.858)
blockchain math. Chainalysis determined who the president was within three hours.

c (04:51.167)
blockchain.

Ryan Naraine (04:56.11)
Congratulations on your return to democracy. Hopefully you join the rest of the world and we get a mathematician helping us to count up there.

c (04:59.019)
Thank you.

c (05:03.859)
It took only something like two days for the US embassy to say that they're happy with the results. They didn't, they didn't come, that's like the most impressive thing that only two countries didn't congratulate him. Russia and the United States and the United States after two days, they said something they're looking forward to work together, but they didn't say congratulations.

JAGS (05:03.886)
your fancy elections.

Ryan Naraine (05:11.256)
They congratulated him officially.

Ryan Naraine (05:29.594)

so we have ambivalence towards it or probably not entirely happy. Can we pivot to the news quickly? I wanted to start, we got a bunch of stuff to get to. I want to start at the top. We have a detailed report from our friends at CISA. CISA's been in the news lately with all the cuts and all the uncertainties surrounding there. We got a new report here on APT 28 slash Fancy Bear, GRU unit 26165. And the emphasis here is on.

Western logistics providers and technology companies that are servicing the Ukraine war. think the tone of this advisory from CISA was like, you're one of these companies in this defense industry, transportation hub, maritime air traffic, IT services, and you're doing anything related to Ukraine and so on, assume that you have been targeted.

The other means they didn't specifically see a breach or they didn't specifically see attack. They talked about heavy, heavy, heavy targeting. Kostin, I know you spent a lot of time reading this new CISA report. What do you make of this? This is wartime targeting that we should be expecting, but what do you make of the quality of the report and what we learned from it?

c (06:26.186)
target.

JAGS (06:31.64)
CISA report.

c (06:40.294)
Yeah, well first of all I noticed there's a lot of co-authors and they say co-sealers, co-sealers, so to just contribute with their seal on the report. There's like a lot of countries in there like the Czech Republic, Poland, Estonia, France, our Dutch friends of course, Canadian friends, and the German like the BND, the BSI, and the BFV as well.

and our friends in the UK. that's like a lot of, a lot of entities put their seals on this report. So I had like very high expectations. Of course, one thing I noticed is that Romania is also listed in there as being targeted. However, as I went through, through the report, I, at least this is my impression that it's more of a summary of like recent happenings and even not that recent.

So a lot of this, I mean, it's been covered in blog posts for the past three years from many different companies. I can name just, let's say Sequoia, Harfang, ESAT. So there's, let's say a lot of this activity is already known and been covered in detail. Well, however, you know, like this is a freebie. So you take what you get, like whenever there's a report with DIOX, ERA rules, I'm a...

I'm a happy panda and in particular I was super happy with the Yara rules. I said, wow, Yara rules from CISA in a CISA report. then like, of course, cautious happiness kind of cautious joy. I put all the rules in my test environment and yeah, well, not surprisingly, they do have some false positives for one of the rules, which is again, it's shocking. I mean, how many times

JAGS (08:16.714)
you

c (08:32.487)
has this happened? How many times did we get Yara rules from CISA to find out that they haven't been tested, they haven't been properly engineered, whoever is writing these Yara rules doesn't follow the best practices, they don't have a meta section with details like hashes, the authors and so on. I don't know, it feels like a... I'll give you an example. So...

Ryan Naraine (08:52.708)
Why is that problematic? Does that send you off on a wild goose chase? Does that like slow you down? Does it make up your work? Why is it so problematic?

c (08:59.793)
Now, like here's an example. So there's this Yaro rule, apt-28 headlays shortcut, which is broken in the sense that it finds a Thunderbird, it finds Microsoft Edge, it finds Firefox, so it has false positives. So if you want to fix it first, you need to find some samples on which it triggers. So for that, people put a hash in the meta. You take the hash, you take the sample, you look and you say, huh, so you need to

play a bit with it so it finds that sample and it doesn't find a false positive. It doesn't have a hash in the meta section. It doesn't have a date, it doesn't have an author. So if you just take that rule out of context, you don't know who created the rule, you don't know who's responsible, there's no reference. And all of that gives you the impression that it's, how to say, it's careless, that's the word. And it's kind of a pity because the...

Canadian our Canadian friends. I actually, I think I said it many times. They have a kind of a standard for how the meta section should look like. And that's like how to say the industry standard. And a lot of people follow that standard. I follow it as well. And it's a pity that an organization such as CISA is just, they just ignore whatever the Canadians have put out and publish these URLs.

Which are careless. That's that's a sad word here not to mention, of course the false positives But like to go back to what you're saying the report I thought it was interesting because it did include some IP addresses that were new for me and they say that these type addresses are involved in brute-forcing activity, of course that you should investigate them so they may overlap with VPN says as usual but

There is, how to say, bit of new stuff in here, but keep in mind that it was mostly built on a lot of work from previous publications, from private companies. It's kind of a summary. you take, just imagine you go to ChurchGPT and say, give me...

Ryan Naraine (11:09.22)
It's like a roll up. It's like a big giant, you know, give me a...

c (11:19.815)
the latest and the greatest on APT 28 with the most recent activities and kind of targeting and malware and let's make a report. You polish it a bit, you add some new stuff and you come up with this. In my opinion, it's fantastic. Like if you ask me what is the most valuable stuff in this report, I think it's the targeting. Saying that there's companies in Poland, Romania, Slovakia.

Ryan Naraine (11:27.202)
and you feed it a bunch of advisories,

c (11:49.467)
Moldova Italy Greece that are being targeted to me that is quite valuable and mentioning the industries again, this is quite valuable information to me together with all the other things. Yeah Hmm

Ryan Naraine (12:02.052)
What does targeting mean? What does targeting mean? They've seen a spearfish over some sort of email thing that says, okay, if you're spearfishing this company, they're being targeted. I wonder, sometimes I wonder.

c (12:08.461)
I think, yeah, like would be nice to say victims. So I think that a lot of people are shying away from saying victims nowadays, because the moment that you say victims, you immediately may become legally viable, liable, responsible. So that's why people say targeting. Targeting has like no legal implications.

Ryan Naraine (12:27.042)
disclosure requirements and so on.

Ryan Naraine (12:34.936)
But when you're retargeting, you understand it to be victims.

c (12:41.031)
I think that and I'll tell you like honestly what I think I think these guys they have some visibility into what APT 28 slash blue Delta fancy bear and so on are doing. I think they have some kind of visibility in terms of emails in terms of network access and so on. So they kind of know who gets started. I think they know who gets infected as well, but they maybe just

can get into those details. Typically what happens is they would reach out privately to their organizations in all these countries that are actually mentioned here like Estonia, Denmark, France, Netherlands and so on and they would say, hey, we think there's a victim in your country. You better get in touch with them and let them know they've been successfully compromised. So.

Sometimes this is kind of a giveaway when you see the other authors co-sealers in a report you kind of suspect, uh-huh So that's where the victims are And but at the same time if I were one of these companies here, I would for sure Take a look at this report And they do have like a very it's this is what we used to call the the cannonball They have the cannonball in there. They drop like all these domains

Ryan Naraine (13:41.764)
right.

c (14:06.47)
like dinDNS, dynamicDNS domains in there and say like block or investigate all kind of activity which involves those and at the same time they have these domains which are typically used for all sorts of offensive stuff like webhook site, fridge, fridge IO, FRG, mock, bin, pipe dream and so on.

And again, they say if you see any kind of traffic or redirectors Yeah, but i'll tell you honestly these aren't this won't be just apt-28 They can be like a lot of of many other things So that's why I say it's a cannonball But again, the cannonball is a good thing you fire the cannonball you block all this thing and

Ryan Naraine (14:36.866)
redirecting to these, right?

c (14:57.158)
There'll be people complaining, especially people doing offensive stuff on ability research, red teaming. They'll say like, oh no, you blocked our webhook site. It's not malicious. We use it for red teaming. So why did you block it? And I'll be like, whatever, it's a cannonball. So yeah.

Ryan Naraine (15:02.338)
Red team guys.

JAGS (15:14.606)
No.

Ryan Naraine (15:15.32)
Juanito, it makes me nervous when you're so quiet for so long.

c (15:16.953)
Shut up, shut up, it's a cannibal. He's building up energy, energy, energy.

JAGS (15:19.264)
It's a cash. I built it. I rewatched the last episode and I was in such a cracked out manic exhausted state that I was just ranting over everybody. So I am am comp. No, no, because I

want to hear what Kostin has to say. If I'm keeping Kostin from speaking, I'm fucking up here. So I today.

Ryan Naraine (15:22.176)
You

Ryan Naraine (15:35.684)
There is nothing wrong with that. Don't listen to the listeners. Fuck those guys.

Ryan Naraine (15:45.538)
Okay, I got a bunch of questions for you though, just in response. You'll be responding to Kostin, because there's three things I want to get to here. One is quality of YARA rules out of CISA. There's an expectation that this is the U.S. government cybersecurity agency and we should get a certain level of quality. I think that's the point Kostin is making.

JAGS (15:47.074)
Today's a collected day. It's a very, you know, I'm coming from a

JAGS (16:02.743)
No, no!

JAGS (16:07.052)
Ryan Naraine (16:09.976)
This is not a new issue. We've talked about this publicly in the past. People at CISA are very, very aware that we have been like...

c (16:13.166)
How very small, what is the budget like? How many hundreds of millions go into interseas? We're going in the wrong way, right? It's not the bomb money.

JAGS (16:18.636)
I guys you're going this isn't this isn't this about you were going it's no no no no it's not it's not that it's not about money it's just like they look

Ryan Naraine (16:29.336)
Let me tee it up and then you go.

Should we expect, I mean, isn't the expectation fair? And why hasn't this been fixed yet?

JAGS (16:34.2)
No, because you're...

It would be, it would be, but the expectation should be higher in this case, I think. and, I think we're putting it in the wrong place, right? Like CISA in this case is kinda like, you remember when project zero was publishing tag blogs from Google? tag didn't have a publishing mechanism, so it would just

Ryan Naraine (16:59.47)
Yes.

JAGS (17:07.896)
find a way to publish its stuff through Project Zero because Project Zero had a blogging mechanism that got through the lawyers and the approvals and the whatever. CISA, in this case, as insane as it sounds to say this, is the Project Zero of the situation. Not in skill, but just in the conduit to release a blog. Because there's like, as we noted earlier, there's like 20 fucking logos on this. And...

The co-sealance in many cases are just people who say, we agree with this finding and we are throwing the weight of our organization behind it. And in many other cases, chances are there's a lot that was written by some one of these organizations or multiple of these organizations and then was all put together under this thing. So every time you said Sisa, I kind of like,

Ryan Naraine (17:41.41)
read it and say, yeah, I'm okay with it.

JAGS (18:05.632)
shriveled a little bit because I'm like, the chances that Sysa put together a major portion of this are in my view, unlikely. The only part that I wouldn't be surprised if they did themselves is the Yara rules at this point because they're bad. But I personally trained some of the organizations that are on this thing to write Yara rules. And I'd like to think I did not teach them this way.

And frankly, I pinged somebody while we were discussing this and they're like, yeah, don't know who wrote that. Let me look into it. So I'm not going to say who, but it's one of us CoSylets. So you go like, who wrote them? I don't know. I am actually using this as an interesting use case for 03 right now. Cause CoSyn and I...

Ryan Naraine (18:54.306)
I was just going to ask, isn't this like, shouldn't AI just be writing Yara rules? Shouldn't we have an AI Yara rule writer app already created that says, take all of this and generate the most perfect Yara rule that includes all the metadata and all the stuff that Costin talks about.

JAGS (18:58.765)
Well.

JAGS (19:06.422)
Yeah. And if somebody would like to fund us to do so, please get in touch with us. no, this is, it's absolutely doable, but within certain measures in a much more complex system, I think right

now the problem that you would have is, and it's a problem that you have across the board with all of these AI applications to things. you, you can automate it.

But the whole point of that is that it highlights the importance of the expert that's gonna read the output and determine whether you got a good result. It means you can scale it, but you still need a coast and Vitaly Kamluk, Sergey Menev, somebody who's sitting there who's gonna look at it and go, yeah, this is a good rule. Well done system, thumbs up. And what scares me with something like.

Ryan Naraine (19:50.062)
like everything else with our use of AI.

JAGS (19:52.312)
Yeah, which is what scares me about highlighting that AI should be used to solve the problem that we're reading here, which is not these people have a lot of Yara rules to write and it would be nice if they had some automation. Instead is clearly nobody involved in this. I'm getting a phone call about this right now. Nobody involved in this is in a... No, no, I can't do that to him. No, no. I'll... Yeah.

Ryan Naraine (20:13.828)
Put him on, put him on, put him on speaker.

c (20:17.73)
Like with the coinbase scammers

JAGS (20:20.812)
Yeah, the call is coming from inside the house on the podcast recording. Sorry. But in this case, what you're clearly missing is, you know, somebody who tested, who someone expert who looked at it and said, hey, this is not because like, look, like Florian Roth and and and some of these other folks have released like Yara Gen tools for many years now. We have ways to get you kick started towards a good.

c (20:35.714)
Who did the QA?

JAGS (20:48.11)
Yara rule and it'll do like 60 % of the job. You still need somebody to take that 60 % and go, this is what's good, this is what's bad, this is the logic that we should add to it, et cetera. So AI is not the issue here, but the issue is very much what we're seeing with this report. I know for a fact that there are experts in those organizations that could have evaluated these rules and who would have known that they were good or not good. I don't get the sense that they did, which just goes to show like, look, there's a shit ton of-

Ryan Naraine (21:16.846)

This report might not be targeting you guys, right? The Yara rule and that portion of this, like let's throw in some things here is not meant to be the final output of this thing. True.

JAGS (21:23.566)
Sure, but that's worse, right? Because it's not targeting us. We can fix the rule. We can determine the rule is bad. You're not targeting us. You're targeting a wide swath of people who just saw a government report come out that authoritatively says that they need to care about these IPs, these domains. Moreover, I'll tell you, in a publicly traded company,

how comfortable would you be saying to your as far as like your fiduciary responsibility goes? Let's say that this report gets dropped, you know, before not Petya and a logistics company say FedEx goes, well, we looked at it, but we didn't think these were good IOCs. Then they get popped and they lose like $2 billion and they go to court, which has happened multiple times now.

and they argue that it's not their fault because this was an act of God and an act of war. and somebody says, yeah, but the insurance companies are going to say, well, there was this report from CISA with 15 intelligence agencies that told you to look at this. Right? So there's a, and that's just my, it's like this kind of straw man argument about like the, the, the onus of responsibility you are putting on these end users who

Ryan Naraine (22:27.886)
And the insurance companies aren't settling these kinds of things,

JAGS (22:47.53)
should be able to take this report and say, something big is going down. I'm going to put these rules into my systems. I'm going to block these domains. I'm going to block these IPs. Like, it's not like I am just going to take it hook, line and sinker. I'm doing my patriotic duty to defend my company. Right. And it sucks when they, you know, doing that may result in.

Look, the cannonball's not a... As Kosen is saying, it's not a bad approach. If you blocked a bunch of red teamers, good for you too. Fuck those people. Like, it's not our job to make sure red teamers have an easy time. Every time red teamers win, they take a shit all over the defense industry and go, ha! You see? You guys suck! We're so good at this! And then when you block something, they do like, my god, guys, that wasn't bad infrastructure. That was our stuff. Like, yeah, okay, good luck. Like, it's just like, what the fuck, man? No!

Ryan Naraine (23:32.036)
Listen to Mr. EDR over here. Mr. Defender of EDR over here. Yes, that's why you're so agitated.

JAGS (23:36.27)
You know how much of a headache red teaming is for EDR companies? Every time some asshole red teamer walks in and like takes a dance around and they go, installed Cobalt Strike. Yeah, like, yeah, dude. I can't. I'm gonna. Yeah.

Ryan Naraine (23:48.302)
Juanito, quickly, targeting versus victimology. When you read targeting here, what's the nuance about what I'm reading? These companies, they've seen a couple of spearfishing things or Kostin believes they have some network telemetry that tells them there's some finagling happening there. Do we assume that when they say countries with targeted entities include Bulgaria, Romania, Ukraine, Netherlands, Moldova, Italy, blah, blah, blah, that these people have already been popped?

JAGS (24:17.326)
I think the bar for what you can put in a government report is fairly high. which is to say, you asked about the language, you asked about targeting versus a victim. And the way that I like, the way I tend to think about is, this might not actually be universally correct, but every victim is a target, but not every target is a victim in a sense.

That's not actually true when it comes to like opportunistic infections and like worms and stuff. like give me, give me in this particular case, let's just say that a target is a softer statement to make. You say the attacker made some kind of activity action or whatever that entails that they were interested in this organization. And some of those targets will have gotten victimized. They will have gotten breached and popped, but not all of them necessarily.

And maybe all of them did, but this is where you see that like government hedging of like, this is what we can say within this high level of confidence. Can you say that they were full on victimized, that it wasn't like a third party, whatever, that it wasn't, they got into an appliance, but they weren't actually able to move into the thing? Did every one of these organizations confirm it? Has every one of these organizations been notified and acknowledged that they were hacked? No, no, no. The answer is gonna be.

know or maybe for most of those. So it's easier to just scale back and say these were targets. That's what we know. Whether they were victims or not, we're happy to have that conversation in private. But and part of this is also going to be like the standards are going to be different, right? Like maybe the Germans are extremely, you know, neurotic about making damn sure that their victims are victims and maybe the Bulgarians are not right. Like, who knows? So you you get this kind of hedging. But to be fair, I think

Look, I'm being kind of negative about the quality and whatnot, but let's approach this from a different angle. The amount of work it must be to get one of these things through the review process of 15 ultra-bureaucratic organizations, most of them intelligence agencies, who are publishing something public, and there's an intel assessment that you're not...

JAGS (26:42.764)
burning sources, there's intel assessments that you're not precluding other activity, that you're in theory that your IP blocking that's fucking over these red teamers isn't actually fucking over some legitimate Western operation, right? Like there's all these sort of like equity bullshit

discussions and they may not be necessary. This might all be a 90 % public reporting, but they had to go through that process like 15 different ways. So in some level, like while I think it's inexcusable to have not great Yara rules,

I think it would be wrong of us to throw the baby out with the bathwater and not acknowledge that somebody went through some pretty hard work to put this in front of us, and I think that's commendable.

Ryan Naraine (27:21.934)
Is it likely that this was in the CISA pipeline as part of what they normally do or this is new CISA focus on flagging? I'm just checking. You're my Washington DC correspondent, bro.

JAGS (27:28.46)
Stop sissing, man. Stop sissing. This is not... No, I...

I'm,

Ryan Naraine (27:46.82)
He doesn't want to talk about CSIC. Kostya, one thing I noticed from the report very specifically was that they said one priority target is shipping manifests, including train, plane, container numbers about these companies that gives them visibility into what's going into Ukraine and when. I'm just kind of putting it alongside how cyber plays a role in these physical kinetic war conflicts.

There's a parallel effort that CISA highlighted, the report highlighted around hijacking thousands of IP cameras at border crossing and rail yards that give them like some real time view of the actual convoys moving along matching up against these manifest things. I think it's just fascinating to get some documentation of the type of cyber activity we're seeing that go along in these wartime things and that kind of defines what cyber war looks like today. Is that fair?

c (28:17.299)
Mm-hmm.

c (28:36.508)
Yeah, absolutely. And there was another thing which caught my attention. mean, in addition to everything you're saying, the fact that they attempted to use voice phishing in one case to impersonate by impersonating IT staff in order to gain access to privileged accounts. So again, that is not often seen, I guess, with these people with APT 28.

And at the same time, yeah, having a glimpse into the cyber side, which kind of supports the physical activities, like all this intelligence collecting about the content of the cargo containers and train, playing numbers and so on. This is fascinating.

Ryan Naraine (29:14.882)

interesting.

Ryan Naraine (29:25.156)
What was your tracking name for this? Right. Sorry, Costin, what was your tracking name for Fancy Bear? What was the great tracking name? So if I see, there we go.

JAGS (29:25.262)
It's brilliant. This is real Intel. Sorry.

c (29:27.613)
It's real,

c (29:33.309)
So for see.

JAGS (29:33.922)
of SC. Well, eventually you went Hades with if you go like the broader GRU construct. To what extent would that be right this day?

c (29:40.957)
Like no actually that's that's different unit right now. That would be a different unit with within that organization like the guy is responsible for the Pyongyang Olympics Olympic destroyer and These other script all poisoning related as punish against Wada and so

JAGS (29:52.962)
Yeah, Olympic destroyer.

JAGS (30:02.126)
But I think that's where it's interesting because when we talk about WADA and Tascas and IOC, like finding out about the arrests of like the Hades guys, that was brought up, A, it was brought up in the Mueller report, which is supposed to be about APT 28, Fancy Bear, et cetera. And B, I mean, we saw the WADA and early intrusions before we knew that that was related to some of like the public stuff.

And that to us was APT 28. Right. So I guess that's where I'm like, I'm looking at that as I wonder sometimes if we should have been looking at Hades as almost like an initial access broker of some sort for APT 28 stuff that we would see later when you talk about some of like the on the ground operations, like the stuff the guys got arrested for and like, what was it Belgium or the Netherlands? The Netherlands. Yeah.

c (30:54.045)
Netherlands, the Netherlands, yeah. I don't know if that is the case, because I don't remember seeing them passing victims, but I may be wrong. I hope like one of our listeners can correct me

if I'm mistaken here and there has been a victim passing between the two groups. But my feeling was that, and by the way, historically speaking, the APT20S slash Sophosy guys

One of their main goals was to figure out if they have to launch the ICBMs, if there's like a nuclear attack going on and if they need to launch a counterstrike and when and all these things like understanding the strategic arsenal. It's not, it's not, but like over time.

Ryan Naraine (31:45.624)
Where is this documented?

c (31:51.056)
their kind of scope widened and then they became interested in extremist activities in the Caucasus in all these breakup republics like Ingushetia, Ossetia and so on and obviously they just expanded, expanded, expanded and then in parallel these other guys who like specialize in poisonings and targeted assassinations also developed cyber branch.

Ryan Naraine (32:19.31)
Correct guys, correct Blizzard guys.

c (32:20.508)
the Hades guys, they're kind of, you know, complimenting each other if you want.

Ryan Naraine (32:26.346)
It's fascinating. It's just fascinating to me that the real-time wartime intelligence, how much it's changed and how the cyber component goes along with it is really, it was nice to see in the report documented.

c (32:37.533)
One of the things which I which I realized by looking at these stories is what do you think you know about? One of these groups today Like it can very quickly change and like six months later. They're doing like a totally different thing From like they were targeting one. I don't know Group like ethnic group in six months. They're targeting the Pope or the Vatican or something else and their mission changes

their tools change and it's kind of, I think it's impressive when you can actually track them across all these operational changes. That's fantastic. But in some cases you kind of lose track and they disappear as it happened like with others like wild nutrients.

Ryan Naraine (33:25.06)
Juanito, you were going to respond to the wartime surveillance live look thing?

JAGS (33:29.486)

Yeah, mean, I think it's actually the more fascinating part of Intel and some of the... One of those areas where you see the clear disparity between what in cyber we would traditionally consider valuable targets or important to protect devices and what in intelligence.

you would consider important to hack devices. Like we talk about, I don't know, Chinese webcams getting popped en masse all the time. You go, there's 40,000 Chinese webcams. They've all been popped by someone. Moving on to the next story. Yeah, it's like some stupid botnet. Let's talk about something else. And it's really interesting when you consider that having 40,000 webcams in a country that you are

Ryan Naraine (34:12.216)
It's some Mirai botnet, we'll go on to the next thing.

JAGS (34:27.862)
in a war with is an insane strategic advantage of like any kind of like war strategizing that has been written over the past 3,000 years would marvel at the idea of having point by point surveillance, video surveillance across another territory, being able to watch and literally count.

Ryan Naraine (34:50.83)
ports and maritime ports.

c (34:52.475)
Thank

JAGS (34:56.056)
how many different container ships were loaded with how many containers and what trucks came and at what time they showed up and how big were they and were they weighed and blah. Like that is a boon for an intelligence agency. That is actually ground truth level stuff that where you go materially, we know this many containers have moved in and out of this port over the past six days.

When somebody claims they're ramping up war production, they're getting new weapons, you go, no, they have the same amount of containers moving through the port that they move their weapons through as they did two weeks ago, right? Like that kind of shit is fascinating. And that's where you see this huge disparity between what cyber security traditionally considers worth defending and worth tracking.

and what intelligence agencies actually treasure value and need.

Ryan Naraine (35:55.46)
Speaking of APTs breaking into things, want to shift to the next story on our list which is Sequoia. Kostin mentioned our friends at Sequoia put out a report on Vicious Trap which is an investigation of a threat actor compromising more than 5,500 edge devices and turning them

into honeypots. More than 50 brands, SOHO routers, SSL, VPNs, DVRs, BMC controllers are being monitored by this actor possibly to collect exploited vulnerabilities affecting these systems.

Is this something we normally typically see? They mention here this is a Chinese campaign from an attacker of Chinese speaking origin. But using those as honeypots to look for exploits and like try to trap vulnerabilities across there seems fascinating to me. Do you get a chance to read this report, Costin?

c (36:45.787)
I did, I did, and I know that... I mean, we have to do the episode like I said, one episode we don't read anything in advance and then we just put like a wig and a mustache and we pretend to be evangelists and to be like, pretend to be experts on this topic without reading anything.

JAGS (36:48.546)
Thank God.

Ryan Naraine (36:50.409)
Yeah

JAGS (37:05.902)
You remember that?

You remember that the American spy that supposedly got caught by the Kremlin like I want to say it was like 15 years ago and he had like a blonde wig and a fake mustache. It was like proof of him being a spy. That would be my costume for for shifty business. That's what we're going to call it shifty biz.

c (37:19.258)
c (37:25.978)
Shifty, shifty, okay, shifty biz, shifty biz. We have to do that. But like, mean, I read like because I thought, I mean, I knew that some people were looking into this. I mean, there's been a whisper of this for a while in some circles, especially with people running honeypots. So this activity was being discussed to me.

Ryan Naraine (37:31.822)
Cause they're assholes.

c (37:55.128)
Like the best image that I have in my mind about this is a book. The one from the Chinese writer, Cixin Liu, which is called Dark Forest. So essentially it feels that we are living in a dark forest where everyone's hunting everyone, everybody else. And you think, yeah, this is a threat actor? No, they're actually, I don't know.

hunting other threat actors and turning your machines into honeypots to catch others. And then there's somebody else hunting these guys. And then there's someone else hunting those. This is a real fourth party collection, right?

JAGS (38:30.242)
this is the real it's the real three body it's the real three body problem like I have not read

Ryan Naraine (38:32.983)
Real spycraft.

c (38:36.639)
It's a real three body problem. It feels like the dark forest. To me, it's fantastic that Sequoia decided to put this out. I think they know a bit more about who's behind it and I think they know a bit more about some of the other things that this actor is doing.

I think that would be good if other companies researchers would be looking into this activity again share more data more gear was because I know I know other companies have very interesting data on this but I guess everyone is careful with legal issues targets not victims attribution might be a bit tricky and things like that

Ryan Naraine (39:25.796)
Is there some risk of implantation, your own business intelligence logic software involved in this to be able to monitor and track these things?

c (39:34.571)
I mean, there's for sure a legal risk here. I mean, there's a lot of us running honeypots, right, in the industry.

Ryan Naraine (39:42.564)
It feels like there's a lot you're not saying, Costin, I gotta be honest with you. It feels like you're hedging and hawing and being careful. Why? You could tell me why you're being careful, but at least it'll help me understand why I'm being like, why you're flutzing around this issue for me.

c (39:46.851)
I need to be careful, Luca.

c (39:55.008)
Because I have an NDA in place. I have an NDA in place.

JAGS (39:58.062)
This is this is what you get for reading you just you get grilled

c (40:02.36)
This is when you feel like the US when they have to talk about salt typhoon, right?

Ryan Naraine (40:09.878)
I don't mean to grill you but for the audience, the audience listening is obviously going to realize that you're hemming and hawing and hedging and what you know and what, but help us understand why.

c (40:12.12)
No, no I Tell you what I am I am I don't know that much myself But I know other people know a lot more and I would love to see these other people also publish their reports on this stuff Because I mean it's very tempting. I think it's very tempting when you do this IOT honey potting to think that

We don't have enough honey pots. We have like 50 but just imagine if you had 50,000 honey pots and how difficult is actually to repurpose one of these things to turn everything into honey pots collect, I don't know files IOCs indicators whatever from Every compromised device and try to hunt for anomalies now. There's there's some companies which actually they make a living

From that look look look look at the cat. That's awesome You have to see this like the video on YouTube like it's the best thing to make your day It's so happy

JAGS (41:21.696)
You're very distracting. Very distracting.

Ryan Naraine (41:23.096)
I always feel like the cat gets blamed when you guys don't want to talk about something.

JAGS (41:27.086)
No, so

c (41:27.223)
I would love to talk more about again, I admit that I'm not the most knowledgeable on this topic and other people, mean, besides Felix, Sequoia and so on, there's other people who also found and looked into these activities. So,

JAGS (41:42.882)
We can get like John at John out house in here or somebody like. Yeah, Danny out of my recipe.

Ryan Naraine (41:45.444)
I should, I should, I should.

c (41:45.821)
companies like Lumen, for instance, could probably say a lot more on this if they want it again, if they want.

JAGS (41:52.238)
I mean, I can be ignorant as fuck on this if you'd like.

Ryan Naraine (41:52.45)
I clarify that this is not Sequoia the venture capital firm. is S K O I A dot I O. Sequoia is a secure. Yeah I have VCs listening bro. I have a lot of VC listeners. Juanita what is your take on this?

c (41:55.735)
Mmm.

JAGS (42:02.104)
Bro, nobody thought it was Sequoia. Bill Corrin is not Bill Corrin is not out here like fucking pumping IOCs and shit like it's just

c (42:13.717)
And I tell you a secret, the first time when I heard this name, I thought it was the capital company.

Ryan Naraine (42:19.128)
Thank you. Thank you. When you keep saying Sequoia, Sequoia, there's a, there's a portion of our audience thinking with the Sequoia venture capital firm. This is a fairly new company too. and this is, you mentioned Felix, Felix Aimee, who was a former great colleague of ours is, is one of the researchers over there. Juanito, you didn't get a chance to dig into this report, but do you have a take on this whole honeypot hunting?

JAGS (42:20.536)
They would, I mean.

In our world, Sequoia is just Sequoia.io.

Yeah.

JAGS (42:39.898)
I did not. Well, so the first of all, like the first thing I thought of when I heard about this was actually whether this was the setup for an orb network rather than a honeypot, because that makes to me, that makes just a little more sense. And I'm not saying that they're wrong. I'm saying that that that I would expect the ultimate utility of having this many devices. Like it's a secondary thing to think of them as a honeypot, right? If an exploit comes.

c (42:51.575)
Mm.

Ryan Naraine (43:08.184)

Territorial dispute too,

JAGS (43:09.954)
Yeah. Well, mean, well, also, like, why would you only use it for one thing? If an exploit comes, great, but that's an opportunistic thing that you just wait for. If you're telling me in the meantime, you're sitting on 50,000 compromised devices that you can set up an operational relay box network, an orb network, which is what the Chinese are using for basically all APT operations around the world, right?

c (43:10.09)
Mm-hmm.

JAGS (43:36.226)
It seems like leaving money on the table to only use them to wait for an exploit to come. Also considering that you've already popped the device so clearly you have some kind of access. I'm not going to say an exploit.

Ryan Naraine (43:47.234)
Right, right. But you're assuming, you're assuming the actor here is the APT and the actor here is not some private sector research group as well in China.

JAGS (43:55.028)
I mean, that would be interesting. But if they're coming from China, I think you have to consider that there is a third player, which is the private sector operational relay box creating companies that are selling that service to Chinese APTs. Like that's part of the problem of the ecosystem in China is I don't think most of these or networks are being operated by the APTs themselves or the

government organizations themselves. believe this to be, yeah, this is farmed out. This is a third party company that's maintaining something and selling it as a service. And look, we do similar, similar things in the US, like anonymizer infrastructure for Equation Group was clearly managed by a company, but it was a series of VPSs. You had a company that was registering servers.

Ryan Naraine (44:27.46)
it's farmed out, right?

c (44:29.024)
Mm-hmm.

JAGS (44:50.924)
that were considered semi anonymous and was creating a web of proxy trafficking. And that's fine because it's technically legal within the US. But if that US company went and hacked a bunch of Soho routers across the world and created a proxy network and tried to sell that as a

service to the US government, they would have a very hard time getting through any kind of legal review. And they would be in a complicated situation, not to mention that Western

cyber practices do not look comfortably or favorably at using infrastructure that is not their own. There you get into the actual territorial dispute. You hack the router and you want us to go through it. Who else hacked that router and who else has visibility over it before we send our operational materials through that infrastructure? The Chinese have an appetite for that. They don't give a shit.

Ryan Naraine (45:44.014)
This is what that feels like to me.

JAGS (45:49.134)
And in some cases, they have paid for it, right? Like we've seen companies like Lumen that will go, look at these 40,000 compromised SOHO routers. We now see all of these APTs coming in and out of this place, and they track the shit out of them. But the West would never accept that. But there's also the element of this that I think I don't think Kosen was skirting around, but that I am too error prone not to skirt around, which is to say if

it weren't for our over-cellless DOJ and the laws around cyber. I have thought many times about how easy it would be for us as defenders to hack all of these, to pop all of these vulnerable devices that are on the internet, dump the memory, and then go looking for what implants are on all these places. The appliance vendors are not helping us. The router manufacturers are not helping us.

We have exploits because we are recovering them from what the attackers are doing. These stupid things are just sitting there vulnerable forever. Why don't we pop them, dump the memory out of all of them, are able to see what the connections are, are able to rebuild the malware, and then we restart them. And they're all disinfected immediately. Yes, they'll still be vulnerable, but that whole fucking network just went down. It's stuff like that where you go, there is some...

I'm sure would be reasonable quote unquote argument that that is a terrible thing to do, but I cannot for the life of me make that argument in good faith. Like routers go out of service all the time. Routers and appliances restart all the time.

downtime of like 45 seconds because your router is restarting has never killed a human being and if it has that really wasn't the root cause. So this pussyfooting bullshit of like well we could but then maybe a baby somewhere relying on a Wi-Fi router to get its oxygen might die and it would be our fault is like yeah think about man

Ryan Naraine (48:07.822)
Think about the babies, don't be dissing the babies.

JAGS (48:11.522)

Fuck them kids.

Ryan Naraine (48:13.38)
Costin, they said the actor is likely of Chinese speaking origin. Do we know how they got to that conclusion? Cause I'm curious if this couldn't be anything else.

c (48:21.424)
I mean, look, like I said, I have an NDA, but I can tell you one thing. People know exactly who is behind us. Not like just Chinese speaking, but the name. Yeah, no, it's.

JAGS (48:25.769)
Hahaha!

Ryan Naraine (48:30.862)
Gotcha. I should take this report at face value. You trust that Sequoia is publishing what Sequoia is publishing is a hundred percent on.

c (48:41.352)
Yeah, sure. It's super, super solid for sure. It's super solid. But I wanted to mention one thing as I was listening to one and I was thinking, look, the temptation when you see like some some kind of for router the vendors.

JAGS (48:41.548)
Vibes. Vibes. Vibes.

JAGS (48:53.112)
Uh-huh.

Ryan Naraine (48:54.574)
Why isn't the vendor themselves doing this? This is the thing that's fascinating to me, right? Like what? I know they don't give a fuck, but it makes so much sense that they have the infrastructure to do it best. Like the Avantis, the Sonic Walls, these guys should be honey trapping more than anyone else trying to capture exploitation or signs of exploitation, right?

JAGS (48:58.158)
Because they don't give a fuck.

c (49:00.562)
You

JAGS (49:12.258)
They learned from Apple. What's the benefit of actually engaging and protecting and knowing and telling people? You know, first of all, yeah. Well.

Ryan Naraine (49:20.334)
Well, come on, you're in the headlines every week now. It has to start having an effect on your sales conversations, your marketing conversations. I know it's not affecting your stock price because Fortinet stock price keeps climbing, at the same time, mean, it must internally, they must be having a security just fucking us over conversation.

JAGS (49:30.222)
Yeah.

JAGS (49:37.464)
So I think it's really funny because you mentioned sort of the EDR space. From the EDR space, when we have a bypass or a serious misdetection, I mean, we treated it like a five alarm fucking fire, right? Like the company is deeply concerned and you put the kind of resources that are appropriate for protecting your customers. And there is an expectation that that could cause you some serious heartache, right? Reputational and so on.

It's really fascinating to look at the appliance vendors and to, because like I don't want to talk about the router vendors like the Soho router vendors, because those are margins games. Like those, they're throw, they are hard, they are trash hardware. It is the definition of like hardware dumping.

Ryan Naraine (50:17.316)
It was about throw away things,

Ryan Naraine (50:25.508)
You're talking about a $50,000 edge appliance device, this kind of impossible to rip and replace things. Yeah.

JAGS (50:29.344)
I'm talking about the yeah, I want to talk about the edge devices. Yeah, because at that point you are you are talking about a sizable investment and you are talking about, you know, reputational damage mattering and there is an expectation of defense and there are enough resources at some of these companies like Fortinet suddenly had like a threat Intel team and they were starting to like push out some reports here and there.

And I feel bad because I'm sure that there's good people there who are trying. I just don't really get the feeling that their organization is supporting them to a level where they're getting to be effective. Because we've discussed it here before. think Kostin had the idea many an episode ago of like, well, why the fuck don't they just put their own appliances on the internet and make them look nice and then just catch the exploits themselves and then fix them?

Right? Like, why don't we ever get a report from them saying, hey, this is what we did, and this is what we found, and this is how we fixed it, and this is what you need to do? It's always so-and-so told us that there's a thing here, and I guess we have to listen to them, so here's a fucking advisory, and then they move on. Like, it's this, you're dragging these people through this gauntlet, and they're not any happier for it. Like, for it, then...

Fortinet, Avanti and so on are not walking out and going, well, that was a crisis, but we used it as an opportunity to grow, right? Like, no, no. It's not zero fucks given. Why did you tell us? Like, we don't wanna know. And that sucks because they're the ones in that position to know the most.

Ryan Naraine (52:04.206)
Yeah, but why if I'm a divaunty?

If I'm at Ivanti or Fortinet, why am I not calling Sequoia now and saying, hey, can we do this project in tandem so that I get, can kind of float me some things that I should be mitigating? Like this is just, it just seems so logical and obvious to me. And it's not fair to say these companies don't give a shit, because like they're there spending, they're patching, they have security teams.

JAGS (52:26.562)
Why is it not fair? I think it's fair to say they don't give a shit. It's not the 90s. It's not the fucking 90s. It's not the first time anybody's done this. It's not Katie Misuris inventing the first bug bounty at Microsoft and people learning hard lessons the hard way because there's no path, right? Nobody has ever walked through this brush. So Katie's out there with a machete clearing that shit trying to figure out how to do it. And you learn some hard mistakes. You make mistakes, you learn some hard lessons, and you figure out some wins.

Ryan Naraine (52:31.501)
Well true.

JAGS (52:56.044)
and they're hard won and then you turn around and you go, guys, I cleared this path. This is what you should do. And people follow the pink hair and they get to success. That is not that. But that playbook is super fucking public. It has been replicated a million times. It's been improved upon. It's been discussed. We've had keynotes. We have literal companies that do this now. There is no version of this where you get to feign ignorance anymore. What you can say is, well,

Ryan Naraine (53:04.164)
And that playbook is public and known, like other companies can pick up there.

JAGS (53:26.616)
They have a slightly harder situation in that they're hardware vendors and they're coming at it with what looks like a fairly deficient update mechanism. So yes, you are going to have some difficulties on the ramp up, but there shouldn't be ambiguity about where you're going with that.

And that's why I don't give them credit because I don't see people who are like, okay, we understand that this is the playbook.

We have been fucking terrible at this. We just hired so and so who's fucking awesome. And they now have these insane resources to revamp our company. We are going to become the security appliance vendor par excellence and fuck all our competitors. Right. Like that would be dope. That would be awesome. And it would take time. But then we would suddenly look at them as like, I don't know, the ubiquity of appliance vendors, the

whatever, where you go, why the fuck would you ever buy any of these other appliances? That's the one appliance that is like gold standard security, up to date patching, perfect update mechanism, uptime, whatever. Their software is so good that exploits come about rarely now. And when they find one, they make sure to take out a whole class of these bugs and like...

You know, there's there's there's an SLA and there's a support whatever and they're inspectable. You can go check this thing and like if you plug into this port on the hardware and you can dump the memory immediately and see what's happening like how fucking I mean, I'm not saying it's an easy thing to do, but it's not an easy. It's not a hard thing to figure out. Like the path forward is not the hard part. They just don't give a fuck.

Ryan Naraine (55:12.577)
It's hard for me to just kind of co-sign with they don't give a fuck. like they have a big security team, they're paying people to go. They're just saddled with technical debt at a level that it's impossible to recover from.

JAGS (55:24.824)
So start over.

Ryan Naraine (55:26.766)
True, I mean this is what the.

JAGS (55:27.662)
It's not stopping them from selling these things. Nobody said.

Ryan Naraine (55:31.128)
Someone called me after, someone called me last week after I was dissing the pledge at length, the Secure by Design pledge and the new one coming out of the UK to say, listen, this pledge is giving us budget. This pledge is like internally at these companies, this pledge is giving me kind of a voice to say, hey, we signed the pledge so we should be doing this, this, this. They starting over isn't really an option. Trying to backport these fixes with the technical debt you've inherited is why we ended up with Ivanti with.

c (55:47.857)
Mm.

Ryan Naraine (56:00.822)
open source thing that they shipped into the thing last week, like the configuration issue with Ivanti and the zero day exploitation there. So it's a terribly difficult problem, but it's just hard for me to understand why they're seeding this bit of research, this kind of honey potting of their devices to third parties when like it's an established norm everywhere else. That doesn't make any sense to me.

JAGS (56:23.726)
I think I understand why. I just think that it's an unsatisfying answer. Like this is their old school companies. They do think that they can get away with it. And there is this question. Somebody somewhere has sat down with a napkin and said, it's gonna cost us this much to improve and it's gonna lose us this much not to. And they go.

those numbers are fine and they moved on. And it's interesting because it's

Ryan Naraine (56:55.605)
Or someone sits in the middle and says, let's sign the pledge and do a trade off where we can kind of say this and we can kind of do some small things and make some nudges forward. That's what it feels like to me.

JAGS (57:06.914)
I just, how many years later would you, how many years would you give them from the beginning, let's set an arbitrary date. Let's say that this shit show of circumstances started three years ago. I don't know. Like, I mean, the Ukraine war had a lot of reliance on these sorts of exploits. So, yeah, yeah, yeah.

Ryan Naraine (57:30.18)
This is why shields up was a thing, right? It was, yeah.

JAGS (57:35.668)
So three, let's say three years ago, it's been three years since they became aware of the Swiss cheese, you know, hardware they were selling and how it was being abused actively at wartime and across the world to fuck literally everybody on earth. It's been three years. If you told me that they did this middle middle ground thing where they're going, well,

fixing it right away, super hard, but maybe we signed the pledge and our whole goal is like, we're going to ramp up to the next generation of our devices being the ultra secure thing. And then we can, we can deprecate all this other shit. We're like end of life, all this stuff and just do a clean break with it. And we'll be like the new Avanti. mean, Avanti already fucking rebranded once, right? Like the new rebrand. Yeah, it was pulse secure. Like I think like now we rebrand again.

Ryan Naraine (58:26.82)

There used to be something else, right? Right, right.

JAGS (58:33.24)
to Vonti and then you like, it's the new next gen appliance that doesn't fuck you for owning it. No.

c (58:38.818)
with AI.

Ryan Naraine (58:39.382)
Actually, they were never pulse secure. Pulse secure, the Ivanti was previously known as Landesk, Heat Software, AppSense, Wavelink, and Shavlik. They had five previous names. They were all separate companies merged into one.

c (58:42.591)
That's Cisco,

JAGS (58:50.508)
No, no, but that, but that's, think wasn't pulse secure another one. Yeah. They, they bought all that. and, and honestly, I, I, there's a talk by MJ Emmanuel from like previous labs con. want to say two labs cons ago, which was like looking at the sort of evolution of the software of these things. You're like, no lab lab scan. Once she did the satellite stuff. Yeah. Yeah.

Ryan Naraine (59:04.43)
Lapscon 1, Lapscon 1.

Ryan Naraine (59:11.416)
They did change, they did acquire Pulse Secure and kind of assume that brand. Yes, you're right.

JAGS (59:16.088)
Yeah. like, but I would not be surprised. And I think MJ's sort of work was in this general direction was like, I would not be surprised if like, there, this software is basically like a collection of fossils. Like if it was literally like going into the Smithsonian and looking at a T-Rex and it's like, just like,

We dug up these pieces from land desk and a piece for full secure like a thing for whatever and it's like PHP with bail wire. And moreover, I'll bet you whatever you want that if you dump that that fucking firmware in front of us that we would find code of different versions of the same software.

like PHP 1.5 and PHP 1.7 and like, you know, like that kind of shit. And you know, you know, it's true. I will fucking bet you whatever you want. If I had the time, like we would do this, but it doesn't matter. It really does not matter because my point about the timeline was if you tell me in good faith, they do care. They're just living with corporate realities and you cannot fix.

Ryan Naraine (01:00:08.164)
It's all duct taped together.

c (01:00:09.92)
It's for sure.

JAGS (01:00:28.448)
and rewrite and change things overnight, nor can you do it in six months. Okay, it's been three years. How many more years do you give a corporation before you admit that they don't give a fuck? How many years do you give them before you go, okay, you couldn't fix this one, but there's another generation of Ivanti products and they have the same problems or like there's a...

Ryan Naraine (01:00:48.58)
Now that's a... Yeah.

Ryan Naraine (01:00:54.616)
Well, corporations aren't humans like the AI isn't a human that can care. No, but the point I'm making is that there might be folks internally there who truly care and who are truly trying, but they're faced. You know what I'm talking about. In every one of these organizations, these shitty organizations, we know a guy or two in there individually who understands realities and they care.

JAGS (01:00:57.166)
Citizens United says completely different, my friend. They are, they have feelings.

c (01:01:15.693)
Take care.

JAGS (01:01:17.166)
I am happy to shine a light on those people and treat them as heroes, but I don't think it's appropriate to give a company a pass because there's a couple of people working super hard to fight against the rest, the 98 % of that company.

Ryan Naraine (01:01:28.182)
A pass, I get it.

Ryan Naraine (01:01:37.228)
And these are the folks who are saying stop fucking hitting the pledge. The pledge is all I have to continue to get a little bit of budget to get a little bit of a stick internally.

JAGS (01:01:41.824)

Right, right. Okay, so then, okay, so you know how we stopped like shitting on on people who work at CISA and whatnot because like, they're victims now and like, we're just hoping that they kind of Yeah, yeah, right. Right, like, you know, well, I mean,

Ryan Naraine (01:01:54.52)
We'll play with the cat during pledge conversations.

c (01:01:58.925)
We just complained about the other rules.

JAGS (01:02:03.276)
That is an objective complaint. I love Cyber Command and I admire NSA and everything, but if they wrote a shitty rule, they wrote a shitty rule. I'm not saying they did. I don't think they did. I really do not think this was done. But I don't know, but I actually have an offer. Would you like to send them some fixed rules to get republished?

c (01:02:14.509)
cool route.

Ryan Naraine (01:02:23.556)
There we go.

c (01:02:23.597)
Sure, look I did this before, I I sent fixed rules before to people and they said thanks and they never got fixed so sure let's try it again.

JAGS (01:02:26.04)
That.

Ryan Naraine (01:02:33.998)
You

JAGS (01:02:34.158)
No, I've got a different offer here. So send me and let's see. Let's give our friends a chance. beyond that, let's talk about, sorry, go ahead.

c (01:02:39.181)
Let's see.

c (01:02:45.325)
I wonder if there's ever gonna be an episode in which we don't complain about Yvanti or Fortinet or any of these vendors

Ryan Naraine (01:02:56.812)

It starts to feel repetitive to be honest with you and I listen to the podcast and we say the same shit every week and I realized like, well, yeah, this is what cyber security basically looks like. It's a microcosm of our industry, right? The same shit every day.

JAGS (01:02:57.357)
JAGS (01:03:08.168)
every single day.

c (01:03:09.38)
You know what I was thinking that like another reason why nobody cares is that it's such a closed ecosystem. It's a closed set. So if there's a vulnerability in what you're going to do, you're going to switch to 40, but surprise like those guys, they also have vulnerability. So everybody in this kind of closed set has the same security issues and actually it's best for everyone.

Ryan Naraine (01:03:20.526)
Lockbox.

c (01:03:36.532)
if they still have security issues, if somebody starts fixing them, that's an issue. Because then everybody else needs to fix them as well. But as long as everyone's bad, like, there's no problem.

JAGS (01:03:42.082)
Yeah. Yeah. Yeah. You know what that's called? You know what that's. Kostin, you know what that's called? Anti-trust. That's what that's called. The fact that no one in this competition feels the need to fix their shit because if one of them fixes it, then they all have to fix it.

Ryan Naraine (01:03:45.694)
If everybody sucks, we're fine.

c (01:03:54.334)
And I trust. I see.

Ryan Naraine (01:03:56.558)
speaking.

c (01:04:04.566)
Yeah. Yeah.

JAGS (01:04:05.802)
is a form of like anti-competitive coordination between mega corporations that is affecting the consumer disproportionately and negatively. Like that is why we put the kind of pressure that we do on these people. And frankly, this is where I go right back to resenting our oversell this DOJ

and stupid laws like the CFAA, because I think that the right solution to all of this is bricker bot. I think somebody should

Ryan Naraine (01:04:10.477)
Collusion, right? Collusion does suck.

JAGS (01:04:35.33)
brick all of those Avanti appliances. And then, only then, will we have a fucking reckoning.

c (01:04:37.324)
You

c (01:04:41.1)
gonna sell more. The only thing is that they're gonna sell more like replacements so that's gonna be seen as a good thing so everyone will say can we get bricked as well please brick us too.

JAGS (01:04:47.608)
and then you brick all the fort in it once and then you brick...

Ryan Naraine (01:04:52.996)
So don't be advocating for breakage. That shit is going to make a baby die in a hospital somewhere. Stop it. Speaking of the same shit, speaking of the same shit year after year, day after day, same shit year after year. Do you guys have the appetite for a vulnerability disclosure debate? Akamai researcher Yuval Gordon yesterday discovered a privilege escalation on April 1st reported a privilege escalation vulnerability in Windows Server 2025 default installation.

c (01:04:55.818)
Hey, hey, hey.

JAGS (01:04:57.516)
The baby, the babies, wifi powered babies.

c (01:05:08.608)
Yeah.

JAGS (01:05:09.742)
Yaaaa

Ryan Naraine (01:05:21.614)
that allows attackers to compromise, in his words, any user inactive directory. Reported it on April 1st, Microsoft said, doesn't fit the bar for immediate servicing, it's just a moderate severity vulnerability, we'll get to it later on. Guy says, hey, this thing is serious enough that people should know that this risk exists while Microsoft refuses to fix it and he publishes a blog post

yesterday and he's taking serious heat for including attack details, like a full pathway to show how this thing could be.

done. He's taking some heat. Florian suddenly discovered the world of full disclosures is filled with ethical complications and there's like been some social media debate. Costin, you and I disagree on this, but I want to give you the chance to kind of hop on here. Who's in the right and who's in the wrong here?

c (01:06:09.131)
I like the fact that we disagree, but we disagree constructively. Mean first thing you know what I was looking for where the CV so first thing I was like if there's a CV that kind of compels Microsoft to fix it so Yeah, good point good point

JAGS (01:06:14.734)
Aww.

Ryan Naraine (01:06:15.682)
Well, you haven't heard my disagreement yet. Lord. It might not be constructive.

Ryan Naraine (01:06:28.984)
But who assigns the CVE? This is something Microsoft would assign during the patch creation process.

c (01:06:34.634)
So does it feel like Microsoft didn't want to assign a CV here? Like it feels like that, right? Correct.

JAGS (01:06:35.618)
the EU.

Ryan Naraine (01:06:39.298)
They could have given them a CVE and patch later, which they did at Black Hat. They did at Black Hat with another Israeli research. I don't remember the name of the thing. Downgrade attacks, Windows downgrade attacks. They issued three CVEs during Black Hat and then they patched it two months later. So there is a precedent for this.

c (01:06:48.34)
Mm-hmm. Mm-hmm.

c (01:06:57.034)
Look, I politely disagree with this technique or tactic in which you kind of try to ransom or blackmail a company into patching it by making it like full disclosure. And then everybody, you know, starts integrating that into their offensive tools. And suddenly you have like a new WannaCry or whatever epidemic on the internet. So I think this can be done in a more

ethical way if you want in a more coordinated way. think that they could have just kept talking to Microsoft, tried to convince Microsoft to explain that it's bad. I personally don't support this. I'm on the side, and I tell you something, we were in the same position where we had about a vulnerability, zero day level vulnerability that was being exploited in the wild.

Ryan Naraine (01:07:33.912)
Yeah. See, this is where my head starts to explode. That the illness goes on the researcher to beg Microsoft.

JAGS (01:07:42.914)
Yeah.

c (01:07:55.019)
in a certain version of Windows and Microsoft refused to fix it. They said yeah, you need to be administrator to be able to exploit it so that doesn't match our kind of reporting criteria. And we could have, of course, we could have blogged and published and give all the details and then, you know, other people start using it as well, but we didn't. We chose to respect what Microsoft said. We didn't publish it.

Ryan Naraine (01:08:07.95)
Yeah, they're borrowed. They have like a servicing bar, right? Yeah.

Ryan Naraine (01:08:20.484)
And I think that that was irresponsible. I argue that what you did, I argue it, let me make my argument.

c (01:08:23.302)
You think that's that's your no, I think it's not my I I understand. I understand what you're saying Go ahead. Go

JAGS (01:08:26.968)
Damn, this getting spicy. I like this shit.

Ryan Naraine (01:08:30.19)
My argument is that you were just an adjoining and irresponsible party by leaving the entire ecosystem at risk because you have this hubris to know you're the only person who could have found this. That's the ridiculous part of this entire thing.

c (01:08:36.562)
No, it's not me. No, I decline. I decline the responsibility. I blame it on Microsoft. It's entirely Microsoft responsibility. What we have here, we could have had the same situation when it was entirely Microsoft's responsibility. Now, I think it's Akamai's responsibility. It's no longer Microsoft. Yeah, it's on them.

Ryan Naraine (01:08:45.102)
Good.

JAGS (01:08:45.88)
I like that.

Ryan Naraine (01:08:47.64)
I agree.

Ryan Naraine (01:08:57.476)
No,

JAGS (01:09:00.235)
No.

c (01:09:00.542)
because they published the details which allow massive exploitation of this in the wild. So we're going to have a lot of bad fallout because of the fact that they didn't find common ground like negotiate whatever with Microsoft and get it fixed.

JAGS (01:09:06.222)
We used to say... No, no.

Ryan Naraine (01:09:06.498)
Juanito, keep one of us honest.

Ryan Naraine (01:09:15.584)
This is bullshit. Juanito, you go.

JAGS (01:09:17.272)
that's an assumption that Microsoft is working in good faith. look, I'm with you in certain situations. We have seen this. And it's more about like when we used to get pissed at like ThreatConnect being the amateurs of the TI space and going, look at me. I figured out this way to like...

identify all APT 28 command and control infrastructure because of this certificate and they would post it and you go, fuck, that was the only way all of us were using to grab all of these APT 28 infrastructure things. They fixed it within a week and you're like, God fucking damn it. All you got out of this was a fucking blog. You goddamn amateurs. That was upsetting, but that's because we had this opportunistic thing that was asymmetrically

benefiting us, the defenders, and it's a door that gets shut for the purposes of a blog. When it comes to vulnerabilities, I feel differently now that I've seen more of just how irresponsible and arbitrary some of these companies can be. Yeah, they may not be suing researchers the way they used to back in the day, right? Defcon, Black Hat, like,

we just going to walk in and sue you and that's the way to fix this. Okay, fine. They're not doing that. But they have found other ways to Stonewall, including the bug bounty platforms, which have become complicit in this because they will NDA researchers and then let them sit in limbo forever. And that's, that's fine. That's considered okay. Right? Like I think the project zero was, there was a kernel of brilliance, even from the start of project zero in putting that

Ryan Naraine (01:10:42.84)
They've found other ways to Stonewall, yeah?

JAGS (01:11:09.358)
Timeline of saying we are gonna publish this shit in six months unless you give us a really good reason and in that and and sorry in three in three months and unless you give us a really good reason and if And if we extend that on the basis of your really good reason, it'll be another three months or whatever another two months It's not indefinite and that's some that's what the bug bounty platforms are missing that makes it so that they're not Conspire co-conspirator

Ryan Naraine (01:11:15.844)
Three months, was 90 days, yeah.

JAGS (01:11:39.16)
co-conspirator in keeping people quiet and muzzled despite the responsibility that those companies have to clients to protect them. And it's built on an outdated thinking that doesn't take into account parallel discovery. And I was very naive about this in the beginning. Coming at it from the threat intel side and not from the vulnerability research side, my thinking was,

Ryan Naraine (01:11:39.534)
conspirators.

Ryan Naraine (01:11:58.318)
This is.

JAGS (01:12:09.038)
What are the chances somebody runs into the same bug? I mean, super low. And then the more we hear from the VR side becoming more open and scaled and there's you've got like the zero day reports and like all this stuff is parallel discovery seems to happen all the time. the reason there's focus on bug classes is not only does parallel discovery happen all the time, but you patch one bug in one component.

And it turns out that there's usually six or seven or however many other bugs in that same component. And you have to consider that if a really brilliant researcher, let's say like a Natalie Silvanovich working for the dark side has spent, you know, six months learning that one component, she didn't walk out of there with one O-Day. She walked out of there with 15 fucking O-Days. And after the first one gets patched, she's going to go.

leverage the same technique or the same vulnerable component and sell 14 other O days. No shade on Natalie, but like that she is like the proto brilliant vulnerability researcher. And if she were working on the dark side, that's what you would see. So there was this project zero mentality of like, we not only do we need to address these O days that we find within some timeline, but we also need to address the category of these, you know,

vulnerabilities because if somebody is latched on this deep to this thing, they are going to leverage either the same technique in a variety of different areas or they're going to go deep into the place they've already invested all that energy into and pull out every other bug that you can find. And that is the mentality that puts me in such an adversarial place with Ivanti and Fortinet and

and perhaps more so with Microsoft because in this case with Microsoft, like they don't have to, it's not like you have to go change the architecture of a CPU and change a fab and change, you know, and wait and try to push a giant recall or wait for people that change. Like it's a fucking software bug. Now, now I don't know the details of this one.

Ryan Naraine (01:14:21.454)
Fix the freaking bug. Just fix the freaking bug.

JAGS (01:14:29.45)
And I know I'm ranting, but there are many dimensions to this. Like, I don't know the details of this one, but a problem Microsoft has above all other companies when it comes to software is that their focus on enterprise support makes them the ultimate legacy support company. Maybe not as bad as like an IBM where you're like supporting mainframes at banks that were built 40 fucking years ago, but like, but pretty bad in that.

It's the reason they've never wanted to address like Kerber roasting or they had such a hard time with Mimikatz and they had such a hard time with these like golden ticket techniques and golden Sammel and like all this shit where you go, look, Microsoft is sitting there going, yes, kids, I would love to fix this for you, but I have to support six different operating systems with 12 different configurations of networking, all of which

need to keep working for 30 years before I end of life any one of them and they need to play with each other at all times. Like Eternal Blue was an SMB V1 problem and we were already on SMB V2, but they had to keep that shit going and had to keep working. You had to enable it because God forbid the baby machine runs on Windows XP and it needs to talk to a Windows 11 file server to keep the baby alive.

And if you change that one tiny thing, then everything breaks. And yeah, they're more secure, but the baby died, right? And that's enterprise security.

Ryan Naraine (01:16:06.532)
Costin, Juanito started his answer by talking about giving vendors benefit of the doubt and having this trust that they're doing the right thing. Do you apply your stance on this disclosure, never going public with exploits or never going public with exploit code to every vendor or do you judge based on who you think is a good fit vendor?

c (01:16:28.969)
I think it applies to everybody. I would, yeah, no, not necessarily. I would say first you report it, then you get the CVE, then you get informed. Like we're going to patch this in a month, two months, three months. And let's say that the vendor says, yeah, the vendor says in the future, you say, okay, guys, we're going to do it like this. We give you 90 days and we're going to publish it after 90 days.

Ryan Naraine (01:16:31.236)
Across the board, across the board you're a non-disclosed guy.

Ryan Naraine (01:16:45.678)
When Microsoft says it to Apache will be available in the future and you as a researcher think that this puts

Ryan Naraine (01:16:58.248)
my gosh.

c (01:16:58.557)
if you patch it or not. That's what I would do. And in 90 days I publish it.

Ryan Naraine (01:17:01.773)
my God. Mike Costian, I have read enough Quarks lab bulletins timelines to know how Microsoft digs these researchers around. Talk to Yvonne R. Say and somebody's old school guys. Nothing has changed from wait, let me finish.

JAGS (01:17:02.656)
Project Zero School.

c (01:17:14.949)
Look, look, I talked to Microsoft. mean, I reported like many zero days to Microsoft. At some point I was like in the top 100 MSRC zero day reporters. And I tell you that there were reasonable people. If that situation changed there, I don't know. But to me, I think you need, you what?

Ryan Naraine (01:17:36.302)

What do you consider, do you consider, do you consider, do you consider Microsoft saying the day before Apache is supposed to be issued, sorry, it didn't make it in, it's gonna come in six months. And then you wait six months and then they say, man, we need 30 more days. you.

c (01:17:50.658)
I would know what I said is, okay, we're gonna wait up to 90 days. Like we will have three months. And if it's not there in three months, it's not ready. I understand. But I'll tell you a secret. I will never publish the exploit code. I will publish a description like the root cause. I'll publish the root cause like without details that allow other people to implement it.

Ryan Naraine (01:18:00.628)
Okay. So for you, okay. And after 90 days, can I publish exploit code?

JAGS (01:18:09.762)
description of the vulnerability. Yeah.

Ryan Naraine (01:18:10.798)
Yeah, none of that changes.

Ryan Naraine (01:18:16.643)
So there are no circumstances under which.

JAGS (01:18:17.454)
Kostin is unequivocally right that you do not publish the exploit code. that has, no, no, the exploit code, the vulnerability description is fair game. The publishing the exploit code, all these assholes, and I will call all of you assholes who spend time developing an end day out of every patch and then putting it on GitHub, fuck you.

Ryan Naraine (01:18:22.543)
You're both wrong.

c (01:18:28.933)
Geek. It's fair.

c (01:18:36.783)
Ha

JAGS (01:18:45.462)
Like how many problems and nightmares this industry has gone through because every imbecile running a shitty low grade operation now has access to the latest end day because somebody was nice enough to put it on GitHub for educational purposes should go fuck themselves. But that's the same thing.

c (01:18:46.095)

You

Ryan Naraine (01:18:57.378)
How many?

Ryan Naraine (01:19:05.451)
That is a different thing. That is a different thing. How many vendors, how many vendors have refused to patch a vulnerability because it's not exploitable? And the only proof I have to show that it's exploitable is to tell the world, here's your proof of concept, here's your exploit code.

JAGS (01:19:15.51)
And if that's the case, if they're saying it's not exploitable.

Ryan Naraine (01:19:21.272)
This is what Microsoft is doing in this case. They're saying there are all these mitigations in place, blah, blah, blah. This is a low risk thing that nobody should care about. Now suddenly the guy publishes exploit code and it's a high risk thing. It's like, come on.

JAGS (01:19:33.144)
Yeah, yeah, I'll give you that. just saying like that is Microsoft's fault at that point.

Ryan Naraine (01:19:38.852)
But that might, but, you can never say never publish exploit code. Cause that's the last, sometimes that's full disclosure is the last only thing you have. I discussed this in my Echo party keynote and I grad you brought up the bug bounty thing and the fact, right? My argument there was, listen, you're being dicked around. You've historically been dicked around by these companies. You're being dicked around today. You will be dicked around tomorrow around all this cloud stuff that's coming. Zero day.

JAGS (01:19:43.427)
that.

JAGS (01:19:47.746)
Yeah. I love that keynote.

Ryan Naraine (01:20:04.663)
Publication and full disclosure, sometimes, sometimes is all we have. the minute you guys take that away, you have nothing left. I mean, that's at the philosophical level how I think about it.

JAGS (01:20:14.146)
Yeah, I-

I agree with you. just don't think and I don't really, I'm not coming down on this particular scenario at all. I think from the sounds of it, the the ECMA researcher has something good and has like a real legitimate concern and is being dicked around. However, reading that this is like a managed services type thing, Imabob, it

I cannot imagine this is an easy fix. Like I cannot imagine that in Microsoft land. Yeah, yeah, yeah, yeah. Look, at no point am I gonna defend Microsoft. I'm just trying to understand, like this isn't one of those where it's like, guys, like you just needed to change two lines of code and I even told you which ones and you just don't wanna push a patch. Like, fuck you. This is one of those where I am sure somebody sat back.

Ryan Naraine (01:20:49.636)
And say that. And fucking say that.

JAGS (01:21:12.64)
and like rub their fucking temples for 30 seconds and went.

there is no way we're gonna be able to address this due to a series of interdependencies between different, entirely different clusters of software and services and products here for another like seven years or something.

Ryan Naraine (01:21:31.214)
Is it possible that this was put into some sort of triaging spreadsheet and the spreadsheet spit out a number that says nine and the servicing bar is 11 and it just falls below the servicing bar and in an automated way your triaging system says, service pack, we'll fix in a service pack down the road. It's likely that that's gonna, it's possible.

c (01:21:45.475)
Ha ha ha.

JAGS (01:21:49.484)
Yeah. I mean, if it's a service pack, that's still fine. It's it's because that would be a service pack for one version of software like it's just Windows. Windows XP needs to wait till its next big cycle because it's a big architectural change. OK, but if it's like we need to change this here and in every other version of the OS and in every version of like the server and domain controller thing and.

in some kind of authentication with your cloud AD environment, then that is a shit show. That's why Kerberoasting and all these different types of Microsoft AD vulnerabilities have been unfixable.

forever problems and people have been talking about them at Black Hat for 10 years. you go, you get this golden ticket and then you do this and that and voila, you're admin and now you're like across the entire network. Like everyone's seen one of those talks. We've known about them forever and Microsoft has known about them and acknowledged them. But like there's, we'll just push out a patch and then we look at them and you go, why haven't you pushed it faster? And then there's, need to architecturally

change how different services are going to be able to connect to each other and then get. I understand. I understand.

Ryan Naraine (01:23:11.616)
Say that. That's all I'm asking. Say that. Document it properly from me and explain why this delay and why it has to be in a service pack. I can't believe we did a responsible disclosure debate in 2025 and we got 20 minutes of content out of this shit. By the way, shout out to Akamai. Shout out to the Gordon guy from Akamai. In the absence of an official patch, Akamai has published detection queries, logging guidance, and even a script to locate these kind of principles that can recreate these DMSs that assume that...

JAGS (01:23:18.53)
I'm not defending them, I just...

c (01:23:24.77)
You

Ryan Naraine (01:23:41.749)
the rights from the old ones. So shout out to Akamai, disagree with Kostin. Hopefully the guy, that's fine.

c (01:23:47.402)
I disagree with you, but we are still buddies. This doesn't met the threshold for us not being buddies anymore.

JAGS (01:23:51.502)
you

Ryan Naraine (01:23:51.552)
Always buddy, always buddy.

Ryan Naraine (01:23:56.063)
Absolutely.

JAGS (01:23:56.844)
It's a nine and the threshold is 11.

c (01:23:58.53)
The temperature is 11.

Ryan Naraine (01:24:01.804)

I got, I got some breaking news out of signal signal messenger. this morning announced that they're adding a new screen security setting designed to block windows recall from taking screenshots of your signal on windows desktop. thing we talked about windows recall at length. This is the AI thing that takes a screenshot every five seconds and put it into this searchable AI fancy schmancy database on windows AI PCs signal is saying, Nope, you're not going to be able to screenshot anything on signal messaging. It's going to bring up this block of things.

JAGS (01:24:31.479)
Valid.

Ryan Naraine (01:24:31.716)
Valid. The bigger issue here is that Microsoft has provided the ability for Signal to do this, but the onus now is on every app to go scramble to put this valid blocker in place for these screenshots. And I expect we'll start to see others follow Signal and kind of implement it within their apps. It's Windows only. It's Windows desktop messenger only, obviously. Costin, you welcome this?

as a mock user.

c (01:25:02.861)
god, I mean instead of fixing the apps, can you just fix windows? Like why do you have to fix all the apps? All the apps that implement some kind of a privacy block so that recall doesn't screenshot that. Can we just disable recall at all? It's not me. It's a cat.

Ryan Naraine (01:25:17.646)
Stop playing with that microphone.

JAGS (01:25:19.192)
Sorry, I wanted to fix the thingy. It's my, that's my fault. No, it's my fault. It's my being in a... I'm distracting from this because Microsoft has sent me a Windows recall device. And now that I'm, now that I'm sponsored, bought and paid for, I completely disagree with this. No, I actually, I feel really bad and my apologies to Dave Weston, but it took them a while to send me this after our last conversation. And I forgot that I had it. I haven't used it at all. I haven't even set it up yet. So I...

Ryan Naraine (01:25:23.172)
Jeez, sorry, constant.

Ryan Naraine (01:25:28.708)
You

Ryan Naraine (01:25:47.556)
Send it back and tell him to fix the fucking bugs and he'll fix it.

JAGS (01:25:48.31)
I need to do. It's literally like that device, like enrollment screen.

c (01:25:53.665)
It can't be long before all EDR products have a feature to simply disable recall or block recall or it will become hopefully hopefully hopefully I I think it's coming. I think that hopefully all security solution will implement a feature to disable recall

Ryan Naraine (01:26:04.856)
That's the expectation, right?

JAGS (01:26:05.11)
shit, me hit up my PMs, one second. Stop telling people.

Ryan Naraine (01:26:08.238)
You think I should expect my security software to do that, Kostin, in all seriousness?

c (01:26:20.237)
Or there'll be like open source tools that you can install to disable recall or just get cancel it or like get rid of this feature from Windows the same way you can disable telemetry collection. I don't know, thinking and typing collection and all this spyware like features.

Ryan Naraine (01:26:35.94)
It's a weird thing though, because if I recall correctly when we discussed this when David Weston had a conversation with us at LabsCon last year, Juanito, it is now turned off by default. You have to manually go and turn it on with like proof of presence, biometrics, proof of presence, and some other things, blah, blah, blah. Why are we so worried that it's gonna be turned on if it's off by default?

JAGS (01:26:50.968)
Yeah. Well, that's that was Weston. That was Weston having Weston had to take it over and our buddy like and like he re-architected the whole thing to have like the reason they had to ship me a device and it wasn't just like some, you know, feature that I downloaded on a VM.

Ryan Naraine (01:27:00.814)
Correct, they delayed and right.

JAGS (01:27:12.234)
Is that it has to connect to this like TPM it's running on this like particular sort of VM within the hypervisor. It's not accessible from the other things. Like it's not just some process. Yeah, it basically has to know that it's you like literally on there. And then there's like an API that connects this VM. Like, this is me this way. Wait, wait, wait. This is me paraphrasing from like from Weston's implementation and

Ryan Naraine (01:27:20.984)
Windows Hello has to be in place to look at your face to validate things.

Ryan Naraine (01:27:31.332)
So then there is no risk to have the EDR having to turn it off then.

JAGS (01:27:39.894)
Look, let's assume the implementation is perfect. Let's assume that it is perfect.

There is a part of this where it's like, well, maybe I just don't want you to collect it. You know what I mean? Like the idea that I can have something ephemeral and choose for something to be ephemeral in my life and not to be indexed. Maybe I want to be able to have a deeply personal and uncomfortable conversation with my wife.

without it being indexed and searchable and available for us to once again rehash someday. Right. And I think that that's, I think A, Signal is acting in our interests in an interesting way. I don't know what change around the deployment of Recall.

Ryan Naraine (01:28:19.94)
for some AI to play with it as well.

JAGS (01:28:37.506)
is necessitating this, but this was, I believe your argument, Ryan of like right now we're saying that this isn't going to affect X, Y, and Z, but we all know that, you know, Dave Weston is going to go on vacation one day and some asshole is going to turn it on exactly so that he can get a promotion. And then, and then all of a sudden windows recalls on by default and considering how hard a time.

Ryan Naraine (01:28:50.478)
Some PM is going to turn it on because he's going to get a promotion.

JAGS (01:29:03.096)
Kostin and I and Silas and everybody else have, for example, trying to turn off Windows Defender, trying to turn off sample submission in our VMs, trying to turn off all this bullshit that's like, the track record's not amazing. And look, there's valid reasons for why you don't want that to be easy and so on, but they could have helped us, like they could have made it a little easier for researchers. So I think it's a valid concern.

c (01:29:10.72)
soon plus.

Ryan Naraine (01:29:14.658)
The truck record isn't pretty.

JAGS (01:29:29.846)
I think it also speaks to some architectural decisions that Mac OS has been taken, that Apple has been taking on for a couple of years now around like entitlements and the idea that the user should get to determine not the user should get to determine the applicability of system wide features on an app by app basis, which is like if you, if you're on your iPhone,

And it asks you like, Hey, should, this new app you installed be able to check other local devices on your network? Like that's a feature that's available on your iPhone, no matter what. And yes, they may have a legitimate reason to, but you get to choose one time, one prompt, whether you actually want this fucking app.

to be able to do that. Should it be able to access Bluetooth in order to know what other devices are around? Then you go, no, it's a fucking Angry Birds game. Like why would it need to know the other Bluetooth? Because it's collecting a fuck ton of telemetry and it's stealing and it's selling it somewhere in an ad network. Okay, well fuck you, no. And that's it. But that entails an architectural sense of entitlements that has been getting pushed by Apple.

for several years now across different versions with differing levels of success, right? Like it's not perfect. There's all kinds of like faults to it. People find vulnerabilities in it all the time. It's apparently a fairly easy, well, quote unquote easy way to like make some bug bounty money. Like even just like being able to disclose like location in some trusted...

Context within iOS will probably net you like I don't know five grand fifty grand whatever like you can go do that but it's just to say that macOS and iOS are designed with that in mind and Spot like to your point about triangulation Spotlight has been available on all of our devices for God knows how long I have never seen it index a signal conversation If I go on here and search something from our three buddy problem chat

JAGS (01:31:46.75)
On Spotlight, it doesn't surface anything from Signal. So there is...

c (01:31:50.322)
Thanks God.

Ryan Naraine (01:31:50.552)
Yeah, but that's because Apple intelligence sucks and they have no intelligence whatsoever.

JAGS (01:31:54.35)
it's there but i can't find it right like no look the only the only bridge the only fault in the

c (01:31:54.866)
Hahaha!

Ryan Naraine (01:31:59.896)

right?

The magic in recall is not taking the screenshots. The magic in recall is the recreation of your life that it can do with the AI on the backend and the ability, the kind of telemetry it gives Microsoft to profile you into like exactly who you are. It's just so fucking frightening to me that why would anyone turn this thing on?

JAGS (01:32:17.262)
I think the scare, so here's the thing, right? Here's the scary part of it all is I don't think, while like we all skewered Microsoft for like, the fuck is asking for this, blah, blah. But if you were paying attention yesterday or the day before, a video dropped announcing a partnership between Johnny Ive and OpenAI, which is to say,

Ryan Naraine (01:32:42.148)
company IO, $6.5 billion for a

c (01:32:43.708)
We saw that. Like for what? For Johnny Ive.

JAGS (01:32:45.462)
Which is to build like for Johnny Ive, because I mean, he is pretty awesome. But also like, do you remember, Kostin? Well, actually, history, right? Apple history. When Steve Jobs gets ousted, he goes to Next. They build the most beautiful fucking piece of hardware nobody ever bought. And then they get acquired in order to bring essentially the OS, which is the beginning of like

modern Mac OS for Apple. There's an interesting similar kind of arc here of getting the world's greatest product designer, literal designer of all time to collaborate with OpenAI, a company with Sam Altman during the Q &A that Dave Itell arranged for us. The way he said he pictured their

AI ecosystem is OpenAI is building the OS, the operating system, and other people are meant to build the applications. And that's why OpenAI is not really looking to compete with the folks that are. Can you stop fiddling with these headphones here? We can hear you fiddling. Sorry. I had to get you back, right? Sorry. Well, so the AI... Sorry. The AI shilling was actually to say...

Ryan Naraine (01:34:00.132)
I want to know when did the AI shilling start just suddenly. We went from signal to AI shilling in a heartbeat.

c (01:34:02.961)
Now I need to do something.

JAGS (01:34:12.298)

Open AI is open. No, no, no, no, no, no. This is not open AI shilling. Hear me out. Open AI as of two days ago started talking about making computers.

Ryan Naraine (01:34:12.472)
Not AI shelling but open AI shelling specifically.

Ryan Naraine (01:34:23.106)
Yes, it's a device. It's a physical device. Did you see the interview with Sam Altman and Johnny? Did you see the interview in the coffee shop?

c (01:34:25.777)
they don't say what it is.

JAGS (01:34:25.837)
So.

JAGS (01:34:29.144)
Yeah, I didn't see the interview. no, I, I do.

c (01:34:29.703)
Yeah, yeah, sure. I saw it,

Ryan Naraine (01:34:33.762)
Because they talked about a physical device that that that some Altman claims that he saw and make his revolutionize his brain.

JAGS (01:34:40.012)
So they're building hardware for an AI assistant because it's not.

c (01:34:42.353)
this this

Ryan Naraine (01:34:44.782)
Vaporware bullshit, I got.

c (01:34:46.008)
It had a certain Elizabeth Holmes vibe, if I may say so. That's how I feel it.

Ryan Naraine (01:34:49.732)
Thank you.

JAGS (01:34:49.966)
come on, Johnny Ive gave us the fucking iPod, man. Like this is not somebody who's never built shit before. Like this dude is like, I'm not saying they're going to.

Ryan Naraine (01:34:53.518)
Defend the PNEI.

Ryan Naraine (01:35:01.72)
And he built an applet quarters too, right? He designed the applet quarters that has birds flying into it, that has birds.

JAGS (01:35:05.058)
He designed everything. He brought us the chamfered edge. Okay. The chamfered edge came from. No, no, no, no, no, no. No, I'm not so sorry. Like coasted. Okay. Like coasting.

Ryan Naraine (01:35:12.75)
So you're all in on this Juanito you're all in on OpenAI being a device company.

c (01:35:13.148)
So like honestly, one thing.

One thing I don't need is a shiny silvery thingy that sits on my desk and records everything I'm doing which is exactly like recall in Windows. I don't need that Like this is exactly what we don't need

Ryan Naraine (01:35:23.374)
Ding!

Yes!

JAGS (01:35:29.006)
You leave this Microsoft Recall device alone! Leave it alone!

Ryan Naraine (01:35:34.852)
Finish at point one.

JAGS (01:35:37.646)
Bro, you just described every device we use. This is a shiny metal device, partially designed by Johnny Ive, that records everything I do with my day.

c (01:35:44.678)
that I command not that one that listens like all the time listens to what you're saying.

JAGS (01:35:53.078)
You're wearing an Apple watch. It's recording. It's listening all the time to what you say.

c (01:35:55.213)

I am.

c (01:35:59.066)
My trust is that the NSA put the software on my Apple watch that in addition to the functionality that the watch provides also provides them with information about what I am doing and in this way they know that I am not doing anything bad these days. Not that I would be doing anything bad.

JAGS (01:36:10.626)
They're running ML.

You're, you're doing it on purpose. This was part of our OPSEC training back in 2014.

Ryan Naraine (01:36:17.528)
You guys are

c (01:36:19.74)
Can I read you guys just one line from the Signal Blog? Which I thought was beautiful. It says, Take a screenshot every few seconds legitimately sounds like a suggestion from a low-parameter LLM that was given a prompt like, how do I add an arbitrary AI feature to my operating system as quickly as possible in order to make investors happy? But,

Ryan Naraine (01:36:36.644)
Yeah

JAGS (01:36:46.062)
Wow.

c (01:36:47.703)
More sophisticated threats are on the horizon.

JAGS (01:36:52.31)
Wow.

Ryan Naraine (01:36:57.422)
We are just so headlong jumping into this AI world in a way where we're not thinking about the privacy implications. I mean, it's just startling to me.

JAGS (01:36:57.504)
Bye.

c (01:36:58.393)
And you know it's right.

JAGS (01:37:08.382)
Look guys, I was trying to get at something a little different with the recall thing, right? Like we all skewered Microsoft for recall. And honestly, that was really the first time it clicked for me. And I feel really ignorant saying this, but it was the first time it clicked for me that Apple had already been doing this for us on device, right? With Spotlight, with the pictures or whatnot. No, well, but it's not just indexing.

Ryan Naraine (01:37:30.83)
Well, not the screenshotting part, not the screenshotting part, the indexing part.

c (01:37:32.681)
No.

JAGS (01:37:37.826)
They are running ML locally on your device to describe your pictures and make them searchable. They are running ML locally on your device to do all kinds of post-processing categorization, et cetera, that makes it searchable and indexing that. Now note what I just said. It works really well. It's phenomenal. Now note.

Ryan Naraine (01:37:54.53)
And it's great, it works fantastic too. You can go say dog August summertime, dog August summertime in the mountains and you'll get all your old photos.

c (01:37:57.989)
Cat.

c (01:38:03.099)
Hmm.

JAGS (01:38:06.36)
how I describe that sentence. said they are running ML locally on your device. And that's why Apple has will always get our kudos and continues to get our money, even though they've been fucking up a lot lately. Because to them, there is a priority to having this beyond device to the point where Apple intelligence is a piece of shit, but it's a piece of shit because they're trying to make it work.

with low with with models that you can run on your device. And it's almost right now it's relatively impossible to get the levels of performance that we're getting used to with LLMs with large language models that run on fucking insane GPU clusters somewhere with the same hardware that you for your phone in a memory in an efficient memory efficient hardware efficient power efficient heat efficient way. It's just not possible. So they're trying to figure out how the fuck to do that. And we should stand them like we should we should want Apple to win. I am not about to give them any fucking credit along the way when they're pushing really shitty versions of things, but we should want them to win. Now, the point, the reason I brought OpenAI and the Johnny Ive thing is that you're seeing why Microsoft thought to make recall, which is the vision that Sam Altman has for

OpenAI as the OS of AI is, is providing people with a life companion style artificial intelligence that has access to all of the information of your life, all of your conversations, all of your pictures, all of your calendars, all of your blah, blah. And it, and it knows you so well that it like, it will

Ryan Naraine (01:39:50.948)
Who's asking for this?

JAGS (01:39:59.7)
know to personalize things and take actions on your behalf and make decisions on your behalf and provide you with relevant information without you even asking because it has this massive agglomeration of information, access to all these different things, access to all your different services, identities, passwords, passkeys, etc. Whatever the fuck it is. And it can do that in a really informed fashion because it has access to that. And that requires a certain amount of

insane levels of information codification. Because it's not just whether you're giving them access to your Google Drive. You never sat there and wrote, I am a well-educated person with this background and this is what I like. And on Tuesdays, I feel like eating yogurt in the morning. But then on Thursdays, I prefer eggs. Like nobody's sitting there.

writing this captain's log of who they are and what they do and everything they want to do. So you somehow need to be codifying all of this information about people and by helping them spy on themselves so that it's available.

Ryan Naraine (01:41:05.476)
by spying on them.

c (01:41:11.833)
Why? Why exactly?

Ryan Naraine (01:41:12.804)
Who's asking for this shit, Gus,

JAGS (01:41:15.662)
There's a vision of the future I actually wrote I wrote almost 5,000 words about this on the way back from pivot con I wrote a paper I was writing a paper about Westworld season 3 and 4 and what it tells us about what the vision is for AI in the future and then I never published it because I felt silly

Ryan Naraine (01:41:33.922)

I segment people by if they made it past season 2 of Westworld or if they didn't.

JAGS (01:41:38.062)
Oh yeah, yeah, yeah. You know a human being to their core, whether they made it past season two of Westworld into three and four or not, which is also why I haven't published it. Yeah. And we're still buddies. You know, it's a nine, the threshold is 11, we're still buddies.

Ryan Naraine (01:41:47.446)
I didn't. I didn't. And the people who made it there are publishing 5,000 word papers. So go, go,

c (01:41:57.239)
last season was the best.

Ryan Naraine (01:41:57.262)
So you believe Juanito, you genuinely believe that there's a future where people need this. They don't know that they need it yet. Costin and I don't know that we need it yet, but we will need it.

JAGS (01:42:03.074)
There is a-

JAGS (01:42:07.278)
So I think that I'm about to let me say something completely asinine. Let me just be careless in how I speak, please. I think that there is a vision. There is a vision of the world where we are suffering from tech from from our success in scaling technology over the past 25 years or so on, where what we have enabled is

Ryan Naraine (01:42:19.391)
Let me check the times.

JAGS (01:42:36.974)
Terminal acceleration ism everything in our lives now relies on such an amount of automation that it is running at a speed that we as human beings cannot ever match or wield or appropriately manage because our brains our throughput has not changed at all I mean

Ryan Naraine (01:43:02.062)
Give me an example. Give me a real world example of one of these things.

JAGS (01:43:06.922)
look at just trying to keep up with our careers, like just trying to keep up with the volume of information that is released about AI, about cybersecurity, the amount of hacks that we do, like the amount of breaches, the amount of IOCs, amount of APT tracking. So right, when I started in this industry, which I came at it much later than the two of you, I had to keep up with like,

Ryan Naraine (01:43:21.622)

APT tracking. It's like,

JAGS (01:43:34.06)
I don't know, 70 Twitter accounts and 20 different blogs. And I had time to learn how to reverse engineer on my off time and somehow become competent enough and even get to play in the big leagues with people just a few years after. Doing that shit today is impossible. You could pick a deeper subset of it, but the notion that you could have a view of

everything that's coming out in this field and somehow be aware of all the technology and somehow process all of the samples, et cetera.

Ryan Naraine (01:44:08.578)
It's impossible with the tools you had then. Your argument is that today you can't possibly survive without embracing the AI tools that are allowing you to do this automation and 10Xing your output.

JAGS (01:44:12.694)
Yeah, it's and it's impossible.

JAGS (01:44:18.99)
So, yeah, my, my, my futurist, my semi futuristic picture that I'm trying to, to, put out here is simply that everything we've been doing up until two to three years ago has been an ever increasing ramp up of automation and its effects on human life have been effectively to create an insane, a sense of terminal acceleration ism.

where it's just, it feels impossible because it is impossible to keep up with everything that is relevant to us as human beings. We just discussed our careers and you said, my God, it's impossible to do X. That's just your career. What about your personal life? What about your extended circle of friends, which are now a global empire of people, all of whom are communicating and generating content on 17 different platforms at all given times? I have.

12,000 unread signal messages right now. like, and it's like, 3,500 of them were just from a community that we created in LabsCon and I cannot keep up with. That is without my meetings, my Zoom calls. I have a PA and partial access to an EA and I can't keep track of my own fucking calendar. Like it's just a level.

Ryan Naraine (01:45:37.358)
You need to slow down brother, you're just going too fast right Kostin? Like slow down, go to the gym, get some taekwondo in.

JAGS (01:45:40.43)
But, but, guys, that, fuck you, you think I have time to go to the gym?

c (01:45:43.649)

can ask simple question. Here's a simple question. How can a shiny round device sitting on your desk fix all that shit? It can't. And what can a round shiny device sitting on your desk do better than an app running on your laptop or your phone?

Ryan Naraine (01:45:50.34)
Fix all of that shit for me.

JAGS (01:45:51.406)
no, no, no.

JAGS (01:46:02.146)
Yeah. So the my point here is, is not to defend what is in the immediate future, but to describe that in the medium term future, what AI stands to be is the great leveler, the the change in evaluative throughput that a human being can has access to in order to handle that acceleration ism. When I can go to sleep,

and know that while I'm sleeping, something that accurately represents my goals, my intentions, has access to my information, my credit cards, my APIs to everything that I use is scheduling my anniversary dinner, booking my tickets for my vacation. When I wake up, it will have sorted my calendar so that I actually only have the right number of calls. It answered.

40 % of the emails I had because they were all bullshit, yes, no, blah, blah things I didn't need to look at. It's effectively democratizing the personal assistant. And that's something that I have access to that has changed my life drastically that 99 % people do not have access to.

Ryan Naraine (01:47:13.166)
Are you comfortable outsourcing it?

Are you comfortable outsourcing that super critical part of everything you're being to a private venture backed company that is built on

JAGS (01:47:23.79)
No, that's where you're getting into the parts of this that are deeply uncomfortable. I'm not arguing that I am dying to give open AI the fabric of my life and give them all my information and depend on them to coddle and baby me through life. I'm not saying that I'm dying to do that. I'm saying that for the sake of understanding what is motivating these

bajillion dollar companies to say that this is what they need to do even against public and massive outcry. Massive outcry pushed them not to kill it, but to put one of the smartest people in their company full time to re-engineer it and still push it because there is this vision. Had you watched Westworld season three and four, you would understand.

Ryan Naraine (01:47:57.154)
That's their hypothesis is that everyone will want that.

Ryan Naraine (01:48:21.326)
Never made it. I'm the other side of the coin.

JAGS (01:48:22.99)
that this is essentially the only way to be the 21st century human we always imagine. And look, man, any future, any retrofuturistic vision of what the 21st century was gonna look like always included some AI assistant, blah, blah. Tony Stark didn't sit there and manually build

the Iron Man suit, had this disembodied magical voice that was commanding a factory and clearing his schedule and waking him up in the mornings. bro, just one last bit on that.

Ryan Naraine (01:49:02.776)
This dependence.

c (01:49:05.653)
But what you're saying Juan, what you're saying is that what they need is Carlit Johansson, not Johnny Ive. This is what you're saying.

JAGS (01:49:13.134)
Well, they cloned Scarlett Johansson without paying her and now they can just get Johnny Ive. It's just, and I'm sure Johnny Ive better be careful because they're training a model that designs devices with chamfered edges and narrates videos with his voice. like Johnny Ive will not have any utility by the end of this. It will be sucked out of him and distilled into a model.

c (01:49:20.465)
Look, that's a reality.

Ryan Naraine (01:49:35.822)
Juanito, Juanito, this dependence on private companies is something that's on the list here. I just was looking at the list of things we wanted to talk about today and there's a story here that in February the US imposed sanctions on the International Criminal Court in The Hague,

c (01:49:51.39)
Wait what what what just happened?

JAGS (01:49:53.102)
This is the best! This is so fucking funny! I'm sorry. I'm sorry.

Ryan Naraine (01:49:57.504)
No, in all seriousness, I want to tee up this story. The US imposed sanctions on the International Criminal Court in The Hague. And as a result of this, the chief prosecutor has no access to his emails on his Microsoft account. Why is this so funny to you? This is the dependence I'm talking

about that you're throwing all of this in the hands of Sam and Johnny Ive to have this device that takes control of your life. And then you see all of this to them.

c (01:50:07.828)
You

c (01:50:14.004)
And

JAGS (01:50:17.934)
c (01:50:19.284)
Hmm.

JAGS (01:50:22.125)
Yeah.

Ryan Naraine (01:50:27.396)
The issue here again, the risk of dependence on IT services, US IT services in this case, but just generally, can you talk a little bit about this dependence and how it affects things when politics and geopolitics gets thrown in? Why did you laugh at this story?

JAGS (01:50:43.074)
Well, I left the story for an entirely different reason, which is that I was there at the ICC when Microsoft and the ICC were consummating their union. I saw Kareem sitting next to Tom Burt and they were practically holding hands. Like it's to this wonderful alliance. dude, literally, like it was just this. Yeah, yeah. Well, yeah, for now he's under some pretty.

Ryan Naraine (01:51:05.411)
Kareem is the chief prosecutor who is blocked right here.

JAGS (01:51:10.894)
hot scrutiny for entirely different than what's, no, anyways, for entirely different reasons. yeah, go Google that story. But it's hilarious to me because it was such obvious capture. And I was there, I remember Lindsay Freeman and I looked at each other and we're like, this is insane. Microsoft is hosting an event at the International Criminal Court. There's regulatory capture and then there's just like,

Do they rent it? do they own the space? Like, can we book other events? Can we have, like, is Tom Berg gonna have his wedding at the ICC? Like, what the fuck is this, right? Like, so much, there's no even, not even like a semblance of like independence. And then to see it all kind of like, like, you know, foot gun, right? Like, to just watch it like blow up in their faces. It's like, you're like, okay, sorry. Cool, bro. Like, the fuck. But sorry, you have a broader point.

Ryan Naraine (01:51:56.43)

explode.

Ryan Naraine (01:52:06.404)
Cost in?

JAGS (01:52:09.042)
Ryan Naraine (01:52:10.136)
The broader point is on dependence on private intelligence.

JAGS (01:52:12.556)
Yeah, and it is a really clever segue. This is a brilliant segue that you just because you're correct. And the part look, that's why I said, let me speak recklessly. Let me just say what I think needs to be said as the argument that I see, like the discussion I see on behalf of these people who are making decisions, right? Like it's not, it's not that they're, they're completely irrational and just building shit out of nowhere. This is coming from a concerted vision.

c (01:52:13.48)
Mm-hmm.

JAGS (01:52:42.4)
of what's coming in the world. And what we need to, there's a reason I keep telling everybody Apple sucks right now, but you should support them because they're the only company that's that continues to try and try and try to figure out how to put enough power in your hardware and enough of like logic and requirements to get you.

Ryan Naraine (01:53:07.876)
They'll hand off a lot of it to the cloud though. mean, there's, there's going to be a lot of the resources. The ones that are useful, the real useful ones will be handed off.

JAGS (01:53:12.28)
But dude, but even that, even that, like they didn't just say, well, sorry, I guess we can't do this. So here's an API call and now open AI knows everything you do. They built all this bullshit hardware and all this obfuscating infrastructure and, know, private cloud compute. So I'm saying like Apple might suck right now. And like, honestly, they keep fucking up Bluetooth devices. They keep breaking the AirPods.

Ryan Naraine (01:53:30.168)
this private code computing, right?

JAGS (01:53:42.062)
Pro Apple intelligence is fucking terrible. And yet we should we should support them. God, it's I you want them. They're fucking like you look like a bee. And it has like, yeah, it just yeah, I fucking I bought myself I bought it.

Ryan Naraine (01:53:48.238)
Let's go buy some new devices.

c (01:53:49.34)
How are the glasses? How are? Please.

Ryan Naraine (01:53:55.992)
What the Division Pro thing? you have one of those too? I told you this guy is way ahead of us, Costi. He's running too fast.

c (01:53:58.172)
The Vision Pro.

c (01:54:03.033)
I don't have them.

JAGS (01:54:07.662)
It's like this... the silliest shit. I should have given it to Martin before he moved to Switzerland. I regret that. Yeah, you gotta... So this... I will be walking... In Apple's future, I'm walking around with this like, battery pack strapped to my hip, looking like a fucking bee, you know, wearing this fuck... And this shit, in the most uncanny way, shows you like a pair of eyes. So it's like a wee... And it's... They're not your eyes. It's like this weird...

c (01:54:09.308)
I am.

Ryan Naraine (01:54:13.796)
and you got a big battery pack on your nose.

Ryan Naraine (01:54:20.484)
Gusting.

Ryan Naraine (01:54:30.948)
Yes.

JAGS (01:54:37.396)
Like, it's the fucking most bizarre shit ever, and everyone was like, yeah, that's cool. This, that's-

Ryan Naraine (01:54:41.412)
If you're not watching us on YouTube, Juan is demonstrating his Vision Pro.

c (01:54:44.347)
You have to.

the bee.

JAGS (01:54:48.68)
wait, I haven't plugged the battery pack in. Forgive me, one second. Like, what was I thinking?

c (01:54:51.954)
Plug them.

Ryan Naraine (01:54:53.284)
Custin, you promised me a small, tiny, shiny box. This guy's running around with a battery pack on his head.

JAGS (01:54:57.709)
Hahaha!

c (01:55:00.242)
look that's what I've seen on the internet like the the Johnny I've um Westworld spy device like sitting on your desk the moment I saw it gave me the creeps that it looked exactly like the the evil devices that you see in the movies

JAGS (01:55:00.386)
Well then...

Ryan Naraine (01:55:06.372)
You

Ryan Naraine (01:55:16.034)
Juanito look like he's going up Whistler Mountain for a ski session.

JAGS (01:55:19.478)
Yeah, yeah, I'm hoping you'll see some. Yeah, it's loading up. Yeah, this is normal. This is this is absolutely what the future is going to look like. People will have conversations like this and, you know, sounds fucking great.

c (01:55:21.306)
Any moment now guys, any moment. Any moment.

c (01:55:34.876)
Gonna talk to your girlfriend or wife wearing these things?

JAGS (01:55:37.654)
Yeah, well, not only will you like it doesn't think about it, right? It has no camera view wherein you can have a a vision of yourself where you can actually see yourself, right? Like you so when

you're calling your wife, it thinks it's completely fucking normal to show her like a disembodied Pixar 3D version of yourself.

Ryan Naraine (01:55:46.702)
You gotta see him. You gotta see him clicking his fingers.

JAGS (01:56:06.52)
talking to her as if that's fucking that's what human beings do. It's not in case anybody is listening right. Anyone. I need to set him up like I need to like have it record my face. I'll spend the rest of the episode. Yeah. No.

c (01:56:14.738)
Where's the ice? We wanna see the bee ice.

Ryan Naraine (01:56:20.036)
He'll spend half an hour having to set it up. We gotta move on.

c (01:56:23.8)
I have a feeling that everybody wants to over complicate things and like shiny devices and helmets when in reality What people want I tell you what people want would be a cat a cat that you can talk to and the cat that reads blog posts when you're sleeping and can summarize all the latest threat intelligence news when you wake up in the morning when you

JAGS (01:56:37.654)
Ellis Coast.

JAGS (01:56:49.89)
Hahaha!

c (01:56:51.781)
do an omelette the cat just tells you what's new like all the things that you missed you don't need Johnny I for that you just need the cat

Ryan Naraine (01:56:56.036)
Yeah. The point you're making is that there's a bunch of useful use cases that doesn't require somebody listening to everything you do and putting you in these uncomfortable privacy complications, right? I mean...

c (01:57:04.745)
yeah.

JAGS (01:57:05.089)
What? What?

c (01:57:07.825)
Correct.

JAGS (01:57:11.266)
Yeah.

c (01:57:11.565)
And the other thing which I think it's important that whatever technology must look like in the future, it needs to look human, not a scary, cold, silvery device spying on you sitting on your desk, but the cat that walks around, hugs you, whatever, and tells you what's new.

JAGS (01:57:32.664)
All you're asking for is like the anthropomorphic warm and fuzzy side of this. And I know you're right, but you're going to be, you're going to, well, I'm sorry, Blade Runner 2049, right? Like the fucking disembodied girlfriend 3D thing. If it looks like Anna de Armas, then here, take, yeah. But look, look at, look at the, well, you'll need Johnny Ive for the fancy rich person version of that. What you see in Blade Runner 2049 and what you see,

c (01:57:37.221)
with Scarlett Johansson's voice.

c (01:57:44.401)
Correct, exactly. I thought that was the most realistic. Yeah. But do you need Johnny I for that?

JAGS (01:58:01.576)
in shows like Altered Carbon and all the sci-fi is that it's usually dystopic because you're not seeing what the richest 1 % of a hyper futuristic universe looks like. You're seeing what the trickle down version of that for the plebs and this like the completely disenfranchised masses looks like, including Star Wars. The whole point of like the Star Wars universe is like you're in the outer edges and you're seeing people who have this like

what clearly is very advanced technology living in like a fucking desert in some shithole planet somewhere that nobody cares about, but they have enough autonomy with robots and stuff and AI of some sort that they can survive. And that's like this, that is the most like sci-fi bullshit version of what we're discussing here in that what we're now talking about is an asymmetrical increase in autonomy.

and the ability to function and do more by yourself. However, Ryan's point is extremely valid. At this time, what we have gotten with the transition from mega tech corporations to basically mega ad corporations to mega cloud corporations and this like...

techno feudalistic version of the world is one where we all have to rent our way to that future. And that is where it gets kind of terrifying because in the Apple world, they weren't, sorry, in the

Star Wars world, they hopefully were not having to spend galactic credits so that the AI continues to work until the fields or they starve. And that is the future that we are.

setting up in the immediacy, which is I can function as a human being at top speed and top capability as long as I can pay Sam Altman $20,000 a month. And the minute that I can't, I am just as fucked as everybody else. And it's it's scary like that. No, I agree with you, right? I agree completely. Moreover, the reason I wrote all that shit about Westworld that nobody has to read is that

Ryan Naraine (02:00:08.068)
Your intelligence drops. Thank you.

JAGS (02:00:21.762)
There are further implications about this notion of codifying what the human being is in some electronic fashion. Cambridge Analytica and Facebook crisis of 2016 and so on was about the fact that it turns out that if you get enough psychometric data about a human being through their casual interactions with technology, you get a pretty horrifyingly accurate

perception of who they are and what they need. And apparently it's okay to do that when you want to sell fucking, you know, I don't know, baby toys to somebody that hasn't even realized they're pregnant yet. Okay. But it cool. It's, it's, it's scary when you then consider what those companies are willing to do and what they're willing to be party to. Facebook was, was perfectly okay with being party to a couple of casual genocides. Like it happens, right?

So what are they doing with that X-ray of who you are that we're not ready to accept as human beings? We're not ready to accept that enough of those stupid quizzes and enough views of how you click on things actually let somebody codify a pretty good profile of who you are and what you choose.

And that was Shoshana Subov's point in the age of surveillance capitalism. We've broken capitalism because there's no such thing as the invisible hand when a company not only can preempt what you like, but also redirect you to things you didn't know you wanted. Because in fact, you did not want them until they made you want them. So very weird world. Anyways, let's talk about cyber.

Ryan Naraine (02:02:03.158)
you that you needed it.

Ryan Naraine (02:02:09.252)
Good luck in your work.

c (02:02:09.566)
Some would even argue that we no longer live in capitalism, but what we live is techno feudalism.

JAGS (02:02:16.734)
as Janis Varoufakis very astutely has said, and he especially focuses on cloud capital. You have built this notion of cloud capital where people are... You need to read the book. mean, honestly, I'm not saying that it's... I'm not saying it's totally accurate, but there is a really important point here, and you can't just dismiss it as Europeans being sort of communist-y. Like, you need to actually engage with this discussion because it is...

c (02:02:31.31)
Yeah, it's worth it's worth.

JAGS (02:02:46.211)
That like we're hearing that from the outer rim. We're hearing that from Europe, but that shit is being built in America. Techno feudalism is American, right?

Ryan Naraine (02:02:54.596)
They are sort of... They are sort of communists.

c (02:02:56.238)
in the meantime in the meantime prosecutor prosecutor Khan moved to proton mail a swiss email provider like we can of course talk about all these fancy futures but when we come down to earth he had to switch to to proton mail which to me i think it's a very powerful lesson like of course everything's fine until things are not fine anymore

JAGS (02:02:59.479)
I love that shit.

JAGS (02:03:27.54)
so many things to say about that, I think we should probably.

Ryan Naraine (02:03:30.478)
We're way past the two hour mark and I just got one small story I wanted to touch on, maybe not for too long. Japanese, Japan actually passed a law, a new active defense law, cyber defense law that allows for offensive cyber operations. Right in your wheelhouse, one E to release the guard rails. This law explicitly allows law enforcement agencies to infiltrate and neutralize hostile servers before any malicious activity has taken place and do so below the level of an armed attack and so on.

c (02:03:34.733)
Only one. Only one.

JAGS (02:03:36.792)
Just one?

Uh-huh.

Ryan Naraine (02:04:00.632)
This is Japan actually codifying its ability to do quote unquote offensive operations, hack back in preemptively, defend forward. Something you welcome, something you expect to see some motion here? Is this something that is a precursor to what we'll see around the world? What do you think?

JAGS (02:04:07.512)
preemptively. It's like defend forward.

JAGS (02:04:20.238)
I am really in, first of all, fucking dope Japan. Like I think it's cool. I'm dying to go to Japan this year and kind of like, well anyways, I hope to have a good excuse to go to Japan this year. I'm really excited about this mostly because if the Japanese can argue that this is a valid use.

projection of quote unquote cyber power, a nation that literally has like a pacifism core tenant in their constitution. I think what you're seeing is a parsing out away from the bullshit militarism and militarization of cyber as a domain, which is, know, as a domain, even calling it a domain is a militaristic term for something that

Ryan Naraine (02:04:51.396)
institution,

Ryan Naraine (02:05:13.144)
First time I heard that it was, who was it, Costin?

JAGS (02:05:17.976)
Hayden.

Ryan Naraine (02:05:18.724)
Matthew Hayden at our event when he said we are number one. That was the first time I had heard him kind of segmented as a domain and I realized this was how the military was looking at it.

JAGS (02:05:20.664)
Michael.

Yeah, yeah, yeah.

JAGS (02:05:28.556)
Yeah, there is a, so there is a really, really interesting master's thesis by a gentleman, Wiener, Craig Wiener, who talks about the fact that like, God, we've gone for so long on this podcast, my

headphones just died. He's, he's talked about the fact that the rise of CNO, of computer network operations, has to, it was not

For once, it was not a major military innovation. It's an innovation bred from the intelligence community. And it means that we have not known how to categorize it, how to inject it into how things work in our government and so on. So the way that it was done in the early 90s was for existing organizations to find ways to essentially

finesse the language into making cyber fit into the existing power structures. So NSA wanting to keep cyber for themselves and not letting let's say CIA or whomever else take it, they said, well, our remit is about signals intelligence, then cyber is about collecting signals at rest. And you're like, what? And it's like,

Yeah, signals at rest, bro, obviously. That's what that is. And you go, the fuck are you people smoking? But like, it's about essentially finding a way to fit it into the existing thing. So for the military side of things, because a lot of this started with the Air Force and so on, is like, well, cyber is another domain. know, it's the air, what is it? Land, sea, air, space.

Ryan Naraine (02:07:26.116)
Cyber.

JAGS (02:07:26.166)
cyber. And that's what that's what Hayden says, right? Like he puts his hand up, he goes, you know what, and so cyber is a domain, which means that that's why you get cyber command. And that's why you get, you know, the Air Force, the same way the the that like, the Navy has planes, because it has to be able to defend itself and so on. And you know, in these correlated domains, then then you also have to have cyber. The problem with that is, okay, that got you through the bureaucracy.

c (02:07:26.667)
cyber.

Ryan Naraine (02:07:30.434)
and check them off.

JAGS (02:07:55.072)
of the 90s into the 2000s and people kind of embracing this brand new thing, but it actually has warped our ability to properly describe cyber in a way that makes any fucking sense. And that's actually an argument I made at SummerCon. I spoke at SummerCon two years ago and had this kind of like...

drunken rant against the whole like cyber power index that the Harvard Belfer Center had put out because cyber power is a nonsensical corollary of thinking about cyber as a military domain.

It makes no fucking sense. First of all, how can you have an objective metric of cyber power when cyber power is a relative measure? We have great cyber power as a country.

Okay. And when you go fight a nation that is entirely undeveloped, how much cyber power does the US have? you know, you're exactly. then you actually have no cyber power. is a relative measure. So that was part of my argument there is just to come back to this notion of like, we have over militarized it for the sake of bureaucracy. And in effect, we have somehow bureaucratized cyber and

Ryan Naraine (02:08:57.944)
There is no cybering to do,

JAGS (02:09:17.226)
a nation like Japan that has a fundamental tenant for pacifism, basically saying, fuck off with that. We need to defend ourselves in cyber, and it is not a way of militarizing cyberspace. It's just some common sense measures for the sake of defending yourself, I think is a great exercise. I want them to succeed. My thing here is going to be, what do they do with it? And because the biggest problem that you'd get

is not that they use it poorly or that they use it effectively, but that they don't use it at all. And that's what we keep seeing with all this shit. At the end of the day, what ends up winning is doing nothing. And like we're spending billions on cyber capabilities that we don't use and they just rot on the shelf.

Ryan Naraine (02:10:00.388)
How is this different, how is this different neutralizing hostile servers and like the kind of things they describe here different from what the Lumen and FBI and Microsoft does with all these takedowns and these neutralizing of servers and sinkholeing servers and so on. This suggested there's more, this suggested the Japanese are clearing the way to do more than that.

JAGS (02:10:26.636)
Yeah, yeah, absolutely. Because first of all, the important difference is that it's the government doing it a B that they can do this. The kind of things that we were discussing earlier where you go. Well, we we can't we don't own this infrastructure. It's vulnerable. We're going to hack it. Boom. Done. Right. Like what we were talking about with the event where I joke that somebody should

do bricker bought their way through all these vulnerable appliances. Obviously nobody wants that. That's not an actual desirable outcome, but it is.

Ryan Naraine (02:11:02.724)
And he was joking. didn't want like some people clips that and have Juanito calling for the breaking.

JAGS (02:11:08.12)
Bro, I don't control. Look, if I call for the bricking and then somebody does some bricking, the idea that I did the bricking is beyond us. think if you think that I'm more responsible for all those devices getting bricked than the people who could have kept them from getting bricked, you have a fucking problem, a variety of problems. And they have to do with the bureaucratization of cyber that we're discussing right now. Again, protect the babies, careful with the respirators. my God.

you know, what if you restart that router for 15 minutes is an extension of this notion that like we treat it as if somebody leveraging an exploit and turning off a device is the same as like a JDAM being dropped on a building. And those two things are just not comparable by any normal stretch of the imagination.

Ryan Naraine (02:11:57.732)
Costin, take the last word on this story. Does this give you, this is...

c (02:12:02.313)
I think you're looking at very nice people, the Japanese through the eye of the mighty American Eagle and thinking that they might be doing or approaching things in a very American way, which in reality, I think it's not the situation here. Making like drawing a parallel between the Japanese and Romania because they like that.

JAGS (02:12:12.632)
Come on!

c (02:12:28.399)
Romania was being infiltrated by Russian drones over and over and the Romanian army couldn't do a thing because there wasn't any law which allowed them to shoot down unmaned aerial vehicles like drones unless it's a time of war so in a time of peace we have to let them fly and the Russian drones were just flying valiantly and happily through the Romanian airspace

Unless of course there was a law and they did actually vote a law which now allows the remaining military to shoot them down and I think the Japanese pretty much approach things in the same way. They want to do everything by the book. they need first of all they need the law which gives law enforcement agencies the right to neutralize these servers. How do they neutralize them?

Well, of course, I guess that that depends on a case by case basis, but in my experience, they've already dealt with cases when they had the means to neutralize the servers through an exploit or whatever. However, the legal part was missing. So I think that the Japanese are just trying to essentially fix this legal issue so they can actually

take care of the problem and stop the malicious cyber servers fly through their cyberspace unattended and just shoot them down.

JAGS (02:13:59.788)
You see, you see the problem with the militarization thing. It's not their cyberspace. It's just one giant miasma of servers. It's not just shooting them down because you, what does that mean? Right? Like what if the malicious servers are being hosted by Microsoft on Azure in an American data center with an IP that comes out of Bulgaria, but you are in Romania and you.

are being attacked by this traffic, but that traffic's actually being amplified through a CloudFlare server, which is this miasma thing of like everywhere it's connected, because the physics of this shit just don't fucking work that way, and none of this stuff makes any sense. But also because somehow you can't compel the people who own the infrastructure to enforce stuff. Like that Luma Stealer story, it's like, that's cool. Thank you guys for like doing this take down. But also like, why does any of this work this way? Right? Like why?

why we have to pat ourselves on the back because a few private sector companies decided to do a thing and I'm grateful to them that they did it, but it does not make any sense that this is the way that it has to happen. And it's this bizarre overextension of the idea of geospatiality to cyber, of the idea of ownership and rentiership and responsibility, regency, over your

cap cloud capital in cyber. If there's somebody running a malicious server that's attacking other people on Azure, why do we have no recourse to tell Microsoft to turn that shit off or redirect it? Or how about you go grab all the malicious stuff that they put in there and tell us what other servers these people bought and how they bought them. And we actually do something about this. But like Microsoft can do it. Microsoft will do it.

Ryan Naraine (02:15:47.15)
Shout out, shout out to the.

JAGS (02:15:51.22)
If you if they feel like it and and when they don't feel like it, they don't feel like it and you go, well, we're.

Ryan Naraine (02:15:59.886)
Shout out to the Japanese for doing it by the book and not having a free for all.

JAGS (02:16:04.898)
Look, let's see if they can do it. I hope they do it. I want to go there and congratulate them myself.

Ryan Naraine (02:16:11.428)
Quickly, Costin, let's close the show with some shout outs. It's been two hours and 16 minutes. Pretty long episode. All the long episode people, you're happy. The long episode people are happy. Let's close the show quickly, Costin. What do you have?

c (02:16:16.136)
Cool.

JAGS (02:16:16.974)
People want a four hour episode, man.

c (02:16:19.698)
Well,

c (02:16:23.315)
I was thinking we need to start like a is it called a curse jar like whenever you drop a penny whenever you say but we do it like we call it an evanti jar so whenever we say evanti we drop a penny in the jar we're gonna do that for the next episode so shi-

Ryan Naraine (02:16:34.797)
Yeah

JAGS (02:16:39.278)
Ryan, can you close this shit out? I'm sorry, Kostin. No, no, but like without covering the fucking Project Raven redux story, with that. No, it. There's a three hour episode, man. Three hour lightning talks. But Petra Kucha, Petra Kucha, Petra Kucha, 20 by 20.

c (02:16:42.108)
I can't. I can't.

c (02:16:48.614)
and Kareto no Kareto Let's do how is it called like lightning talks lightning talks 15 seconds 15 seconds for the project ravel 15 seconds

Ryan Naraine (02:16:51.916)
I have, I have like ten other things on the list. We're at two hours and twenty minutes, you guys.

we'll get to it next week.

Ryan Naraine (02:17:05.732)
15 seconds. Let's touch, let's touch this UAE thing quickly, quickly. Kim Zeta wrote a story on her zero day.com, zeta-zeroday.com website that former workers of the Department of Defense digital service, blah, blah, blah. Some folks who resigned from the DOD post, DDS post Doge as a response to Doge and the Department of Government efficiency efforts.

c (02:17:07.366)
15 seconds.

JAGS (02:17:24.61)

DDS.

c (02:17:25.286)
dodge?

Ryan Naraine (02:17:34.476)
are now being recruited by United Arab Emirates folks to work on AI for their military. You mentioned Project Raven Redux, which was a previous episode where the Israelis were recruiting Americans to go do some offensive security operations there. What is the significance of what Kim wrote about here? Why do you want to talk about this story?

JAGS (02:17:44.334)
Blah, blah, blah.

JAGS (02:17:58.818)
You want to take a custom there?

First of all, because it's fucking hilarious on a variety of levels. Second of all, because my understanding is that the DDS people are actually really talented. Like they are actually people that you will regret not having. Yeah, like this is not just like, some random IT dudes that you can just kind of cycle through. So that. Yeah.

Ryan Naraine (02:18:18.617)
Losing.

Ryan Naraine (02:18:26.83)
So there's a real story here that there's a bunch of really, really talented people who are no longer with the US government because of Doge, and now they're in play, and they're some international folks.

JAGS (02:18:32.086)
Yeah, yeah, yeah. Not only are they in play, but then some mysterious person from the UAE shows up, like quite front-facingly reaches out to the department, basically being like, can we get contact with these people that just left and then go and offer all 30 of them a job in the UAE?

Ryan Naraine (02:18:58.628)
We're best friends with the UAE now though, right?

JAGS (02:19:01.812)
sure, except the reason I said Project Raven 2.0 is that the subtle subtext, the not so subtle subtext of how this is being described is that the concern is that this is basically for G42. Like the

Ryan Naraine (02:19:18.856)

G42A is this United Arab Emirates company that's been kind of mentioned in some Senate papers and some papers around around alleged work with China's government and intelligence service. So there's like some complications there. Help me understand what Kim is reporting.

JAGS (02:19:28.558)
I mean, it's been mentioned in this podcast.

JAGS (02:19:38.572)
Well, there's some complications there in that there's a lot of discussion about G42 being involved in some not amazing things like the Toetalk chat app surveillance thingamabob and the fact that the CEO was previously running Dark Matters, supposedly, allegedly Dark Matters Pegasus unit. And so there's all that.

I would like to also remind folks here that as of last year, thanks to a billion dollar investment, Brad Smith sits on the board of G42, if I remember correctly, I believe so, which is part of the discussion of like, were we bringing them into the fold or is Microsoft just happily playing whatever side it wants on this? And to then see this like,

Ryan Naraine (02:20:21.112)
really?

Ryan Naraine (02:20:33.859)
interesting.

JAGS (02:20:37.202)
The reason I brought up Project Raven is not to stigmatize the CEO himself, but to say like, this sounds really fucking familiar. Like this already happened in the UAE where you had a unit of people with like cyber point with a legitimate contract to help them set up this like, and like counterterrorism unit in the UAE that turned into a infamous hacking unit brilliantly reported by the Reuters guys.

that we are told what's turned against Americans and other folks, right? Like, so it isn't like just a casual, ha ha, well, I guess we lost some talent. They're gonna go work and like have a great time out in the Emirates, which I'm sure they would, but.

Ryan Naraine (02:21:22.414)
But don't these talent tree, like shouldn't these folks have the option to go work wherever they want to work? Like why?

JAGS (02:21:28.088)
Sure.

c (02:21:28.098)
Why did you fire them, yeah?

Ryan Naraine (02:21:39.16)
That's what we did with Project Raven though. We kinda demonized those folks.

c (02:21:50.564)
15 seconds.

Ryan Naraine (02:21:52.236)
I know, that's why I didn't want to start this. I knew this would go down in a pot. No, no, no, go, go, go at this. We're all in now.

c (02:21:55.396)
What if we save it for the next episode?

JAGS (02:21:56.735)
right. You want to just cut it? Like, we'll just cut it here. Yeah. No, no, no, fine. Okay. Yeah, fuck it. Let's just leave it for the next one.

Ryan Naraine (02:22:04.014)
Now we're invested. I'm invested now. You can't do that. Give me the 10 minute version. Let's close in 10 minutes.

JAGS (02:22:05.838)
Now you want, all right, fine, fine. Fine, we'll do it live. So the interesting thing on the Project Raven side is actually the dynamics of how this comes about. And it's why this is not that dissimilar right now, though, admittedly, we don't know that these people are gonna go to the UAE and be doing nefarious things. Let's not malign them, right? But what's similar is...

c (02:22:09.185)
One minute, one minute.

JAGS (02:22:30.488)
There was a contract to do a thing in the UAE that was approved by the State Department and they were supposed to be helping the folks there learn to do this CT stuff. they admittedly, the Americans were not supposed to be running the ops. They were just supposed to be supporting their counterparts in the UAE, training them, et cetera. And then out of nowhere, that contract for whatever reason gets canceled. And the Americans that had been supporting get offered these like

spectacular jobs. And then where the big difference is they're no longer tethered by American, at least in their thinking, the American laws and the American guidance is what they could and could not do. And that turns into this Project Raven thing where now you're hacking whomever, right? You're hacking iOS devices and there's implications that allegedly Americans were hit in that process and so on.

Ryan Naraine (02:23:01.764)
Practitioner roles.

JAGS (02:23:29.73)
That's what makes it turn so kind of nefarious. But note that the people who turned to go work for Project Raven can claim that they did not know that this was not allowed, did not know that this was not appropriate. The people who take this job now are in a... Well, you're in a post-Raven world, so I'm curious how many people accepted the offer.

Ryan Naraine (02:23:49.368)
You hear AI and military.

JAGS (02:23:59.04)
And some of those people, mean, look, you just took their fucking jobs away. Maybe they don't feel like they have much of a choice. And that's not to say that they're going to show up there and break the law immediately or anything like that. But it's also in a much harder situation where they have to admit, well, there is a history of this turning into some kind of wrongdoing that will be prosecuted by the FBI at some point. So what do you do? Right. Like this is a much different situation.

Ryan Naraine (02:24:23.256)
This is your guidance to those folks to avoid that.

JAGS (02:24:26.678)
My guidance to these folks is just to be really fucking clear on what they want to be doing and where their lines are and when they choose to walk away. And frankly, if you have to surrender your passport to be there.

Ryan Naraine (02:24:42.68)
red flag.

JAGS (02:24:43.246)
I mean, that's not a red flag. is human trafficking adjacent. So like fucking figure out what the fuck you're doing with your lives. Like that's all I'm saying.

Ryan Naraine (02:24:48.438)
All the Flags!

Ryan Naraine (02:24:53.678)
Gustin, got a thought on this? you been tracking and following? Practicing. Cyber Peace Institute will come and save us all.

JAGS (02:24:55.404)

Maybe you can ask Brad Smith what they should do.

c (02:24:59.746)
I am not buddies with Brad Smith so I can't ask him personally. I have a lot of thoughts but I think we're out of time so why don't we just continue this story the next time because again what's the most valuable thing in a story in my opinion? Iox. And there's no Iox yet. When there's Iox let's go back and revisit it.

JAGS (02:25:09.771)
Aww.

Ryan Naraine (02:25:10.498)
There we go. Play with the cat.

Ryan Naraine (02:25:20.324)
No Iox, story.

JAGS (02:25:20.526)
Yet.

Ryan Naraine (02:25:27.012)
Do you have any shoutouts or plugs or hellos for anyone?

c (02:25:29.41)
Shoutouts to our good friend Florian Roth for calling out things for what they are. know shoutouts to my good friend Alexander from the UAE where he works for a very legitimate company not this kind of other things that we've been talking about. And of course to all the people we've seen recently at conferences I know this week was a week of BotConf unfortunately I couldn't go there.

But shout-outs to all our former colleagues who were there having fun. I hope they're enjoying and Hope to see them maybe another year next year

Ryan Naraine (02:26:11.268)
Just from my side that's accounted to cost in shout out to you Val Gordon for holding the fort Holding the fort and keeping these people honest Juanito you close the show quickly with some last words

c (02:26:16.46)
Ha ha.

JAGS (02:26:22.434)
okay. So first of all, I, and you're going to hear me ad nauseam on this for the next few weeks. just saddle up people. the labs con CFP is open. Now's the time to send us some dope shit. I

don't, I do not want to hear from you on June 25th, telling me what an awesome talk you had and you wish you had submitted it.

Ryan Naraine (02:26:39.512)
closes on June 23rd.

Ryan Naraine (02:26:49.058)
We're pretty strict with deadline too, so.

JAGS (02:26:50.838)
Yeah, we have to be because also anyways, we have to be.

Ryan Naraine (02:26:57.412)
Your AI should see, you.

JAGS (02:26:58.118)
Windows this this fucking Windows device is now like insisting to be just okay What it is it All along it has thoughts it didn't like me talking about Brad Smith. So the also folks Who reached out for sponsorship after the last podcast? Thank you so much and anybody else who's interested like now's the time obviously we'd love to have the support There's a lot of people kind of going through some harsh economic headwinds. So

Ryan Naraine (02:27:03.598)
Cause then it's listening time.

c (02:27:03.745)
He was listening all along.

JAGS (02:27:27.37)
We definitely welcome it to keep the conference the way that it's been. thanks to all the folks who already sort of supporting us. Yeah, CFP is open. Invites have already gone out to alumni. Invites will go out to folks that are starting to request as of, I believe, 10 days from now, or less, probably a week from now. Beyond that, shout out to my friends in the AI Sommelier Society. We will be having our monthly meeting this Sunday, which should be a fairly interesting time.

Ryan Naraine (02:27:57.646)
drinking wine and chilling open AI shit.

JAGS (02:27:57.77)
just, just talking shit. You know, I don't drink wine, but I will be talking shit about, about AI stuff. Well, we, it's the, we're so, we're experts for models, bro. You have to taste like the fruity earthy tones of 03. no, and, I mean, I, one can only wish he would be offended by the poor aesthetics of my place.

Ryan Naraine (02:28:04.716)
You Somalia, I thought you would have like a wine, wine.

Ryan Naraine (02:28:15.172)
Justin make it stop please.

c (02:28:17.679)
Will Johnny Ive be present?

JAGS (02:28:25.526)
But the last thing, one, what? Yeah, go.

Ryan Naraine (02:28:26.744)
Wait, I want to add one thing to your LabsCon thing. Wait, wait, before you go on, I wanted to like give a head a shout out from the sponsorship side that you mentioned to the folks at Framework who donated the laptops for our best speaker prizes, those amazing laptops. They've committed to doing it again. Shout out to Framework. Those guys are amazing. Cisco Talos and Luta Security. You mentioned Katie Massour, Luta Security and those guys have all been big supporters of ours. And I think it's important to mention and tag them.

JAGS (02:28:40.0)
god,

JAGS (02:28:55.116)
Yeah, no, we're thrilled to have everybody back and hopefully to expand that circle. The last shout out is my way of kind of sneaking a story here in a way. But shout out to our friends at the NSC, Alexei, JD, and who I'm not saying they were involved in this, but whoever at the National Security Council heard that NSO was coming to town to ask them to get removed from the entity list and told them to pound sand.

c (02:29:22.625)
you

Ryan Naraine (02:29:23.448)
I saw that.

JAGS (02:29:25.08)
Thank you to our friends. We're very proud of the work that you're doing. We appreciate that you're holding the line out there.

Ryan Naraine (02:29:31.716)
There's a great line in that story. The company came to the US for a meeting and apparently the whole idea was that they were going to ask the Trump administration to remove the blacklist and

some of the sanctions activity. the quote there was the company was not forthcoming in its motives for seeking the meeting. So they were turned away.

JAGS (02:29:49.858)
Just, you know, I think we need to give credit where credit is due. Thank you to our friends that are out there holding the fort.

Ryan Naraine (02:29:57.11)
And another story we never touched was that the fact that the NSO was ordered to pay nearly 170 million to WhatsApp in that lawsuit. is a throwaway story that's been on our list for a long time. So shout out to those guys.

c (02:30:06.323)
Mm-mm.

JAGS (02:30:08.054)
I assume they flew over here to deliver the check or something. That's what they were probably looking for.

Ryan Naraine (02:30:11.843)
Absolutely. Anything else?

c (02:30:16.207)
And the other thing, how did we not talk about the story that AJ dropped? About the tele message, hip dumps?

JAGS (02:30:22.328)
Which one?

Dude, look, this idea that we can't have a three hour episode is some corporate bullshit is what it is.

c (02:30:31.455)
Hey

Next episode, shoutouts to AJ for an amazing story.

Ryan Naraine (02:30:39.47)
Thank you folks, it's been great. are two hours and 30 minutes in, which is the perfect sweet spot. Whatever we miss, we miss. Now I'm not fucking listening to any of those folks. What we miss, we miss. What we talk about is what we talk about. Sorry.

JAGS (02:30:45.294)
Until we get a Spotify contract like Joe Rogan, then we will be having our five-hour episode.

Ryan Naraine (02:30:56.974)
Thank you gentlemen and we'll catch you guys next week.

c (02:30:59.719)
Yeah, bye.

JAGS (02:30:59.79)
Thanks, guys.