Episode 67: The Three Buddy Problem

Apple Exploit-Chain Bounties, Wireless Proximity Exploits and Tactical Suitcases

Cast:

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

Costin Raiu (00:00.335)
Bye, life.

JAGS (00:00.734)
No, we can make all the mistakes we want. There's a- not unlike YouTube. Everybody's there just comp- why- why are you talking shit about Tavis, man?

Ryan Naraine (00:01.26)
You sure we're not live? Hello.

Ryan Naraine (00:10.786)
Hello everyone, this is Ryan Naraine and this is episode 67 of the Three Buddy Problem, hanging out with my buddies, Costin Raiu out in Bucharest, Romania. What's up, buddy?

Costin Raiu (00:20.644)
Hey, round number 67 is the first prime number after 64, which is our number.

Ryan Naraine (00:27.16)
Who's gonna say six seven? Six seven. Do you guys not know this meme? Or meme or whatever it is. okay. You got homework to look up six seven. Ask your high school kids what six seven is. This is so stupid. Anyway, welcome aboard to the podcast. We have a lot of things to get to. I wanna start with my buddy Juanito.

Costin Raiu (00:29.029)
No, no, what is it? 6-7, yeah, okay.

JAGS (00:30.624)
Six, seven. No. We're not hip or cool.

Costin Raiu (00:43.559)
yeah, yeah.

Ryan Naraine (00:50.19)
is just back from Offensive AI Con, which is Dreadnought's first shot at an invite only Offensive AI Con. What was the tone there? What was the big takeaway?

JAGS (01:01.654)
honestly, they did a phenomenal job. like the Dreadnose folks are friends. They're, they're, you know, they're friends from, from labs con. They've sponsored us the past, you know, three years. and, we're very cool about sort of putting this thing together. kind of taking on the same model as labs con is sort of like the, days, the invite onlyness and whatnot, but very much making it their own, like it, which was very,

Ryan Naraine (01:27.8)
Shartox.

JAGS (01:29.878)
So actually the talks were longer. um, the, the vibe was much more like beach Bummy, which I think is more like kind of like Dreadnode, right? You're in the San Diego beach sub or people were surfing. Like instead of hiking, people were going off to surf, uh, after, which was, you know, it pretty cool. Um, much more relaxed in like the parties were not as like hardcore, which actually meant folks were

Ryan Naraine (01:40.93)
whole San Diego video.

JAGS (01:56.914)
having a lot more conversation. Look, I think it worked really well. I really enjoyed it and the invite list was much more appropriate for the topic, right? A lot of the AI lab folks, the people who working on like AI red teaming and some of this tool development. So it was great. I'm actually really looking forward to the next one. I mean, this was pretty flawlessly executed on their part. So, you know, a lot to look forward to there.

Ryan Naraine (02:24.898)
The flashy promo was a panel with Dave Aitel, Perry Adams, former DARPA AIxCC, and Rob Joyce from the NSA. What on earth did they talk about? Was this on the record, off the record? Like what was that panel about? It was the flashy kind of promo thing. I saw a couple of pictures on the internet and now I wanna know what they talked

JAGS (02:41.055)
Yeah.

JAGS (02:44.781)
I think, so if I remember correctly, all of this was with Chatham house and I, so I'm not going to go too, too into all of it. Yeah. But, more than anything, I thought it was hilarious because you had, you had Rob Joe is sort of like giving like a very measured, like very measured responses and then Perry making fun of Dave, I tell the entire time, and sort of them riffing on each other. So it was a good conversation. Look, what I, what I'll say about the overall discussion.

Ryan Naraine (02:49.72)
I'm like, I hate this shit.

JAGS (03:12.833)
is it was really interesting to hear AI being discussed more as what I consider sort of applied AI and a lot more discussions about like, look, this works, this doesn't work, we tried this, this was great, this does not work at all. And...

Ryan Naraine (03:31.062)
all focused on the offensive front, entirely on the offensive front.

JAGS (03:34.342)
almost entirely. But what I'll say is it wasn't offensive in the way that if you go to offensive con, we're just talking like vones and exploitation. was more like there's a lot of automating tooling for red teaming, automating tooling for quote unquote offensive operations. But the subtext is largely defensive. You're basically saying, hey, we really want to automate

You know, vulnerability discovery, we really want to automate, um, you know, reaching feature parity with bloodhound, reaching feature. Like how do we test things so that we're basically, um, able to conduct red teaming ops in a, in an autonomous fashion where you actually have a good sense of whether you're accomplishing anything, right? Like think about it right now, you're running this shit by the numbers.

How do you say, yeah, the AI agent used these tools and it actually got through to this domain controller and it found these credentials and it did this, that, and the other, right? Like you have to find, like the thing with AI is part of this is it becomes a matter of like how do you effectively verify that the thing did what you said it did so that you can then do a hundred runs, a thousand runs and go, this model does better in this way and not the other.

So it's almost like formalizing a lot of the ops in ways that I think are, were really interesting to listen to. And then you get into the sweet spot. And this is where I think Dreadnode did an amazing job in like their talk. What was it? Shane and Nick Landers did this talk on the second day. was like super understated, but they basically showed,

Not their platform. think they're way too shy about showing off their platform. Like they don't want to like be salesmen, but like they didn't show their platform. They showed the results. And at one point they quietly were just like, yeah, by, doing it this way, by tuning it in this way, we got, I think it was like an eight billion, like an eight B parameter model, which is fairly small to outperform one pro in these operations.

JAGS (05:54.794)
And then you go, excuse me, right? Like in just the management of the entire sort of like chain. So essentially what, for those that don't know what like Dreadnode sells and I swear I'm not a salesman for them, I'm just a fan. Well, I'm just, dude, I'm excited about their shit. I honestly think they need to push it a little harder because what they're doing in my mind is a hedge against the inherent

Ryan Naraine (05:55.007)
in specific things.

Ryan Naraine (06:08.759)
Yeah, you sound like a pitch man here now.

JAGS (06:23.551)
position that the frontier labs are in to scam all of us. And I think Anthropic has recently showed how willing they are to do something like that, right? When they, when Anthropic quietly degrades the model that you're using, doesn't tell you and then still charges you the same amount or still puts you on the same quote unquote plan. As consumers, we're effectively just fucked, right? Like what way are you supposed to say, you know, this would be the equivalent of like,

Ryan Naraine (06:51.007)
You're singling out on Tropic, but this is across the board, right? I mean, how do I know that when I punch something into chat, GPT, it's the thinking model versus the auto model. mean, in the background, they're doing whatever they want to

JAGS (06:59.667)
Well, look, it may be across the board, but I'm singling out Anthropic because it became apparent with Anthropic and I personally experienced it with Anthropic. So I'm gonna give Anthropic as much shit as I can in this process.

Ryan Naraine (07:11.607)
But at a general sense, this is how this stuff is built. Now it's built that they have all the control to kind of shift you around from model to model based on like power patterns and usage.

JAGS (07:19.335)
And this is where you get something really cool with what Dreadnode has put together, which is their whole thing is to create essentially recipes for testing. the idea being, I love the way they

framed it. They were like, look, models age fast and models are gonna keep coming out. And the idea is essentially,

How do you know that you're consistently getting the results from a model that you need to be getting in order to get reliable results from what is a non-deterministic system? Like as it is, if you're developing any kind of tooling and it has to be reliable, you need some kind of testing harness and evaluations and so on to be able to say, this thing will give us more or less the right answer in 94 % of cases. Great. Now I ask you,

If you like, Gabe recently described me as a maximalist. If you're like me, you go and you choose the heaviest model, the most expensive model and you go, great. It did the thing. That's not a business, right? Like you can't automate that. You can't use that a hundred million times if it's the most expensive version of token generation that does what you need it to do. So then the question really becomes kind of like this exploration of, okay.

Let's say, let's say we figure out that LLMs can do this kind of reversing and you go, okay, we did it with GPT-5 Pro Plus Asian, it costs $2 a run. You're okay, well, that's not gonna work very well for us, is it? And then you take that same recipe in that platform and you go, okay, well, let's try every open source model. Let's try every open source model with this temperature versus that temperature. Let's try every open source model with this verifier versus the other one.

Let's try every non-open source model, blah, blah. And then you can actually get this sense of performance where you go actually, weirdly enough, Kimi K2, which is available this easily and like this cheaply with these settings gives us the same performance as we were getting with GBT5 Pro at like 0.02 cents a run.

JAGS (09:34.217)
That's when you start to get into the actual business side of this, which goes like, how do we manage our fucking cogs? What does efficiency actually look like? How do you get reliable, effective output without spending whatever money, you know, Sam Altman decides is worth it? Well.

Ryan Naraine (09:48.333)
Well, you go pay somebody else to tell you though, right? Like you have to find budget to go pay Dreadnought to tell you that.

JAGS (09:53.514)
Well, you have to find budget to pay dreadnought to give you the means to answer the question for yourself as many fucking times as you want from that point forward. Right. But like, like think about, think about what we're discussing here. Like this is not a consumer platform for the sake of like, you know, random so and so this is a matter of like, if you're building anything that is supposed to rely on models.

Ryan Naraine (09:58.727)

That's what I'm saying.

Oi.

Ryan Naraine (10:07.82)
No, I get it.

JAGS (10:16.917)
To me, it's like either you figure out a way to build this for yourself or you buy it from them because the question becomes how the fuck like this would be the equivalent of us having like a trucking company and every time you pull up to a gas station, you don't know what like what concentration of like gas you're gonna get and you go, well, let's see, right?

Ryan Naraine (10:37.068)
Right, but you become an added cost though, right? Because you still have to go pay a guy to tell me, come help me use this gas station. What does unleaded mean? What does unleaded not mean? Am I really getting 1.36 gallons? Like, that's what you're promising, right? I have to go pay a guy to do that. It just feels like.

JAGS (10:50.975)
Yeah.

Well, it's less than the thousand people you fired because you automated, you know, whatever the fuck part of this thing, right? Like the other part of this is I actually think that if you have a business built on these things, that it's an unavoidable cost because how do you know that you're getting the same value and the same output today versus tomorrow versus one? If I tell my customers that every time they jump on, you know, Sentinel one console, they they're going to get

Ryan Naraine (10:59.531)
Yeah,

JAGS (11:22.621)
reliable output from an LLM assisted tool that tells them what to hunt on. I'm just fucking, let's say like I'm just tying a ribbon over, you know, chat GPT, open AI. on, you know, today it worked amazing. And on Wednesday, they're like, well, we need more GPUs to generate, you know, videos of Sam Altman stealing GPUs. So the, you know, the, the, the protein folding and cancer research can go fuck itself. We're lowering that capability.

You have no way to know that unless you have some kind of harnessing around this.

Ryan Naraine (11:53.655)
So you're, right, and there's an independent verification point that kinda keeps the Frontier Labs honest about, you know, what.

JAGS (12:01.577)
I, yeah. But look, let's not bury the lead here. I'm not talking about like just, like, how do I make things cheaper? I think it's really fascinating to understand that for certain problems, tuning a way cheaper open source model the right way will outperform the really expensive, slow reasoning model that you can get from a frontier provider. Like that's the real takeaway here.

The other parts are just, you know, nice to have.

Ryan Naraine (12:35.862)
Costi and Jumpin. Are you following this?

Costin Raiu (12:37.63)
No, I am, but from a much more practical point of view, like I can of course speak in theory about the advantages of all that, but I was thinking that actually this can actually save you money in the following sense. Just to give you an example, let's say you use Geppetto to do reverse engineering, which I do a lot lately. And I noticed that, let's say I use a local model.

JAGS (12:38.654)
Yay.

Costin Raiu (13:04.286)
running on one of my computers on a Macbook and I use chat GPT through the API maybe for all or like one of the four models for speed. If I run it locally, it can be like 50 seconds per function. If I use chat GPT, which costs some money, it can be like 25 seconds. And for me to save 20 seconds is way more valuable than a few cents that we spend.

on using the Frontier model like you say. So from this point of view knowing that whatever model which actually finishes in 15 seconds on my laptop has the same quality output as the Frontier model would be fantastic I mean because in the end is not the money but it's the time so if this actually saves you time by providing results faster I think that is the most valuable side of things.

Ryan Naraine (14:02.326)
Are you using both Frontier Labs and local models in your daily workflow custom, or are you just outsourcing all of it externally?

JAGS (14:02.655)
Think of it.

Costin Raiu (14:12.272)
I am using both. mean, I have very good results with the OSS models from OpenAI, like the 20B model, which runs on the Macbook. It's actually, it's formidable. My opinion is it's superior and the results are superior to pretty much everything else. So I tested, I use like different things, but after OpenAI released this set of models,

JAGS (14:26.709)
Crazy fast.

Costin Raiu (14:40.789)
I'm just using that. I'm not using anything else nowadays when I have to run things locally and yeah, cloud, of course. Yeah. The frontier models are a bit superior, a bit faster, you know, a bit more polished, more capabilities, maybe larger context windows. It's actually funny. was analyzing one stock from LabsCon. I first of all, I transcribed that using whisper.

running locally on the Mac and I can share it. Yeah, I did it locally so that I don't upload that 1.2 gigs file anywhere. So I did it locally on the Macbook with it worked brilliantly. And then it was funny that the 20b model from OpenAI, it was unable to crunch the ideas from that talk. It was like too much. It was like...

Ryan Naraine (15:11.116)
So you have the text transcript, share it with me after.

Costin Raiu (15:37.757)
the context the token window is too little please increase token token window please masters i increased i increased it was crashing it was unbelievable it was crashing lm studio yeah running d20b model from open ai

JAGS (15:45.749)
My apologies to the open source model.

Ryan Naraine (15:57.216)
Talk a little bit about like what the Frontier Labs are doing. OpenAI put out a Chad GPT October report that talked about what kind of threat activity they're seeing from different parts of the world, which is kind of like this niche factor that I've always talked about. before we get that, that's Leo Dong in the news. want to jump in quickly. Costin, before we go on, before we start the show, start the show, Bucharest Cybersecurity Conference was this week and you were out there as well. What is that scene like?

JAGS (15:57.494)
That's really funny.

Costin Raiu (16:25.692)
So that's the first question. What is Bucharest Cyber Security Conference? sounds like... It's possibly the largest cyber security conference in Bucharest. Maybe... I don't know. Perhaps Defcamp is bigger, but Defcamp is maybe a convention. I don't know. I think we're like maybe somewhere between 400 to 500, somewhere in that range.

Ryan Naraine (16:28.042)

Yeah, yeah, yeah.

Ryan Naraine (16:31.935)
They're all of Bucharest here.

Ryan Naraine (16:44.799)
How many people out at this cybersecurity conference thing?

Costin Raiu (16:54.909)
Although it says a cybersecurity conference, my feeling was more of a policy conference. Like everyone was wearing suits. Like the first thing you get, you go there and see everyone's wearing suits. I was like with the jacket. yeah, typically cybersecurity conferences is not full of people wearing suits. That's one.

Ryan Naraine (17:06.495)
Nice.

Ryan Naraine (17:16.349)
Is it a for profit corporate thing?

Costin Raiu (17:19.06)
It's actually organized by the DNSC, which is a Romanian cybersecurity directorate. they, yeah, our CISA organizes this event. They also did it last year. Last year, in my opinion, was a bit bigger. think this year were a bit more restrictive in whom they approved. So I had actually friends who applied to attend, which was free, but they got rejected because essentially all the seats were full.

Ryan Naraine (17:24.825)
I see. Thank you, Orciso.

Ryan Naraine (17:45.203)
I see.

Costin Raiu (17:45.851)
Um, and like I said, maybe it wasn't necessarily security focused, but more like policy, but there were like some amazing people there. So it was a good chance to catch up with our friend, uh, Mark Graham. If you, if you remember Mac pie from, um, uh, back in the days, he was with mystic. He's with the raggles. He's with the raggles nowadays saying he was in one of the panels about the industrial security and the threats. So was good to catch up with him as well as, um, a lot of people.

Ryan Naraine (17:59.02)
Mm-hmm.

JAGS (17:59.996)
Wow. the fuck is Magpie doing over there?

Costin Raiu (18:15.772)
whom I know since high school and it was funny like they're all now like CISO of that and like a COO at that company. everyone is more or less connected to security from let's say my close friends from back in the days. So more like an opportunity to see old friends, see like a few talks about policy and yeah, catch up with friends.

JAGS (18:43.903)
What does policy look like over there? So yeah, I was gonna ask like,

Ryan Naraine (18:44.085)
Was there a lot of energy there around? I was going to ask the same question. Was there a lot of talk around like drone stuff? Like what is the policy discussion dominated by?

Costin Raiu (18:46.703)
What is it

Hmm.

I'm afraid it's nothing that serious. Look, it's, no, I can tell you it's more along the lines of things such as a NISTU directive. So there's like this, don't know, maybe not everyone is familiar with NISTU, but in Europe suddenly this is a big thing. So NISTU is this directive which...

Ryan Naraine (18:56.575)
Nothing sexy. Misinformation maybe?

Costin Raiu (19:16.325)
Practical from a practical point of view it means that if you are a company in one of these critical sectors like energy oil Or you're actually a company that provides services to them Then you need to register with the NSC now Why in case there's some kind of a disruption of cyber attack suddenly like a small player has the potential to Disrupt the national energy grid or something like that. So imagine that the national energy grid they use

some antivirus product, a random one. And then that vendor gets hacked and somebody deploys a destructive malware through that product to the national grid. So the NISTU directive essentially kind of regulates, tries to regulate this issue. So there are like lot of round tables and discussions about this one. While others were about education. Like a big problem is that nobody's teaching kids.

how to survive in today's digital world and there's like all sorts of things from grooming, spearfishing attacks, there's like people logging on in online games and grooming kids and

things like that and there's basically no curriculum in schools they don't teach that typically the other way around the kids teach the teachers

because they are like more savvy with computers and passwords and pass keys and security and antivirus and such and bypassing did I tell the story with Wikipedia? don't think I did Wikipedia is blocked at my daughter's I have no idea why they would block Wikipedia that's silly right? Chagy Pity is blocked Wikipedia and one day she comes back home

Ryan Naraine (20:45.973)
Bypassing, bypassing parental controls.

Ryan Naraine (20:58.186)
cheating.

JAGS (20:59.349)
That seems... That seems silly.

JAGS (21:07.625)
Yeah, fucking cyclopedias, man.

Costin Raiu (21:09.946)
she connects to the internet and one of my scripts detects a shady connection and I'm like implant implant in my home network and I'm tracking very quickly where does it come from where is it where is it like it's her laptop and like okay we look I look in her laptop and what do you know there's a VPN like a new VPN and I'm like what's that she says we have a

Ryan Naraine (21:19.018)
You

JAGS (21:22.719)
you

JAGS (21:32.138)
Huh?

Costin Raiu (21:35.299)
There's an Indian kid in our class. He's a genius with computers and he showed me how to bypass the school filtration so I can access Wikipedia. The very Indian computer savvy colleague installed one of these shady VPN applications, which immediately triggered one of my rules. And I was like, okay, let's replace that with a more reputable VPN. yeah.

Ryan Naraine (21:41.407)
the Wikipedia blog.

JAGS (21:45.417)
Jesus Christ.

JAGS (21:59.382)
Here's sweetheart, it's time to get you your own Mulvad subscription. You are old enough.

Costin Raiu (22:03.385)
It's time for your own Molvad. Yeah, well, like, oh, 14 years old is time for your Molvad VPN subscription. Yeah.

JAGS (22:11.743)
coming of age story.

Ryan Naraine (22:15.08)
Well, while you were at offensive AI con and cost inward this Bucharest cyber security conference, Apple security chief, Ivan Kirstich went to hexagon for his first keynote since in years, I believe, since his last talk at Black Hat. In fact, I'll just mention here, I invited him to the podcast. had a conversation. I had invited him to the podcast and he says, I kind of remove myself from the media glare after that last Black Hat talk. I kind of

JAGS (22:15.614)
I love that.

JAGS (22:27.696)
black hat right?

Costin Raiu (22:27.96)
Take it.

Ryan Naraine (22:41.546)
I got enticed to come out at Texacon and this is gonna be the last one. At least that's what he told me. That's his excuse for not coming on the show, which was a bit of a bummer. at Texacon, Ivani actually announced some pretty significant news around Apple's Bug Bounty program. And the big one is a $2 million payout for exploit chains comparable to these mercenary spyware attacks. Some of them, you know.

Costin Raiu (22:41.624)
Mm-hmm.

Ryan Naraine (23:08.614)
zero click, one click things. $2 million, not for vulnerabilities, but for full exploit chains. Does this move the needle? Does this move the needle and keep it out of the hands of someone wanting to sell it to a Paragon, an NSO? That's the battle, right? The battle here now is how are we pricing this thing to entice folks to give it to Apple instead?

JAGS (23:32.854)
I mean, how comparable is that to the current pricing? To me, my outdated ignorance, it sounds like the numbers we were hearing about the black market sort of paying for an exploit chain. And they too would be paying for an exploit chain. And so I'm sure it doesn't mind collecting pieces of vulnerabilities, but they need chains. So it sounds like we're in the ballpark.

I guess, and that's.

Ryan Naraine (24:03.466)
Yeah but does this move the price? That's my fear here is that Apple gets into the ballpark and then the ballpark moves.

JAGS (24:12.435)
Well, but but that's good, right? Like, think about it, right? Like at the end of the day, if the whole point of this is that you're just trying to increase the cost and the scarcity of these things, then if Apple pays two and that means that so has to pay five, then you know, and then Apple pays three and then so needs to pay eight. Right. Like that's the whole point. Right. Like that's the whole point of this whole situation. You're not going to stop the bones from coming around. The weird machines are going to be weird.

Ryan Naraine (24:26.686)
That's the goal.

JAGS (24:42.463)
But the, but talking about like, think about it from the perspective of a paragon that has to like keep operations going, right? You, you're effectively saying, okay, this thing that our entire business relies on to function day to day for our most basic operations, right? Those exploits are not for the every once in a while thing, right? Like that is a part of their day to day product offering.

Especially with no persistence in it, right? Like the whole point being, you know, we're not setting any persistence so that we don't get caught. Any time somebody restarts the phone, you need to reinfect it, which means you need this exploit chain to somehow to still be valid. Now you're telling me that exploit chain costs at least $2 million. Every time we use it. You've got this, you know, like you got to kind of gird your loins and go.

okay yeah we're there we're good it didn't you didn't get caught and then it gets sure

Ryan Naraine (25:45.236)
They're still in business though. They're still in business, probably profitable business. So let's not, let's not pretend that it's affecting them in any significant. Well, it's affecting them, but.

JAGS (25:50.258)

Sure. Well, it is. So I think where you would see it affecting them is not whether they're in business or not, or whether they're getting contracts or not. But if you see situations like the if you remember after the hacking team leak, if we would go through the hacking team emails, you would see moments when they would be like, we're putting a stop to all operations. We need to go fix this shit. Like, you know, basically like a no service.

period, because what you're saying is right now, like we're unsafe. We don't know that we can essentially, do this without getting caught or without somehow making the situation worse. We need to go replace a component or we need to go, you know, re rejigger the platform or really rejigger our persistence mechanism, whatever, so that we don't get caught. with the, with this exploit situation, it's much more interesting because

You're not talking about rejiggering the malware, the implants themselves, because there's as far as we know, no like meaningful detection capability on iOS itself. But you are saying that you can't actually guarantee that any of this stuff will get on box unless we find another exploit chain. And in that, like I look, I don't like Apple's approach, but I respect it for its consistency and for it's like.

its pragmatic approach in that it actually has some kind of a strategy. The idea being like we're neglecting the implant side of it. And I'm sure Apple people will say, no, we're not, we're doing X, Y, and Z. I'm like, no, you're fucking neglecting the implant side of it. I don't give a shit what you say. But you are boxing people in into saying like in order to get on here, you've got like only a couple of mechanisms. And the one really, the one that most of you are relying on

is based on these exploit chains. We're gonna make this shit as expensive as possible and then we're gonna burn them as often as we can. It is a viable mechanism.

Ryan Naraine (27:51.486)
Austin.

Costin Raiu (27:54.28)
look I think at the moment

Ryan Naraine (27:56.308)
Sorry Juan, I didn't mean to interrupt you. There was a lag and I thought you were going to

JAGS (27:58.41)
No, no, no, no, no, you're fine. You're good.

Costin Raiu (28:01.366)
No, I want to say that if you ask me, it makes no sense to sell to Apple. Like at the moment, I know it sounds brutal, but it makes zero sense if you're driven by financial point of view. It makes no sense to sell to Apple because you can

Ryan Naraine (28:17.811)
And there's a subset of folks that that's just their primary motivation. I'll get as much money as I can for these findings,

Costin Raiu (28:21.798)
sure they want to make money so i think the only way we can make this work and i know it will make some people upset and it'll make me not okay in their books but i think that we need to extend the sanctions against the companies like nso and whoever to the people selling them zero days only then it will become it will become

Ryan Naraine (28:44.872)
That's a tick.

JAGS (28:44.919)
yeah.

Costin Raiu (28:47.685)
logical to sell to Apple so you avoid the risk of getting sanctioned for fueling and supporting these abuses and these abusive businesses. Otherwise, in the current state of things, it makes no sense to sell to Apple for less money because again, there's a bunch of companies buying zero days, if you remember, $10 million, some companies out of United Arab Emirates.

some russian companies were hyping 20 million dollars for the full zero click chain with persistence and that's still like i don't know 10 times more money than what apple offers unless we find a way to make it risky and dangerous to sell to nso and the likes it makes no sense to sell to apple

Ryan Naraine (29:34.313)
Problem is that though.

JAGS (29:35.222)
That's where you end up in like intellects of territory, right? Like you sell to those people and it doesn't go super well. You can't even pretend to just be selling to like a reputable country along the way. like, I think I take your point, Kostin, about it having to be kind of more, more risque. I think honestly, I would put it a little differently. I that's like a profit maximization function. What I would say is

If Apple chooses to be reliable as a buyer, they will have a much greater impact than if they just try to be the highest bidder, which is to say in the past, we've seen instances where people were like, yeah, I reported the thing and then they like jerk me around for six months and then decided they weren't gonna pay me and they patched it. And like when that shit happened, yeah.

Ryan Naraine (30:28.809)

Those are the only stories I hear though. Like I've never heard of someone saying they've gotten 500,000 from Apple for a bug or an exploit bounty. I noticed in the wired piece that accompanied this announcement from Yvonne, he was quoted as saying, we've done a few $500,000 payments in the past. I've never seen anyone documented publicly. The only documentation I get is people, the only documentation I see publicly is when they dig around folks. So I feel like there's a misbalance there.

JAGS (30:47.125)
I I'm sure that's also with an NDA, right?

Ryan Naraine (30:56.103)
Before you finish up your point Juanito, wanted to, under Costin's proposal to sanction even sellers, doesn't that just reshape the market entirely? Prices come dropping down and then again, you're just, I don't understand how that fixes the.

JAGS (31:11.591)
You need to be careful. You need to be careful. So look, in my view, I think we tend to focus too much on the money. It makes it sound like it's like this casino payout type situation. Yeah, yeah. But that's my point. I think that's the head. The fact that it's the headline is focusing way too much on the money when what you are ignoring is the fact that like these people are working their asses off. These exploits are not easy.

Ryan Naraine (31:20.925)
The money is the headline though. The money is the headline.

JAGS (31:37.352)
Like I have immense respect for people who can come come up with like an iOS exploit chain. And what I hear from people who know how this shit actually works is that now it's the kind of work that takes teams. It's not just a single savant out there who's just like just popping out an iOS exploit chain. One of the smartest people I know, like I know it almost killed her to like develop one of these things on her own over months and months and months. And like when you when you look at that situation,

the reliability of being able to monetize your effort, I think is a much more important factor than how much you make for it. And that's something that Apple could, if they're smart, and they lower their guard and they go, yeah, maybe we already had this exploit chain or like the relevant vaults in the back, but we should just pay these guys their fucking money for the sake of.

Ryan Naraine (32:17.778)
Lean in, right?

JAGS (32:33.897)
the program for this and like and not hide it under an NDA, but instead say, hey, you know, congratulations to these three fucking geniuses. We just like paid them out two million dollars

for, you know, whatever. And we've patched stuff in the next, know, we will be patching stuff or we patch stuff six months ago, whatever the fuck you want to do. But the point is, it's a dark market. It's a it's a gray market, which includes a certain amount of unreliability and a lot of like.

game theoretical concerns about whether like are we investing too much time into a thing that won't pay off? Are we gonna tell somebody about the thing and then they won't pay us? Are we gonna get screwed over by the broker who's in the middle of it? Are we gonna... Exactly. And Apple can change the reality of that business if they just become known as the, look, if you showed up with a chain, you're gonna make some fucking money, period.

Ryan Naraine (33:12.349)
That's the reality of that business, right? That world, yeah.

JAGS (33:26.757)
Maybe it's not 10 mil, maybe it's two, maybe it's not two, but it's 1.5. Maybe if it's a duplicate, we'll dock like 400,000, but you still get 1.6 million. All of a sudden, you are working towards a reliable payout. And a reliable payout is much more valuable in a lot of ways for people who are doing this day in and day out than going to like the broker and the thing and the maybe of the money, maybe 10 mil. Like I'll take

I'll take two mil for sure over 10 mil maybe on something that could be burned in the next, you know, Citizen Lab release. It means something.

Ryan Naraine (34:07.369)
The thing is there will always be

Costin Raiu (34:07.493)
Yeah, but again, there's no retribution and there's no risk. So it doesn't matter if it's burned by the next citizen lab. If you personally are not affected and you don't get named and shamed, I think it's fine. Moreover, you can get paid in crypto and you don't have to pay taxes, which I think is also can be a problem if you live in some countries, right?

Ryan Naraine (34:11.603)
there's.

JAGS (34:27.071)
Well, you're not, because in many of these, my understanding is in many of these cases, they're not getting paid. Like, it's not like you just show up and they give you like a briefcase full of money and you shake hands and you walk away, right? Like the, many cases, what happens as I understand it is you get, let's say, maybe you'll get half upfront or a third upfront, and then you get paid a certain percentage or a certain amount.

for every month that the exploit is still valid. And then the minute it gets burned, you're done, right? And it's like a way to, it's also a way of controlling that this person doesn't take the money.

I take 10 mil from you and then I turn around and I sell it to Apple, right? you know, so in many ways that gray market has developed its mechanisms to keep itself sort of, you know, healthy or honest. And that entails a certain amount of like, you know, hedging and...

Ryan Naraine (35:08.297)
and then go patch it, yeah.

Costin Raiu (35:09.49)
burn it

JAGS (35:25.469)
fear and uncertainty. And I think that's my main point is I'm glad Apple is talking numbers that are starting to sound like they're closer to the ballpark of the great market. I think the main mechanism that they can rely, that they can lean into, that they should lean into, that would make them the de facto person to go sell this shit to is to be reliable and to lean into paying people instead of

looking for a reason not to pay them, which is the experience that a lot of folks have with bug bounties, where you go, dude, like, especially with this, right? Like the effort that we're talking about, if it takes months, if it takes a bunch of people, then we're not talking about like $2 million for a single individual is a lot of money. $2 million for the work of like six specialized people over three months is not a ton of money.

especially when you don't know if you're going to get paid at all. And like that's that I think that's the part that like rewards for justice never figured out. That's why it looks like a fucking scam. But with the bug bounty platforms, with being the richest, one of the richest, if not the richest cash richest company on earth, just lean into paying these people to develop the relationships, lean in. Even if it's Dev Null, even if you go out, already knew about this one, just pay their fucking money.

for the sake of establishing the reputation that goes, dude, why would you put yourself in bed with the Saudis? Just go to Apple and like, Ivan will write you a check. That's a good, that's a way to actually disrupt this.

Costin Raiu (37:02.811)
Yeah, but we need to...

Ryan Naraine (37:02.888)
The for these commercial spyware platforms isn't going away anyway. I just can't help but think this just keeps pushing the prices up because the demand for zero click chain, one click chain, these things are super, super valuable. Even if Apple shifts the prices from one million to two million for zero click chains, remote attack with no user interaction.

from a million to two million, then one click ones, which is a remote attack with one click user action from 250K up to $1 million. You're now helping to push the prices for those things on the gray market, on the black market even higher. Is this the goal? mean, Kostin, you've always talked about imposing cost and making sure we're making the bar, raising the bar so high that only a few people are capable of doing this. Is this like a win in your book?

JAGS (37:39.423)
which is great.

Costin Raiu (37:53.832)
I think it will be very difficult to keep the bar high from a technical point of view because you need to innovate. as soon as Apple introduces some new features, innovation, iOS 26, things like that, there will be new bugs. They will introduce new attack surfaces and then it will be very difficult to keep these numbers up. just imagine, I remember the story from a few years ago when

Ryan Naraine (38:10.62)
new attack surface.

Costin Raiu (38:21.618)
Was it Zerodium that was actually saying that we have so many zero click chains that we just don't we don't need basically we we don't buy them anymore. So like these numbers, you know that Apple is mentioning here, you can't sustain them like for an unlimited amount of time in the sense that if let's say a dozen people just walk in with their zero days and they're all

Ryan Naraine (38:30.46)
We don't want anymore, yeah.

Costin Raiu (38:50.305)
unique and different from each other, I very much doubt that they will be able to pay every single one of them.

Ryan Naraine (38:56.188)
Still a drop in the bucket for Apple in the grand scheme of things, I mean.

Costin Raiu (38:59.739)
true but like what is the total budget of this program because we know how these things work they get a budget of let's say 20 million dollars for five years and then they need to pay like for the best box with that limited budget it's not unlimited so at the same time I think I think it's very important that this program whatever it works it has like the

Ryan Naraine (39:06.173)
Yes.

JAGS (39:15.925)
It could be.

Ryan Naraine (39:18.152)
You

Costin Raiu (39:23.077)
The carrot and the stick. So if it's just the carrot and paying like it will not be enough to shift the tides. You need the stick as well. So maybe they need to work with the Trump administration or whoever to make it more risky to sell zero days to sanctioned companies or mercenary companies that are known to have been involved in abuses. So only when you have both of them, I think you will make a change.

Ryan Naraine (39:51.783)
That's that's that's a hot take. One of the other things Apple announced is some new, some new categories. Yes. Yes.

Costin Raiu (39:55.217)
Can I stop you right there and tell you one story? From back in the days, I used to have a friend who was probably very well connected in this field and he was for sure developing and selling all sorts of capabilities. And he told me once we met at the conference and he said like, I want you to meet some fellows. And I said, okay, who?

I can tell you a lot of things about them, but we need to go out and meet them like this location. And I was like already afraid. So, yeah, in the evening we go to that place, to that location. And he says like, allow me to introduce my friends. And then he says, if you have zero days to sell, they pay the best money on the market. And then I realized it hit me.

JAGS (40:28.927)
KISS

Costin Raiu (40:47.108)
that for him the most important thing was who pays the best money on the market. The risk that we go to like this shady place in the evening that's nothing like it didn't really matter that much as it mattered to me. To him the only thing which mattered was that those guys they paid the best money on the market. So I mean as long as motivation is high and the payouts are high

and people have this mentality and ethics are low, I don't think things will change a lot. I think they'll stay pretty much the same way.

Ryan Naraine (41:22.12)
They've added new categories as well to the Bug Bounty program, including big payouts for gatekeeper bypasses, iCloud access up to a million dollars, WebKit sandbox escapes, and an

interesting category here, wireless proximity exploits getting a million dollars. Do you see Apple's interest in these being triggered by...

Attacks happening in the wild or this is more conspiracy. Ryan is asking what kind of wireless proximity exploitation is actually happening or this is more of a theoretical. Let's try to do a pen test against specific things.

Costin Raiu (41:48.952)
Hey.

I'm confident that conspiracy ran knows exactly what he's asking and everybody else listening to our show they know about the tactical suitcases that sell for something like 8 million, 10 million, 12 million dollars delivering Wi-Fi zero days that compromise the wireless adapter baseband and from there they can jump into the care. I don't know it's things that I heard.

JAGS (41:54.621)
Not theoretical. That is not theoretical.

Ryan Naraine (42:19.259)
What is he talking about?

JAGS (42:21.182)
No.

Costin Raiu (42:23.15)
If you go to certain conferences and hang out with the right people, essentially there are things like this, tactical suitcases. I think I've seen photos from, so what they do is essentially you get a suitcase in which there's a laptop typically and some wireless equipment like a lot of antennas.

Ryan Naraine (42:35.185)
What do they do?

Ryan Naraine (42:47.003)
Like the stuff that the Secret Service just sees.

Costin Raiu (42:49.578)
Hmm possible something like that but wireless also in the sense of Wi-Fi here because that's super popular and what you need to be is just you need to be in the proximity of the target then this they will actually list all the wireless adapter Macs which are constantly broadcasting and looking for known Wi-Fi networks and as long as you can identify your target and say like this is my target

Then you can deliver a zero day to that target, which eventually it infects their machine with spyware. And there are several companies selling these tactical suitcases. They start at pretty,

pretty significant prices. And then you have to pay per additional pack of targets. So they support something like, I don't know, 50 targets. And if you want to infect more than 50, then you need to pay extra.

one such company I spoke to the people who used to work there and they said like yeah we have customers in a dozen European countries we only sell to NATO we only sell to European Union countries and we have over a dozen customers and all our customers they're super super happy so this is probably okay in the sense that a lot of abuses by the way

happen when the target and the attacker they're not in the same country right? know Algeria spying on Macron or things like that that's like super extreme cases

Ryan Naraine (44:29.607)
Do you put the the Villexity finding about Wi-Fi proximity in Washington DC with that Russian attack in this category of wireless proximity exploits that Apple is really interested in here?

Costin Raiu (44:44.929)
I don't think so, no. I think what they're targeting are exactly these tactical suitcases that we have seen, which leverage zero days in the wireless adapter baseband and they have the ability to infect your computer. They just need to be in like a range of something like a hundred meters from the target. So these for instance are extremely powerful when you use them in airports, when you use them

effectively when you're tracking your target, let's say, and you can follow them like physically with a mini van or maybe at a cafe and you just follow them for a let's say long period of time then you can guess their wireless adapter Mac and then it can target their phones, can target their computers, their laptops and so on.

Ryan Naraine (45:36.647)
So a million dollars, a million dollars. Sorry, Juanito. I didn't realize you were there because you're still there. OK, sorry.

Ryan Naraine (45:47.333)
Gotcha, you were gonna say something.

Ryan Naraine (46:01.619)
We lost him. We lost him. We crashed out. The question I was going to ask you as a quick follow up was this $1 million price for this wireless proximity exploit suggests that Apple thinks this is a significant issue. Apple knows these suitcases are a significant problem, right?

Costin Raiu (46:02.317)
We lost him. He'll be back.

JAGS (46:17.812)

building suspense, was building suspense.

Costin Raiu (46:17.867)
Well, yes. Yes, because I think we probably reached a point where these are actually more powerful and more prevalent and Apple doesn't have the same ability to spot and catch them as they have with, let's say, browser based exploitation with iMessage based exploitation and so on. So the artifacts may be a lot less scarce. You don't get the same kind of logs payloads.

Ryan Naraine (46:19.941)
You're good.

Costin Raiu (46:46.783)
I think I remember there were a few cases of not just wifi, but like pure wireless. I mean, wireless slash GSM exploitation targeting Android phones. If I remember correctly, the case that I am familiar with and the security in that space is very lax is very poor. Also the ability to catch them.

and to page them is also very very low so it makes it makes absolute sense it makes total sense to me that they're willing to throw one million dollars into this kind of exploits

Ryan Naraine (47:27.949)
One, you were making a point about this before. You're back, camera's working fine, lights are fine. Don't stress about anything.

JAGS (47:29.876)
So yeah, I was gonna say I am. So, Fede Kirschbaum in the chat last time said that my camera had been focusing on the background instead of me. And I remembered that and I'm like, oh, I'll open the software. And the minute I did that, it went to update the firmware for the camera and just like crashed it all out. that's my bad.

Ryan Naraine (47:49.371)
Security, always security.

JAGS (47:51.988)
so, it makes perfect sense when you think about like, what, what are we talking about with these exploit chains, right? Like when we talk about the normal exploit chain, the whole point is that you have some way of like remotely getting this device to load something. And then, then once you're in it, as long as you don't kick off things with like persistence or other, you know, mechanisms that might throw off like sandbox entitlements and so on, you're basically scott free. And the expensive part here is how much.

is being put into like defending, you know, let's say these parsers or like you're in lockdown mode, right? Like the thing isn't even working at all. But all of that is defending a very specific entry vector. And if you can somehow fuck with the Bluetooth stack or you can somehow fuck

with the Wi-Fi stack, you're home free, right? Like none of the shit that we were just describing really applies to you.

and, I think that's, that's actually, it's actually really interesting, that this is being put in there in that, in the, in that category, as an acknowledgement of that reality that we've all known about this whole time. and also I think showing some of the, the shortcomings of Apple's approach, the reason you want it to do, you do the threat Intel shit properly. The reason that you do want to have an on device like

telemetry generation and ability to do incident response properly is that you have to account for the realities of the space, not the theoretical, well, this is how, if someone was gonna do it, we think they would do it this way. So we're only gonna put all our eggs in this one fucking basket. And then you find out later on, it never occurred to us that somebody would, I don't fucking know, exploit this other thing, come up with this other way.

And, and that's how they've been loading their malware. And I think that's what a lot of our careers, especially Kostin, who's discovered so many like genuinely like concept breaking new things where you go, holy shit, this threat actor has been doing X. They've been, you know, affecting the, the, infecting the firmware of the hard drive. They've been setting up a boot kit that loads the operating system instead of

JAGS (50:14.949)
You know, the operating system loading the malware, right? Like those types of things are situations where had we had the discussion and I'm sure the discussion has been had with the manufacturer or the relevant protector of that software, they would say that's not going to happen. That's a theoretical concern. And then you show up and go, here's a threat actor that's been doing it for six fucking years. And I think that's a dynamic that Apple has neglected.

Ryan Naraine (50:38.862)
Yeah.

JAGS (50:43.571)
or just not really given the right kind of attention. And in this case, this is an admission that they've dealt with it. And I think that that's fascinating. I think it's great and I'm glad they're willing to pay for it because that is an area that also needs the same kind of love and attention, right?

Costin Raiu (50:52.49)
you

Ryan Naraine (51:03.494)
From that budget that Ivan Kirstich got for this program, he got 1,000 iPhone 17s that Apple says they will donate to civil society groups ostensibly to pass it down the chain with iPhone 17s with the new memory integrity enforcement technology that we talked about recently. I believe

his Hexagon Talk was the technical details of that and doing his promo tour around MIE. Costing 1,000 iPhones is a big deal.

Costin Raiu (51:30.89)
Yes, yes, I think this is the probably the most significant security initiative that I've seen from Apple recently trying to help these groups and keep in mind that an iPhone 17 with this memory integrity enforcement in lockdown mode with iMessages and FaceTime disabled and running something like Signal on it is a formidable tool.

Ryan Naraine (51:53.798)
You still gotta use WhatsApp though, right?

Costin Raiu (51:55.881)
I said with signal on it. I don't know if they'll be using WhatsApp but even our friends at WhatsApp nowadays they are like super super on top of things. Shouts to our friend Ivan, the other Ivan at WhatsApp. The other Ivan, right. So to me this is fantastic. I like that very much. The only question is of course which groups like civil society. Who decides which groups in which countries, who gets what.

Ryan Naraine (52:03.152)
They're on top of things, yeah.

JAGS (52:10.536)
the other.

JAGS (52:22.621)
Bill Marsak.

Ryan Naraine (52:22.694)
CitizenLab will get 500 and they'll distribute it to their 500 people within their network that are popular targets. I mean that's a win, right?

Costin Raiu (52:26.173)
Mm-hmm.

JAGS (52:27.016)
Well.

Costin Raiu (52:31.059)
would be nice to have some transparency in there like how are these distributed and what is the kind of impact they are making I would love to see a report saying how much exploits attempts this mitigated how many were stopped and things like that and obviously if we were like in our company like back in the days people would be beating us very hard with the stick to justify those money like

Ryan Naraine (52:38.384)
Criteria,

Costin Raiu (52:59.613)
They want to see the return on investment. They want to see the success stories with the journalists, with these civil society groups. It's essentially promoting and emphasizing how good the several devices were for their operations, which again, there they are. Really? How much is that? It's like a million.

Ryan Naraine (53:17.531)
A devices out marketing budget is nothing, You don't think?

JAGS (53:21.459)
Well, wait, wait, but they're there. That's I mean, honestly, Apple could do this. Apple could do this 100, 1000 times over, and it would still not be a lot of money for Apple. And I think that is that is part of the discussion that we're having about like the exploit chains. Right. When you go like when I say they just need to reliably pay out like I don't give a fuck what your budget is and you shouldn't give a fuck what your budget is like this is about supporting the entire iOS platform, which is the most secure

Costin Raiu (53:26.142)
million and a half.

JAGS (53:51.536)
operating system on earth as far as we know and like that that is worth whatever money you have to pay even if you have to pay redundantly with these devices I say a thousand a thousand devices not one and none for coast and which is kind of sad but the but you don't qualify what I'm what I'm really interested in though is like how are these devices prepped like what makes these devices different

Costin Raiu (54:09.863)
I don't qualify.

JAGS (54:19.013)
Is it just like a different, you know, software thing? Is it a different hardware thing? Well, no, but like the research devices and the whole point of it is that they're set up differently, right? And that's, think, you know what I like about that is I like the idea that it's gonna make these threat actors have to once again, hedge their bets and go like the same mentality that threat actors have around windows machines where they go, well, what, what?

Ryan Naraine (54:21.231)
should be out of the box iPhone 17.

Costin Raiu (54:26.483)
Hmm.

Ryan Naraine (54:27.66)
the research devices.

JAGS (54:47.379)
what version and what security solutions on there, you know, like there was a time when we saw things that like, we just not infect things that had Kaspersky on them or not infect things that had Sentinel-1 on them or whatever. And you go, cool. They did some testing. They figured out that the detection is solid enough or they're worried about the cloud component or they're worried about whatever. So they just avoid that threat, like that target altogether. And that's something that nobody on iOS has had to think about really.

not meaningfully, because you go, they're all the same devices out the box. And look, these people on that podcast won't stop bitching about how they can't defend these devices. So just hit whoever the fuck you want. Hit Macron for all it matters. They're all the same devices. And for once you're starting to kind of like, hopefully you're adding that question mark of people being like, is this, is this, is this one of those research devices? Is this going to get our fucking $10 million?

exploit chain burned like that that is actually valuable.

Ryan Naraine (55:49.798)
Speaking of Macron, we got fresh news this morning, the head of UniCredit being targeted by Paragon with a zero click delivered by iMessage.

We know for a fact that Paragon tools are being used in parts of the world here. Why is this one significant, the Unicredit CEO being targeted in Italy?

Costin Raiu (56:16.936)
I think it's a huge story, it's probably not receiving enough attention but it's also a very new story I think I saw it around 4 p.m. my time so that was like just two hours before we started recording and pretty much all the other victims Paragon graphite victims that we know about and they were exposed before they were journalists they were activists so they were like people

involved in that side of politics, don't know, exposing government corruption if you want or being anti-immigration policies and so on. More or less, more or less, but understandable from the point of view of let's say logical, logical targets like the kind of targets that a government or an adversary or another government let's say would be targeting. this

Ryan Naraine (56:53.893)
understandable targets.

Ryan Naraine (57:00.665)
from an academic point of view, from right.

Ryan Naraine (57:12.099)
the reason these tools exist and are so valuable.

Costin Raiu (57:12.977)
Hmm

Maybe. But yeah, the head of UniCredit, an Italian bank, right, targeted by this is I think it's a totally different case. And we haven't seen targeting of let's say business people and bankers and such in the past. Because I think because most of the targeting is extremely expensive, so you need to choose these targets very carefully.

So in this case, mean, people are speculating or saying that simply because he was involved in politics as well. That's one of the reasons why he was targeted. He got a notification from Apple in April, I think on April 29th this year. So I say that probably.

He was also involved in politics, but what this story essentially teaches us is that you don't have to be an activist. You don't have to be a journalist to be targeted by these tools. Like look, head of Unicredit in Italy was also targeted. That means that other people can get targeted. I know like from my sources, from other cases that I have seen, which is that CEOs and other business people also

got these notifications, not just politicians, not just activist business people, in particular powerful business leaders, business leaders involved in big deals, mergers and acquisitions, people who leverage and turn a lot of money. They also got these notifications from Apple and from Meta. So I think that this story, once again, it just confirms how these tools are actually used and

Costin Raiu (59:01.656)
It tells us that, especially if you're the CEO of a large company that you should worry about. If you work in one of these companies in IT security, then you should care about your leaders. You should care about your executives. And I think one of the most important things is that you need to establish a program to actually check their phones regularly for infections and not just to companies, but governments. One of the things that I hear a lot is

Essentially, a lot of governments do not have thorough programs to regularly check the phones of people in positions of power, like ministers, senators, and so on, for malware infections. And whenever they get these notifications, they typically, they keep them.

themselves. They don't tell anyone because they're afraid, they're ashamed, they're worried, whatever. So I know that a lot of governments are looking into this, trying to build programs to actually handle this issue and the same I think should be true with companies. Remember like

the triangulation story, even Kaspersky said who was targeted? All the top managers. So it was targeting all the top management in the company.

I mean, yeah, you should think about establishing forensics and methodology to handle these cases in companies.

Ryan Naraine (01:00:31.96)
When you mention executive CEOs, your source is saying that a lot of these guys get them. There's a lot of economic espionage happening by these tools or this is like a small tiny thing. And then how do we counter that? Does this change the perception of what these companies are, these parasite companies are, if they're enabling this kind of thing in addition to everything else?

Costin Raiu (01:00:43.077)
Hmm.

Costin Raiu (01:00:50.373)
That's tricky. I don't think it's necessarily economic espionage in the sense of stealing secrets, but more in the sense of being able to know inside things which they can leverage in deals, right? It's a stolen secret. It's not like Chinese style stolen secret, right? When they're like stealing formulas for vaccines or, but yeah, but knowing that they are discussing internally.

Ryan Naraine (01:01:03.012)
That's a secret. That's a stolen secret.

JAGS (01:01:07.891)
Thank

Ryan Naraine (01:01:13.412)
just monitoring negotiations, stances and stuff, right?

Costin Raiu (01:01:20.047)
Well, I hope to God that they will not bring this issue into discussion and this is the issue that they actually bring into discussion.

JAGS (01:01:24.688)
Right.

Just knowing the numbers, man. Like that was classic Chinese negotiation tactics in Latin America, Africa forever. You walk in knowing exactly what the limits are, like how much money you can spend, how much like what your budget is. Like that's the end of the negotiation right there, right?

Costin Raiu (01:01:43.077)

Yeah. And especially when this kind of negotiations are kept on like country level, I don't know the country X is waiting on buying Huawei 5G technology or no, and they have $20 million. Huawei comes and their technology is $19.999 million.

Ryan Naraine (01:02:02.66)
0.6 yeah right up to the edge

Costin Raiu (01:02:07.926)
So yeah, I don't admit that I understand the reasoning behind some of the cases that I have seen and why those people are targeted because it can't be country level deals. I mean, some of these things, it's probably valid to someone and we probably don't have the full picture. I mean, this is one of the things that I learned is...

Ryan Naraine (01:02:24.814)
valuable to someone.

Costin Raiu (01:02:34.008)
when victims don't make sense it can either be a mistake or we don't have the full picture I've seen mistakes including funny mistakes in which people with similar name were hit with something because simply they had the name that was similar to someone else or like yeah I mean it happens who I need to know? I don't know

Ryan Naraine (01:02:55.672)
One eater wouldn't have that problem at all.

JAGS (01:02:58.159)
Nope, nope. If they hit me, you know, they mean to hit me, right?

Costin Raiu (01:03:04.709)
There's no other, there's no Juan Andres. I remember by the way, we were joking with our good friend Vicente, if you remember Vicente Diaz, who's now with Aristotle. If you Google Vicente Diaz, there's like a famous Spanish singer, like Grand Exitos style of singer from back in the day. So that's like the most famous Vicente Diaz.

Ryan Naraine (01:03:04.91)
What are-

Costin Raiu (01:03:31.828)
in the normal people world. In our world it's our Vicento obviously.

Ryan Naraine (01:03:37.125)
Speaking of things in this space that I don't understand at all is news coming out this week that the LSO Group, is like the poster child for this world, has been acquired by US investors. There's a report out of Israel that was confirmed by TechCrunch that a Hollywood producer

named Robert Simons has led the deal, subject to Israel and US regulatory review. Question for you, Juan, right off the bat is, how do you acquire a company that's either sanctioned or on the entity list?

JAGS (01:04:00.317)
What the fuck?

JAGS (01:04:06.195)
Bye, yo.

Ryan Naraine (01:04:06.806)
Help me understand what kind of shenanigans are happening here.

JAGS (01:04:09.652)
I don't understand what kind of shenanigans are happening here. Let's start there. I also think it's hilarious to talk about them doing this deal for tens of millions when I'm pretty sure NSO had to buy Francisco Partners shares back for $500 million or something like that. The numbers have cratered. I think the minute that you're talking about

you know, having having a Hollywood producer be the one managing your your deal, right? Like we are clearly scraping the bottom of the barrel and and and probably gaming folks who, you know, have perceptions that may not be entirely well informed. At the same time, I think it's really telling that they're willing to let this kind of embarrassing bullshit happen because it lets you know that there's nothing of value left within NSO as a structure.

like as a corporate structure. And the question...

Ryan Naraine (01:05:10.852)
The product and the tool still exists and it is in use though,

JAGS (01:05:14.471)
Well, but is it NSO? Is it NSO or is it NSO2 in Cyprus? Is it NSO or is it NSO3 in Saudi or UAE? now, you...

Ryan Naraine (01:05:26.884)
What does that mean? Is there like, you're dropping like a...

JAGS (01:05:31.791)
I mean, I'm making names up, but it's like a well-known thing in the industry that most of these companies, basically around the time that NSO gets sanctioned, most of these Israeli companies basically just fold close up shop and all of a sudden you see companies pop up in Cyprus or Saudi Arabia or the UAE and it's the same talent, it's the same people, it's the same general structure.

Ryan Naraine (01:05:33.998)
Okay.

JAGS (01:05:58.656)
For all we don't know, but I wouldn't be surprised if contracts just got transferred over like, you're no longer an NSO customer. And now you're a customer of the, you know, the Royal Bank of NSO, you know, in Riyadh or whatever the fuck you want to call it. And and it goes to show kind of the frailty of the sanctions mechanism in going after a company in particular and not affecting the

Ryan Naraine (01:06:27.522)
Individuals?

JAGS (01:06:28.763)
the individuals or the underlying structure somehow, right? Like you have not in any way affected the operations of that company. You took a shell, you know, a name and put a lot of it. Like, look, if putting sanctions down was as easy as like clicking like two clicks at the finance department, you know, whatever, and you go click, click, now that's sanctioned.

and then tomorrow if they come up with a new company, then we will also click, click and sanction that too. Then I don't care, but it takes so much effort to enforce any kind of sanctions against a given entity. And then the minute they rename the entity or they get a different company, like then you're gonna have to go through that whole process again. It's just not a mechanism that's fit for purpose in slowing these people down. And the other side of this is I...

I don't know what this producer is trying to do or like what the value is in all of this.

Ryan Naraine (01:07:31.597)
Wait a second, you don't believe that this NSO group acquisition here by this Robert Simons is the NSO company that we know.

JAGS (01:07:32.069)
I... wait...

JAGS (01:07:43.163)
No, I think it is by in name only. Like you.

Ryan Naraine (01:07:48.206)
That's what I mean though. When I say the company, we know the company with a tool that's... Listen, these guys were boasting that they were helping the Israeli army in the war. I mean...

JAGS (01:07:51.965)
It is the company we know, but here's the thing.

JAGS (01:07:58.77)
Yeah, yeah. And I wouldn't be surprised if they were or they weren't. But the issue here is really if you know how these sort of company acquisitions play out, especially these like skeletons or like little startups or whatever, what is attached to the company? Right? Like the talent that developed the thing and the talent that ran the thing, the talent that grew the software.

It may not be there anymore. It's almost especially with a sanction entity. It's almost certainly not there anymore. Then like we know how these operations work. You have a platform and you have an implant and then what's fueling it is actually the exploit chains, which are ephemeral and the contracts that you have, the fact that you have the right connections with governments and so on. And they believe you and they they trusted you enough that they put money in contracting cycles, right? You know, the bureaucracy looks like.

So those are the two most valuable things that that company has is essentially like this software. Well, three, the software stack, the talent that produces and maintains it and, and the customers that it has. So I don't think the talent, there's no way that the talent is there anymore. Like no fucking way. This is hard enough with just a normal and healthy and legal company to like get through a startup and actually have your talent want to be there.

I'm I will be I don't know. So I would be shocked if they haven't somehow moved the contracts and whatnot to some other entity, assuming that, you know, Julio and all these other folks are still intent on maintaining what is a very profitable business for them and almost a sanction resilient business, which is an insane situation to be in.

I would not be surprised if they were moving all of that to their new venture in the UAE, whatever. And so what do you have left? Are you just basically selling a company that has a platform that can do iOS, whatever, but you're selling it to people who are not savvy enough to understand that without the exploits, without the talent to develop the exploits, without

JAGS (01:10:14.897)
the contracts into existing, like what you're buying is like a shitty, a random quality infection platform that is not going to work. And you're not going to be able to do anything with unless you can supplement the two things that you're not getting. unless Hollywood producers have some good exploit broker contacts, like I really don't, I think this is like somebody getting played hard.

And I'm assuming that what they think is because Paragon was bought by AE and that was a very profitable venture and that they're now seeing like possible contracts with the US government that they're going to be able to do the same if they just like pick up this bucket that is NSO, such a recognizable brand, blah, blah. But I just do not see how you're not being sold like a bill of goods. You're definitely getting played.

Ryan Naraine (01:11:11.363)
think he's on the right track?

Costin Raiu (01:11:12.48)
Maybe. I was also thinking that perhaps one of the possibilities here is the talent would be willing to return if the company was to change hands and come back into the kosher side of things with the US government. So if, let's say, it gets bought by Hollywood, then suddenly, you know, the sanctions are lifted and then it's again the best place.

work nowadays and then the talent simply returns so perhaps it's part of this whole strategy to make it viable again so of course we may never know we'll have to see

Ryan Naraine (01:11:52.963)
This was always a jewel in the eyes of Israel. The NSO group had a big building up. It was was a standard there. And I believe the Israeli government also has used it in part of bargaining chips and so on. So the idea that the NSO group gets sold out to US is significant in some fronts. I don't know what tech is going with it, which customers are going with it. I don't even know if it's a real deal.

Costin Raiu (01:11:59.63)
Mm. Yeah.

Costin Raiu (01:12:08.319)
Hmm.

Ryan Naraine (01:12:19.36)
be honest with you, because there's been no like official announcement. There's just been like some press reports and confirmation.

Costin Raiu (01:12:22.729)
could be part of the agreement to whitewash it, to make it safe again, to make it reputable, to leave the sanctions and so on. Like TikTok.

Ryan Naraine (01:12:32.33)
possible.

JAGS (01:12:32.465)
What's valuable? What's valuable about it? let's write like this thing has been it's been sanctioned, which in itself is not going to get reversed that easily. But even if it were, it's not like it's Microsoft where it's like one hundred and twenty thousand, you know, person organization and all these patents and all this software and all these buildings and properties and contracts and whatever. I mean, never at that level. Right. Like you're still talking about at best amid. Yeah. But but that's my point.

Ryan Naraine (01:12:53.118)
It used to be though, right?

Ryan Naraine (01:12:58.518)
Not at a Microsoft level, but yeah.

JAGS (01:13:02.425)
What is the value of fighting for it? Right? Like this is, you don't want the brand brand, like brand value in, in espionage is it's exactly, no, dude, it's not, it's, it's a counterproductive thing. Right? Like what happened to hacking team hacking team had gotten burned a bunch of times there've been technical reports and whatever. But like, once you build, once your brand becomes like a matter of like kitchen table discussion for policy wonks in DC.

Ryan Naraine (01:13:09.152)
Yeah, that might even be negligible.

JAGS (01:13:31.449)
You have fucked up royally, right? Like a long time ago. So like, I just have a hard time seeing what about NSO as a corporate structure has any value whatsoever other than like whatever intellectual property, software or possible contracts you hope to transfer over. And then my point becomes that it's almost certain that this thing will be worthless unless you're attaching

Ryan Naraine (01:13:34.432)
long time ago yeah

JAGS (01:14:01.284)
it to a place that knows how to use it, knows how to develop for it, knows how to maintain it, which is like, dude, if Paragon or Quadream or whomever was buying NSO, then I would say, NSO must have built some pretty cool internal tooling or they still have like 20 contracts with a bunch of governments that last for another five years. And these people are being smart and saying, we're going to take this carcass.

and we will expand our business with something we didn't already have. And that would be, it would be really interesting, but it's being like, it's so fuck the fact that it's like a Hollywood producer, like that alone, that makes it sound like hilarious and silly. But even if it was like, you know, yeah, but, but no, I think that just like, just made the punchline really obvious. But like, if it had been, even if it had been like a, like,

Ryan Naraine (01:14:46.146)
Diluted the story, right?

JAGS (01:14:58.451)
a VC or a hedge fund or a financial institution or whatever the fuck that doesn't know how to maintain and run these things, I would be equally skeptical because I think that, you know, I just just thinking about it from an &A perspective, I just cannot think I cannot come up with something that makes this husk valuable.

Ryan Naraine (01:15:19.348)
Enough of a dapplin' spyware. Let's update a couple of quick stories because this one took an hour and 15 minutes on the one story. I have another story I wanted us to touch on last week on this podcast, because you and I were digging through the Oracle CPU patch update for July because the chief security officer told us that the

JAGS (01:15:24.007)
Bro, we spent like a fucking hour on this, this is insane.

Costin Raiu (01:15:25.576)
Hmm.

Ryan Naraine (01:15:42.691)
You know, people had not been patched and this e-business ransomware thing, this Klopp ransomware extortion attacks were happening. This week we find out that all of that was a waste of time. It was actually zero day. It was actually a brand new CVE 2025 61882 that these guys were actually exploiting. And we find out because another ransomware gang that's a rival of Klopp outed them and dropped their exploit that we were able to confirm was zero day.

Costin Raiu (01:15:45.874)
they get on.

Ryan Naraine (01:16:12.674)
Two things here. why, like why cost Juanito we talked about this. We know Oracle is a company that are versed and have very high quality people, very, very talented people. Why is the chief security officer at Oracle providing bad guidance a week for a week.

JAGS (01:16:33.179)
know what was what was so bad about it because like I actually I'm feeling relatively right.

Ryan Naraine (01:16:37.802)
It felt like some victim shaming. Let me throw it out what was bad about it. It felt a little bit of victim shaming. This is a July patch that we issued a long time ago. Go back and do your thing. A little bit of that came out to me. Turns out it's actually all day.

JAGS (01:16:51.431)
Wait, but it was a thing where it's like, you have this patch and they said, and like, we're investigating and we will provide more. And then they did. So like, this is the part where I wanna like, I don't wanna, sorry, let's be fair. And I'm feeling particularly partial towards Oracle, I'll admit it. like, but well, let's play this one out, right? First of all, Oracle is a new,

Ryan Naraine (01:17:10.818)
Same with me. But this was a fuck up.

Costin Raiu (01:17:14.013)
You

JAGS (01:17:21.051)
It's by far not a new company, but it is a new player in the security, in the engagement with the security space in this way. I don't mean, sorry, Ryan, you're giving me the look, you're giving me the right look. What should I say? Let's put this differently. It is, I think this is the first time I've seen them drop any thread into.

Ryan Naraine (01:17:32.492)
Slow down.

JAGS (01:17:43.633)
So to me, what I'm judging them, I'm judging them not as a massive old school incumbent mega corporation, but rather I'm saying like, welcome to the scene. There's gonna be some mistakes. The muscles are not well developed yet. This is your first time doing this. Welcome. I'm happy that you're here. I'm sorry that it's under these circumstances. Then.

Ryan Naraine (01:17:46.466)
What does that say?

JAGS (01:18:08.452)
We talked about it, I think, in a surprisingly measured way last episode, which is very unlike me, where we said, you know what, give them a little bit. Let's see what happens, right? Like that they this they may, if they dig in further in the wrong direction, then, you know, we're perfectly right in like skewering them. But like, maybe they'll do better. And then frankly, what I saw after, which is like, I got a call and like, I got a call the day after the podcast dropped.

Ryan Naraine (01:18:13.077)
We did.

JAGS (01:18:36.455)
And they were like, look, this is where the state of the investigation is. This is, you know, what we found so far. This is what we know. They were very frank about like, this is the state of that platform. It's fairly old school, like whatever. Like, this is not an impressive vulnerability that you're going to see. It's just like part of having a legacy business. And then they went, this is, these are the O-days, sorry, these are the, these are the IPs. This is why we think it's CLOP and we're going to release more stuff.

Ryan Naraine (01:19:01.822)
Iox

JAGS (01:19:05.329)

And the next day they dropped it publicly. So they had gone around talking to whomever they could on the private side and they eventually dropped a blog. Yeah, they had a no day and it got exploited and you know, it's probably it being massively exploited by a ransomware gang is a bad fucking look, especially for like a business product and like that going straight to corporations. None of it is a nice situation. And

You should have the discussion that you're trying to have of like, well, why the fuck is this your first one? Right. You've been around like they're basically like a dinosaur of a company in the tech space, which means they're like a well established one. OK, sure. I give you all of that. But I also want to just kind of like recognize that they started on on. I know, but I'm saying like I'm giving I'm giving them some rope and they're not.

Ryan Naraine (01:19:54.315)
You're giving them long rope, I get it. You're giving them...

JAGS (01:20:01.064)
fucking like they're not putting it to waste. Like I've seen these people working and like even after that, I see them reaching out in trust groups and asking people, hey, do you have any more on this? Do you have any more on that? man, these people dropped the blog. Did somebody put us in touch with them? Like we wanna talk to them about whatever. Like they are really in it. So like whatever you, whatever you.

Ryan Naraine (01:20:22.219)
You're always in it when there's a crisis, man. I'm going to be the counter to it. I love my friends at Oracle. You know that. mean, the head of assurance there is someone I respect and admire. I know what's happening. Their CS, their chief security office is getting bad guidance. Going out last week to say, go, apply July patch and you'll be fine. It's bullshit. And the fact that they didn't know better and they put him to provide that guidance was just a comms mistake. Say what you know.

JAGS (01:20:26.833)
Yeah. Yeah. Yeah.

JAGS (01:20:38.301)
Sure. Right. Right, right.

JAGS (01:20:46.639)
Well,

Ryan Naraine (01:20:48.533)
We don't know, we believe. Give me some better language than just go apply this July critical patch update.

JAGS (01:20:53.649)

No, look, the see the see so statement or the CSO statement was a fuck up and like,

Ryan Naraine (01:21:00.193)
But the comms is a crucial part of all of it. mean, official comms from Oracle is a crucial part of it. We just can't accept fuck up and say, it was a fuck up. Like, you had people scrambling to

JAGS (01:21:02.259)
I agree. agree. just let's let's let's break this up. Let's break this up into its components. So I think the issue that we have here is because Oracle is new to us in this space in this way of doing things, we lack granularity because if this were Microsoft, we would say fuck this person and so and so did this thing bad. However, Mystic did this great thing.

and Dart is doing this whatever. And with Oracle, we lack that. And all you see, all the public is gonna see is this CSO statement, which is a shame because it's a bad one. And clearly these people need better advice on crisis comms. And at the same time, I don't pretend to know what Oracle wants because we have a playbook.

And Ryan, like you're a master at that fucking crisis comms playbook because we played it under the most adverse possible circumstances before. And we have a playbook for what it means to come out looking good and winning and winning ground. You know, here's a crisis. Let me use it to establish better relationships. Here's a crisis. Let me use it to build trust in my brand and executives. Right. Like, yeah. Yeah, you have a crisis, but I'm

Ryan Naraine (01:22:21.633)
improve transparency.

JAGS (01:22:26.041)
in that crisis, I'm going to show you that I'm here for you and that I'm leaning in and that I'm that you can trust my word and like that I'm just like that. And that's the part that these corporations miss is they. It has to be well, but in this case, I think it can be because we know that there's these tech pockets that what they're lacking is a brand, right? Like if if if they had the Delphic research team.

Ryan Naraine (01:22:36.895)
It has to be real though.

JAGS (01:22:53.743)
And like that was the threat Intel team. You can take that guys. I think that's pretty good. And that's their threat, you know, threat Intel team. And those people are building a brand and now they have a conference and they're sponsoring security events and now they're asking for disclosures and like all that shit. We would be standing those dudes and we would just be looking at the C-suite going, Hey, go listen to your fucking people. They know what they're doing. In this case, we're seeing that play out. It's just obvious that the C-suite at Oracle

Ryan Naraine (01:22:54.177)
You

JAGS (01:23:23.343)
is not getting the right advice. don't know how to do the right comms. because it's the first time they're having to do this publicly, they don't know how this plays out, where you can make a statement today that gets people off your back in the first week. But in the long run, it's going to make your customers not trust you anymore. Because they go, when we had this crisis, all you gave us was this bullshit.

Or like, your tech guys helped us, but publicly you left everybody else out to dry. Like shit like that, it makes you look like just a company that cannot be trusted on security. And at the end of the day, once there's an awareness that of your product as a source of vulnerability, if you cannot be trusted for security, that is the ballpark. That is the end of that conversation. They will go looking, or they're going to wait until the day that like,

Google shows up, Salesforce shows up, whomever, says, why the fuck are you still using that? We have this thing, and let us give it to you for cheap, and you try it, and once you turn on that, you're done. The people who've been using this fucking Oracle EBS shit have probably been using it for 20 fucking years without even thinking about it, right? So it's a weird situation. think Oracle's fumbled it from a business perspective, more than from a security perspective. From a security one, I think they're doing fine. They're doing well. Like those dudes are working hard.

Ryan Naraine (01:24:50.698)
remotely exploitable without authentication CVSS base score 9.8 The Oracle advisory came with indicators like Juanito mentioned. Costin what is this Oracle EBS and they exploit POC, scattered lapses, retard, club hunters, what is the significance of that is there?

JAGS (01:25:07.965)
You can't use the R word. You had to redact the redacted clop hunters.

Costin Raiu (01:25:12.953)
the artwork Ryan you mean Ryan is the forbidden or which one do you remember like was it the last episode that you asked me like how how should this warning actually look like and we were saying like it should be like this is what we know so far and that and that and that and then at the end indicators of compromise and either perhaps the oracle

Ryan Naraine (01:25:13.928)
Is there a conspiracy Ryan question here?

JAGS (01:25:19.635)
It's a part of the file name, man.

Costin Raiu (01:25:41.539)

People are listening to our podcast, shout out if they're listening, and look like how do they say like you ask and you get it. It's in the Bible, right? Ask it and you should get it. Think as you should receive. We received like there is an indicators of compromise table here with some IP addresses. Then there's like these three hashes. And I was happy when I saw that the only thing

Ryan Naraine (01:25:43.498)
Shout out to the Oracle team. They called Juanito after apparently.

JAGS (01:25:45.308)
I don't know.

JAGS (01:25:56.175)
Yeah, that's right.

Ryan Naraine (01:25:57.13)
and you shall receive it.

Costin Raiu (01:26:10.077)
is that when I looked at the hashes and I think it originally when they published there wasn't any description and then they updated this on October the 6th so originally it was published on October the 4th and then on the 6th they added these descriptions with the article and I went to VT and I grabbed them and then I was like what the fuck is going on here like what who are these people like what is going on in my

Ryan Naraine (01:26:24.202)
You didn't have the description, right? You didn't have this description with his names. You had to go find it by, yeah.

Costin Raiu (01:26:39.992)
Obviously the top question here is how did they find them on VirusTotal? Like who uploaded them to VirusTotal? Like what is going on? It just feels there's another side to this story here. Whoever got them... Who are those guys? Are they really another competitor group or is it like a three-letter agency opposing as a competitor group? Who are those? And yeah, when I... Me personally?

Ryan Naraine (01:27:06.058)
Well, who do you think it is? What is your guts? What is your gut feeling? You can be asking questions on the podcast. Your job is to answer them.

Costin Raiu (01:27:10.429)
yeah you know me you know me i like conspiracies like the conspiracy world is better than the real world i think that someone saw the initial blog and they were like facepalm you know the

picard from star trek with the facepalm and they're like no no no it's not the july thing you guys and they're like okay how do we convey the message

Ryan Naraine (01:27:18.282)
What do you think happened here?

Costin Raiu (01:27:35.219)
Okay, let's upload it to VT. Let's pretend that we are this group and then let's tell Oracle, Oracle go patch that thingy and everybody's happy.

Ryan Naraine (01:27:38.504)
Let's tell Oracle to go look at this VT identifier.

Ryan Naraine (01:27:45.578)
So this is just a POC. That was.

Costin Raiu (01:27:48.599)
It's working POC.

JAGS (01:27:49.972)
Well, I don't know. Okay, wait. Let's break this up in several things. First of all, I think the upload to VT is just the defenders trying to share in a TLP green fashion, right? So like, don't think that the VT upload, my assumption is that the VT upload did not come from the disclosers. Then I...

Costin Raiu (01:28:05.303)
Mm-hmm.

JAGS (01:28:15.559)
Had we not had this weird branding around it and like, I would have assumed that this came to us the way that every Oday comes to Avanti and Fortinet and so on, which is the magical mystery research community in the middle of things found this on, know, some infrastructure ran into it in the middle of an investigation and they went to the vendor and said, hey, you idiots, you're getting exploited.

You don't you obviously don't know this, but we found the exploit. So here's literally the script that's being used. So go fix your shit. And that, you know, that dynamic is what makes me be so critical of Fortinet and Avanti and so on, where I know I'm like, I know you motherfuckers are not discovering any of this. It's being handed to you and then you want to act as if you can be trusted. So fuck you. That that.

Theory kind of goes out the window in this case because I've seen a thousand of those situations and I've never seen them Branded like a fucking calm kid on crack and like put all these insults and stuff So there does seem to be some element of this that is some weird drama

between You know the some some of these groups. So maybe I mean like what happens if somebody defected

from Klopp and went over to Shiny Hunters and like took the exploit with them or like, you know, like there's, there's all kinds of ways that, this could kind of play. And these things are that petty, right? Like they are internet squabbles, right? So I don't know the truth. I just think that, that in this case, there is kind of like, there is a possible story here that's kind of hilarious. And, and I don't know. I don't fucking know.

Ryan Naraine (01:30:05.887)
Pretty big sting though, because I saw Austin from Google threat intelligence say this isn't a hundreds, perhaps thousands of companies affected. And I just want to make one last point here before we move on from this story. Well, two points. One is for all the shit I'm giving Oracle, shout out to Oracle, like Austin said, to actually providing some indicators, helping people to go accelerate detection, threat hunting and containment. That's all we ask. Like at the very least, you got your shit to deal with.

Costin Raiu (01:30:23.702)
Yeah.

Ryan Naraine (01:30:32.381)
help your customers deal with this shit that you pass down to them. So shout out to Oracle for that. Hopefully more companies do this at the end of it. The second point I want to make here is I'm noticing more and more journalists hanging out on these leak sites, communicating with these ransomware assholes, and then going back to companies and saying, yes, I saw the data. It's real. Like you're enabling that shit. Like you're part of the ecosystem. In my opinion, I could call names because I see it happening all the time. I'm not going to call names.

But if you're a journalist hanging out on a leaked site and confirming that yes, is clop and going back to a company like Nvidia and saying, yes, I saw the leaked stuff and it's real and it's true. And then going and writing a story that yes, you saw Nvidia's data on a leaked site after you're a part of the problem. I'm sorry. Thank you, Costin. No names, no names yet.

Costin Raiu (01:31:02.07)
Call names.

Costin Raiu (01:31:19.198)
I agree. Call names, call names.

JAGS (01:31:22.131)
I so wait, wait, wait, wait, wait, I will uncharacteristically come out. No, no, I will uncharacteristically come out in defense of one thing. It may not be research and it may and it is contributing to enabling certain extortion demands. However, I. I do think there is a legitimate reason for those journalists to be there.

Ryan Naraine (01:31:27.421)
This is not research.

JAGS (01:31:49.74)
and to be a part of this, is how often the vendors pretend that that is not actually happening. The ransomware crew goes, hey, we have all your fucking data and your MSSP, your vendor, your appliance provider, they lie and they go, they don't have your data, that's bullshit.

Ryan Naraine (01:32:09.619)
They're lying.

JAGS (01:32:15.205)
or like, it's not as bad as they say they are, or we know everything about these guys, they're not gonna disclose it. And there's a, like the only thing that gets us to the public conversation and the customers having some semblance of what is actually going on is a journalist that goes, I don't know what the fuck so-and-so is talking about. I saw the data myself, it's there. And like, so.

You know, there is a countervailing force here that I I'm all for them. Or look, the other one, right? Your PII got leaked because your vendor got popped in part of a ransomware thing and they send out an email that says none of your passwords or passports or anything important has actually leaked. And the only reason we know that's not true is because a vendor like a journalist is in the back paying attention like the.

I can see, I'm saying there's a legitimate one there. I'm not saying it's good for the ecosystem. I just like, don't fault a journalist being in there in the first place, you know?

Ryan Naraine (01:33:07.26)
I don't know.

Ryan Naraine (01:33:12.34)
Hey.

Journalists hanging out on leak sites is legitimate news gathering. I give you that 100%. If you should get in there and you should be news gathering and doing your thing. Journalists writing naming and shaming stories after vendors refused to pay a ransom. And journalists writing stories that saying this company's data is there for sure. And you've only been given that because the ransomware guys want you to name and this vendor into speeding up a payment process. That's bullshit. And I see more and more of that. It's just...

JAGS (01:33:19.005)
Sure. Yeah, yeah, yeah.

JAGS (01:33:41.939)
Yeah, I'll give you that. I'll give you that.

Ryan Naraine (01:33:44.039)
And it's called journalism today because everyone is chasing the newest TikTok bullshit. that's my.

Costin Raiu (01:33:49.03)
only that but remember when ransomware groups were actually launching programs for journalists in which they were willing to share some of the profits with journalists who are willing to hype the stories so that's like a real thing

JAGS (01:33:58.674)
Whoa.

Ryan Naraine (01:34:03.007)
There's an entire ecosystem of like ugliness there that I'm calling attention to. seeing it more and more in news stories, guys hanging out on leak sites and confirming that this vendor is affected. And yes, I saw this piece of data and I'm like, dude, you're enabling that shit.

JAGS (01:34:14.919)
mean, I mean, we have to do it too. Like I, know, Jim Walter was writing me Friday night at 1 30 in the morning about like the output of this, this leak site. What was it with the fucking timer that was supposed to clock out last night, right? Like we have to do that. So in some way, yeah.

Ryan Naraine (01:34:19.955)
Speak.

Ryan Naraine (01:34:36.369)
legitimate research. The other part of it isn't. Communicating with these guys and helping to be part of ransomware negotiations is a problem. I want to shift gears quickly, speaking of vendors and problems. Ivanti, I just noticed this. Our favorite vendor, Ivanti, was, reminded us they were the first people to sign the Secure by Design pledge. They were the very, very first here to sign the Secure by Design pledge. Just got

JAGS (01:34:52.437)
no! No!

JAGS (01:35:04.211)
They've had the longest with it.

Ryan Naraine (01:35:06.407)
ZDI, the Zero Day Initiative that buys vulnerabilities and buys vulnerability details and so on, released 14 new Ivanti advisories. Bare bones advisories with no technical details marked as

Zero Day because they remain unpatched. And they remain unpatched because Ivanti is asking for six month extension after agreeing, like in one case there was a bunch of them. There's 14 advisories on the ZDI page, all marked as Oday.

No technical details, no patch information and so on. The only mitigation offered is given the nature of this vulnerability, the only salient mitigation strategy is to restrict interaction with the product, which is basically don't use this product. But in the timeline that the ZDI published to justify their reason for going all day is July 2025, the vendor communicated that the issue would be patched in September 2025.

And then in July 29th, five days later, the bandit requested an extension until March 2026 for a variety of these vulnerabilities that are all remote code execution, like pre-authentication, post-authentication. So pretty gnarly looking things. Ivanti we know has been in the muck of this thing. What do you make of this, Kostin? Is this something that surprises you? Like, what do you make of this mess?

Costin Raiu (01:36:27.197)
Look, you are dropping some numbers there. said like six months. to me, let's just for people to visualize what that means. So ZDI reported this vulnerability in June, June of this year. And in September, or apologies, in July, Ivanti requests an extension until March, 2026.

So that's like a total of what? Nine months, nine months required to patch this zero days. To not patch. I mean, yeah, it tells a lot. I remember there was a discussion at the countermeasure conference a few years ago. And there was, I think, a Canadian general who was talking about

JAGS (01:36:59.027)
to not patch, they're still not patched.

Costin Raiu (01:37:19.514)
a couple of things and security of different platforms from different vendors and he said the amount of zero days in some specific platform is not the most important metric. One of the most important metrics is actually how fast they are able to patch those zero days. Can they patch them in a day? Can they patch them in a week? And how responsive they are. If they request like nine months to patch this potentially

like super disruptive zero-day vulnerabilities, I think that's a very very bad, very bad mark.

Ryan Naraine (01:37:56.605)
It's a symptom of how shitty things are in the background.

Costin Raiu (01:37:59.714)
Correct, it's a symptom and it's not the problem as always, not the symptom, the problem is the disease and how do you fix that? If you ask me, I don't know, I mean, nowadays whenever you

mention Ivanti, there's another zero day in Ivanti, yeah, and the water is wet, yeah, what else is new? And the stones are hard.

JAGS (01:38:18.771)
shh

Ryan Naraine (01:38:19.026)
this is a security vendor. Like I remind folks that Yvanti sells security products. This is a security vendor that like, mean, we should hold them to the highest possible standard. They signed the pledge and made a big deal out of it. this is not unfair for me to call attention to this shit after you've paraded yourself as like a, wanting to talk to me.

JAGS (01:38:42.775)
I, you know what I, you know, yeah, you, no, no, no, no, no. You know what I'm curious about? Why that date? I'm curious if we had let them go, if they were going to announce the products were like end of life and they were coming out with like a new thing. You know what I mean? Like this, it's like, it's, it's, I can't give them the benefit of any doubt. Exactly. Like the most sleaziest possible thing here would have been.

Costin Raiu (01:38:43.538)
The water is wet.

Ryan Naraine (01:38:43.646)
You

Costin Raiu (01:38:56.946)
Mmm.

Ryan Naraine (01:39:00.028)
I'm not gonna patch this. Like you can't give them the benefit of any doubt whatsoever. You look for the most nefarious thing. That's the expectation.

Costin Raiu (01:39:00.434)
Mmm.

JAGS (01:39:12.103)
That's the end. That's my expectation of it. And that says everything and that says fucking everything because you guys know I'm not being unfair. Like I I would not be surprised because like what excuse do you have for not like you'd need an omnibus of patches. You're going to reengineer your entire the entire software platform. OK, reengineer it but issue a fucking patch. Right. Like it just nothing about this is the right way to go about it. And we also know it's not their first one.

It's their umpteenth one. So clearly there's like they're in my view. It's hard to look at Evante and not think that they are an entirely incompetent vendor for what they're selling. And that is not. It's not, just a pure perception without substantiation, considering that Evante is a company that's selling something.

made up entirely of like acquisitions and rebrands. It's almost like a company that is like acting as a P holding company. And I mean, maybe that's even what it is. I don't fucking know. And it may not even be in a position to actually maintain these things.

Ryan Naraine (01:40:30.814)
I agree with you that the worst possible thing that could happen is what my expectation is. And you bringing up that possible end of life timing could quite possibly be the truth. Could quite possibly. By the way, shout out to ZDI. Without ZDI, we don't know any of this stuff. And shout out to companies who are starting to find another.

JAGS (01:40:41.819)
I mean, come on, man. Come on.

Yeah.

Ryan Naraine (01:40:53.394)
This is like another layer in the disclosure process. Usually it's from full disclosure all the way to this new coordinated thing. There's like another layer here where if a vendor is going to be tardy and they keep asking for extensions, we're going to out them. We're going to out them with some bare bones details that doesn't put people at risk, but give people some sort of mitigation. In this case, there are none. It's like, don't use this product, which in itself should be the right mitigation anyway. But again, shout out to ZDI for this policy and I wish more people reporting vulnerabilities would take on this policy.

JAGS (01:41:14.877)
Yeah.

Yeah, when are we gonna get this, when are we hearing this from Hacker One or Bug Crowd, right?

Ryan Naraine (01:41:27.722)
They're not really, they're not really brokers at all. They're there to represent the interest of vendors and keep researchers on the NDA. You know my take on that stuff already.

JAGS (01:41:35.271)
Well, then I know and I agree with you, which is why I'm saying ZDI just did this and I mean, out to them. And what matters about the fact that they did it is that this is a new thing. And I would like HackerOne and Bugcrowd, two companies that make a giant point out of their community engagement.

Ryan Naraine (01:41:54.556)
Right.

JAGS (01:42:03.558)
And we have friends, you know, at least in bug crowd, hacker one's weird. But like, I'm, my point is they kind of have to at this point, because if you want to say that you're not like a racket on behalf of corporations that are paying you money to muscle security research, which in turn, like let's describe,

Ryan Naraine (01:42:08.446)
We have friends in both of those companies. They could and should be doing better at holding vendors accountable.

JAGS (01:42:32.643)
Let's call out the full chain because they have made this look like a market and a service. they are that's turning this in, you know, turning this into a business alienates the fact that what security research actually is, is a good faith endeavor for the wellbeing of all consumers. It's a form of consumer protection that people engage in either for commercial gain or for reputational gain, or just because they fucking feel like it.

And you have now created a mechanism of extortion by which a company can silence the only thing that was pressuring them to improve their products by virtue of an NDA and a bit of hush money. And in many of those cases, you're not even paying those people that hush money. You're just making them wait. So I think HackerOne, BugCrowd, and the other bug bounty companies have a responsibility

to actually be this transparent, to have a clause the way that Google Project Zero has always had a fucking clause that said, this is a mechanistic process. Other people are going to discover this vulnerability by virtue of it being there. So you have X amount of days. You can ask for an extension if there's a good reason for it. And otherwise you can go fuck yourself because there are stakeholders here that need to know that this is there.

Ryan Naraine (01:43:57.576)
There's a, there's some big gaps in the system though. I'll just caution you. There's some big gaps in the system there where in many cases, HackerOne isn't even the, HackerOne is a payment platform. The very, very big vendors don't even use HackerOne as like a bug bounty payment. They're like the payment platform to help shift money around. the, negotiation is direct between vendor and, and, and researcher. In many cases, HackerOne has nothing. No, no, no, Yeah, they have no bite.

JAGS (01:44:21.787)
It's like, is this like, you, they're just a payment platform, like for ransomware negotiations, as in the case of like Sullivan and Uber, right? Like that kind of a payment platform. Yeah. Let's, let's

talk about it as it is then. I just, I don't have a, I don't have a good view of the bug bounty platforms in the first place. And that could just be my

Ryan Naraine (01:44:30.397)
In some cases, yes.

Ryan Naraine (01:44:39.111)
Bye.

Ryan Naraine (01:44:44.433)
I'm not a fan of them, I think they've been a net negative to the industry as a whole since the creation of it.

JAGS (01:44:48.467)
I think it's surprisingly parasitic for something that is sickly sweet in its discussion of its community building and support.

Ryan Naraine (01:44:58.597)
of its value. agree. Any last thoughts on that, Kostin on Ivanti? Close the book on Ivanti. I want to move on to one last story before we got to go.

Costin Raiu (01:45:06.351)
I mean, you know my opinion about these kind of platforms. You need to take all the risks into account. So if you're still using some of these platforms, moreover, if by some accident you actually get ransom thanks to one of these zero days in one of these products.

Maybe it's time to evaluate other solutions like you need to do your own due diligence, understand what is available, what is perhaps the best option for you. So yeah, I'm not recommending any particular solution myself, but I mean, looking at some of these incidents, water is wet, like it feels that almost every week there's another zero day mean one of these products just, you know,

try to build the foundation, the security foundation of your company on things that are solid, on things that don't have millions of zero days, that don't take forever to fix them, that you can trust and you can leverage for a long period of time, that work on open source hardware, on hardware that you can actually upgrade over the years without being stuck to one place or another.

And you will see that long term that investment will pay off. you will overall, I think you will overall be better if you pay more attention to these choices.

Ryan Naraine (01:46:36.669)
Great, great, great, great sage advice from the master, of course. And I'll shift to you, Kostin, to touch the story quickly, because this is in your wheelhouse. Chat control in the European Union

is off the table again. You were complaining the last time we mentioned chat control on this podcast, you said, my God, we're heading into dark times. Now it feels like some companies, Denmark, I believe, that was originally backing this legislation, scrapped their vote, which threw it out.

Costin Raiu (01:46:43.951)
Ooh.

Costin Raiu (01:46:49.101)
We don't know. We don't know.

Ryan Naraine (01:47:05.851)
Provide the synopsis for the audience on what's happening.

Costin Raiu (01:47:06.149)
Germany. Yeah. Well, yeah, so this this proposal, which is actually is coming back. This is the fifth time that we they are somehow trying to push this crazy proposal that would essentially force the scanning of everyone's encrypted messages for offensive material with offensive material to be defined and determined at

probably later times at the moment they're pretending that that's CSAM so child pornography but we know very well from past experiences that once you start breaking encryption and you start looking at people's personal communications you are opening a Pandora's box like I used to live in communist times back in the days when Securitate would simply open everybody's letters to read them

You know, summarize in some cases, letters would no longer be delivered. In other cases, the letters would just go to your security file. We are just fucking going back to those times with all these repeated proposals and people just don't seem to understand what you have there. One red horizons. very nice.

Ryan Naraine (01:48:21.797)
it to the camera.

JAGS (01:48:24.26)
My copy of Red Horizons falling apart. What an amazing...

Costin Raiu (01:48:27.52)
of Florida.

Ryan Naraine (01:48:28.359)
We gotta put it, should we put it into the Tree Body Problem Book Club?

Costin Raiu (01:48:32.045)

We should. We should.

JAGS (01:48:32.194)
absolutely. Shout out to the security. Amazing.

Ryan Naraine (01:48:36.487)
So Kostin, it's off now completely. Where do you think it is?

Costin Raiu (01:48:36.733)
I look it's not the fifth time. here's what happens. Denmark, which holds the presidency of the European Union, they were pushing this again, hoping to get it approved. And the big issue was that Germany, who previously opposed this rule, they were like kind of signaling that they are ready to accept it. And then, you know, people starting making noise.

There's actually a guy called Joachim who put up a website stopchatcontrol.eu which was in my opinion the winning move in this whole game. People could just go to this website, you select your country and then you click a button and it crafts an email that you can send and apparently this massive amount of spam from people managed to turn the vote around.

Ryan Naraine (01:49:29.489)
It's not spam, is it spam? If I send you an email, is it spam? Yeah, yeah.

Costin Raiu (01:49:31.309)
This amount, let's say this massive reaction, reaction from constituents, reaction from normal people, people like me. So I did send the one round of emails to the Romanian representatives in the European Parliament. I got zero replies, obviously. So I sent another one last week and I was surprised. I got one reply. I got just one reply. So one representative actually, they replied back to me. I think it was an auto reply, but nevertheless.

Ryan Naraine (01:49:59.751)
You got something.

Costin Raiu (01:50:00.332)
I got something back and you know it's the following that he never supported this proposal. It's a flagrant violation of human rights and blah blah blah. And thank you for being active on this topic. And I was thinking to myself, this guy who answered, he's one of like 50 who answered. And I think that politicians, they still don't understand the reality of nowadays.

They think, you know, like you're campaigning, you get the votes, then you go into parliament and you do what the fuck you want for the next five years or whatever. This can't happen anymore. Like if you just go there and you ignore what you were saying, like what you promised and ignore what I want from you guys, then you will not be reelected. You won't be there the next time. Like this guy in particular, he was a candidate for presidency in the Romanian elections.

So the fact that he replies and he cares, like it's an incentive for me to vote him the next time. And I think that the politicians, they don't understand this rapid cycle of modern technologies. When you send emails, when you use online platforms, social media to poll your constituents to listen to what they want. And then when something like this comes up to reinstate the old securitate rules, then you do in

like how it is best for your constituents, not how people order you to vote or how you think that you should be voting.

Ryan Naraine (01:51:33.085)
Listen to this European and his democracy.

Costin Raiu (01:51:37.163)
You're laughing, right?

JAGS (01:51:37.363)
Hey, think that no, no, I look I say I'll say this I think the most valuable thing to come out of this situation the umpteenth fucking time is that True activism like I'm a huge fan of contra points. I like it's my my YouTube video essayist crush and

Something she said recently is that misery is not activism. And that line has stuck with me because we all know people who seem to be under the impression that being miserable and sounding miserable and raining on every fucking parade and having some shitty thing to say is a way of being engaged in political activism at a time when folks feel dispossessed and they feel alienated and they feel

upset about a variety of things about, you know, Gaza, about the, you know, right wing presidency, about AI, about whatever. And the truth is that I think that's a way of pacifying ourselves, that we are somehow externalizing the bad things that are happening around us. We're disavowing them by virtue.

of speaking, of telling everyone who will listen that this is something that we do not approve of. But that is not equivalent to doing something about it. And it isn't actually being better than your any other neighbor and any other person who's just trying to fucking survive and feed their family and just make it to the next day. A lot of people are not thrilled about the situation that we're in. I think it's awesome that

we are seeing that there are ways within our wheelhouse as technologists to actually enable better outcomes. This dude set up a fucking website that made it frictionless to advocate for yourself at a time when everybody is busy and dispossessed and terrified about their future livelihood and completely burned by fucking housing costs.

JAGS (01:53:59.698)

and living in a life at a lifetime of such disproportional diffusion of resources that we are the richest humanity has ever been and the poorest that the developed nations peoples have ever been. And they don't have the fucking time to try to figure out how to send out a fucking email to the same fucking people who are not going to answer because they don't give a flying fuck what you have to say.

unless it's overwhelming and express that they're uncomfortable with the fifth iteration of the same futile effort, which means these people know that you don't want it they're just pushing and pushing, hoping that they can get one through. This is my way of bringing this back to the technologists who have all, like all the ones that have become defeatist and will not stop whining, which is why I need to like have

policies in our private group chats that politics cannot be discussed in this way and that you need to go to. I literally have had to create off channel like side channels to be like, look guys, you're all welcome to talk about this, but just do it over there. Everybody here is actually just trying to make it to the next day. And it's, they don't need to virtue signal every day or like express their anxiety every day about disavowing the externalities that we're dealing with. But

What this dude is showing us is that we have things we could be doing. And if you care this much, if you have this much time to whine and bitch and moan about how terrible our environment is, clearly there are creative ways that you could be enabling people to make a difference. And I invite you to take that energy and redirect it towards things that will make a difference like this website. That's fucking great.

Ryan Naraine (01:55:51.644)
Every time I hear about chat control and your fifth, sixth time going over it, I think about our own encryption debate here, back-dooring encryption debate here that just always pops up at some point and then you have to remind folks and it feels like a cycle going. So I feel you on that, Costin.

Last thing before we go guys, wanted to touch on this quickly because it was a topic that we've discussed in detail in the past is VirusTotal announcing simpler access for a stronger VirusTotal. We got a blog post out of our friend Bernardo Quintero that provides news on some key access tiers, like new pricing structure basically, addressing some of the, want to tell you you're already squinting, addressing some of the,

Well, how to describe this virus total losing its way in the community. Nah, you you know, you've described it in the past as, know, all the community components that made virus total so fun and interesting. It's kind of gone away. These big giant million dollar bills that showed up to our buddy Vicente doing his thing at virus total. What do you make of the new announcement that there's a VT community component here for free. There's a contributor component here for free. There's

JAGS (01:56:39.763)

ambiguity?

Ryan Naraine (01:57:02.7)
VT Lite from 5k for some Lowa. Like what do make of it? Is this an attempt to address what you've been complaining about?

JAGS (01:57:09.853)
I didn't see this as an attempt to address any of it, like not even remotely address it because all this is is like an announcement of the way things are. Like this is the way things have been forever. Nothing new in it at all. I mean, and it's not even it's not even giving any clarification. I actually I read it twice just being like, did I like am I missing? Like what the fuck am I missing?

Ryan Naraine (01:57:25.573)
So there's nothing new in this.

Ryan Naraine (01:57:36.581)
Wait a second. are also, wait, wait, wait. We are introducing a contributor tier, a dedicated model for our engine partners. Is that new?

JAGS (01:57:45.606)
No, that's the same shit we were a part of at Kaspersky 10 fucking years ago. That's the contributor. You're feeding us samples, so we're going to make it cheaper for you. That is, or like we're going to give you a free access to like, Miss Detection. That is the same. That's the fucking same thing that we've been a part of for 10 years. They didn't introduce shit. No, they're just officializing the way things are. Everyone's complaining that the prices have gone up.

Ryan Naraine (01:58:06.309)
So now that this is new.

JAGS (01:58:13.778)
that the free tier, the lower tiers don't make any sense, that it's completely unaffordable for people who just want to do threat intel, that like all this shit and what they just released is a blog that says, yes, you're right. And this is the thing. Like we're just gonna, we're gonna put it on a fucking table.

Ryan Naraine (01:58:28.155)
Is this true, Karsten? Am I losing my mind?

Costin Raiu (01:58:32.36)
What? No, I was thinking here, look, we know that... So the thing which attracted my attention in this plan, and by the way, I recommend everyone to take a look at this block from Bernardo. In particular, there's this tire which is called VT Duet, which in theory, is it like the largest? Is it the biggest tier?

in the list in theory unless there it says actually key access tiers meaning there are other tiers in addition to these four that we're talking about here and with VT Duet you get full out feature set high API quota and community intelligence only so I think that a lot of discussions around the VT pricing model were about the fact that

Ryan Naraine (01:58:58.617)
It is.

JAGS (01:59:03.687)
Can you put it up?

Costin Raiu (01:59:26.584)
If you wanted what you used to have, then you're automatically being fed this mandiant slash Google threat intelligence on top of VirusTodo. While the main complaint from people was that they do, we don't want that. We, we want only VirusTodo. don't. And people like salespeople were saying, well, unfortunately that's not available anymore. So like take it or leave it. If you want it, you will be getting this.

Ryan Naraine (01:59:41.221)
I don't want all of that shit.

Costin Raiu (01:59:55.815)
new threat intelligence with your subscription and it will cost you only $1 million per year or something. So if this VTDUET is what VT used to be with a high API quota and you only get community intelligence, I highly commend this move, which I think is pretty, pretty nice and people will be happy with it.

Ryan Naraine (01:59:56.131)
Other thing, the upsell.

Costin Raiu (02:00:19.704)
Now the annual price for that it says based on the number of affiliates covered and contribution level. In other ways it's negotiable, I guess. But it does leave some kind of a hope like for smaller companies that for like 5k per year, they can still get some low API advanced search, Yara hunting, even file downloading, private scanning. So

To me, at least some parts of this announcement, they sound very good. But I am like, yeah, on the positive, optimistic side of things.

JAGS (02:00:54.129)
can't, I can't like that that 5k part it it I think there's a fundamental flaw in it and if if if VT fixed it it would become amazing and it would become a

like it would make VirusTotal of a quality and usefulness that I could only dream of, which is VirusTotal's queries are not complete in their results. And that means that I cannot know that

If I spend one API call on a query that I know everything I need to know about that, like that the response is complete, right? Like I've complained about this a lot with retro hunting. think retro hunting is like, it's the prime example of a...

of a business model destroying the utility of a new capability because they charge a fair amount for retro hunting. And that's okay. I think that that's a computationally expensive process and it yields a lot of good value. So you should charge for it and you should make some money on it. However, the fact that you get the results of like the past 90 days or the past year and not the full corpus.

means that there's a, not just a diminishing utility to running a retro hunt, but an incompleteness that makes it not that useful and not, you know, I can't just run a rule and say, I know everything there is to know about this as far as VT is concerned. And if they don't have something, I should go look for other data sets. Similarly with the API queries, with the VTI queries, like having that limitation on

JAGS (02:03:11.459)
it not being a complete picture of what is in VT means that 5,000 API queries isn't shit without like being able to run a query every 10 minutes just to try to have completeness of what comes through the API because I can't afford the file feed, which is like way more expensive. I actually cannot use this for threat Intel purposes unless

you start giving me complete answers. And so my plea to VirusTotal is you have just reinvented yourself as GTI. You are providing exquisite threat intelligence now to the people who can afford it. And I have access to it and I love it. I think it's great. But

If you want to be supporting the security community, if you want to enable threat intelligence as something that happens in places that aren't multi-billion dollar companies, then the way to do it is to provide complete answers now. And then you can charge 5K, 10K, 15K, 20K, 50K, I don't give a shit. But then the model, the...

product model and the pricing model can be aligned and people can get true value from it instead of the rule beating mechanisms that we're all developing where every company that wants to do threat Intel has to invest at least, you know, you know this much money and then build a system on our side that's querying all the time and checking all the time and trying to complete the picture and trying to build our own submitter databases and our own blah, blah. It's like guys, just let's get honest.

with what the actual value proposition of your product is and then charge people what it's worth. we can and that way when you give it away for free or when you give people a $5,000 tier, it means that they have a fighting chance of competing with the other people that are spending a

bajillion dollars and you still have a healthy ecosystem. But right now, that's just not that's not something VT is enabling.

Ryan Naraine (02:05:26.426)
and there's no attempt to create an alternative or a competitor. What does that say?

JAGS (02:05:31.367)
There are attempts, there are attempts, but I think it says a lot about the market. I think it says a lot about, no, not at all. This is a necessity that will continue to be a necessity. It needs some rejiggering. like, look, I'll put my money where I'll put my own sort of reputation on the line. And I am very quick to scrutinize companies.

Ryan Naraine (02:05:40.077)
Is it too late?

JAGS (02:05:59.144)
and to scrutinize the efforts of other people. And that's not a nice thing to do all the time. If anything, look, I'm talking about VirusTotal and I say this with some apprehension because I love VirusTotal as a product. They're a partner of ours in my threat intel business role. But dude, I admire folks like Bernardo and Emmy who started this and like so much of my career.

Ryan Naraine (02:06:16.474)
We're all friends. We're all friends. We're just having an honest conversation. Yeah.

JAGS (02:06:28.197)
and my career wins have come because of VT. Like I am partly, I am in many ways indebted to Virus Total and to these folks for like many of the wins I've had in my career over the past 10, 15 years. So I speak with apprehension as I kind of like criticize them. So let me criticize myself as well. I started a company

that I co-founded a company called Stairwell that could have, that sought to fix a lot of these issues and to create an engine that was this sort of complete answer engine, right? Like you ran a YAR, like you put all your files in the thing, it's all got ACLs and privately segmented. So you're not worried about who gets access to your stuff, but you have all your files somewhere and

Every time you run a Yara rule, would know your results would be of every fucking file that we know about in your environment and in, wherever else. And to be honest, that technology was meant to be we used to call it foundation. It was the stepping stone. It was the very bottom of what the company was going to build on. Because the idea was you have this inventory problem.

which I categorize as one of the fundamental security problems, period, the inventory problem. What exactly do we own and control? How many assets do we have? How is it configured? How many files have we ever seen at what times, when, and where? How many IPs and domains do

we contact? Which ones, where, how often, and how? Without being able to answer those questions, you're...

To the degree that you cannot answer that question, you have an indefensible environment. It's an inverse correlation between answering that question and being able to defend it. So why am I bringing all this shit up? It's not an advertisement for Stairwell. I think what I'm saying is like...

Ryan Naraine (02:08:37.113)
It's the first time I've heard Starewell properly describe what they actually do.

JAGS (02:08:40.059)
Yeah, well, yeah. Well, and I think that's part of the problem, right? Like I obviously I am not with Stairwell and I went off to S1 and I've been at Sentinel One almost five years now and I'm really grateful and happy with what I've been able to build at Sentinel One. So I'm in no way here like pitching for Stairwell. I actually like that meme of like the cartoon guy like poking at a thing with a stick going do something like that's been me staring at Stairwell for like the past two years going

Here's your fucking chance, Google just pushed virus total to do a P move to like basically do price discovery higher and higher and higher to find who your whales are and how much you can force them to pay. then like everybody else can get fucked. Like that's a P move and that's usually not what you would expect from a multi-trillion dollar business. Or maybe that's exactly what, yeah.

Ryan Naraine (02:09:33.401)
That's the Stanford MBAs do at Google, though, right? Yeah.

JAGS (02:09:35.971)
Exactly. Yeah. Some, some fucking Mackenzie or like Boston consulting group, you know, genius decided that this was the way to go about it and is effectively destroying the, the, you know, the threat Intel industry and ecosystem in the process. so I'm, what I'm saying is like, I have attempted to put something together to do something like this before and a it's not easy at all.

Right? Like there's dynamics that you want to, there's the technology, which I think you can build some pretty amazing stuff now, a lot easier than when we tried to do it. just on cloud offerings and data bricks and stuff like that. It's not as hard as it was when we tried to do it. then there's like the problem with stoking a community and serving, sourcing files that are net new and unique. Like that's something that I think VT has gotten pretty weak on, for quite some time because

of well how other companies abuse that model. And then I would say that part of the difficulty here is

basically competing with VT. Like I think that the biggest thing that keeps some of the potential competitors in line is this kind of like fear and apprehension, the same fear and apprehension I feel when I talk about VT because like I love it and I never wanted a replacement. I wanted VT to just be the thing everyone contributed files to and like the one thing that enabled all of us and hey, it's our friends who are all in.

Ryan Naraine (02:11:10.105)
Monopoly is never good.

JAGS (02:11:12.433)
Yeah, I agree with that. like, so that's why I want like, I want Pasquale to succeed with rational edge, right? Like that's a that's a VT like front end that's doing VT like things, but new cooler processing things. And and it will let you and it's designed to hunt and it's information dense and it's not meant to be a see so panel slapped on a technical platform, right? Like it's so, you know, I'm all for it. At the same time, I look at Pasquale's thing and you know,

He's a small shop trying to do a very big job that also includes the complexities of, for example, if you want to be really successful, how many files are you going to fucking store, man? Are you talking about, you know, six petabytes, eight petabytes, 10 petabytes? First of all, can you get them? Can you get good ones? And second of all, can you store them and process them? Right. So Pasquale is building the front end that Stairwell should have built.

Costin Raiu (02:11:56.671)
Hmm.

JAGS (02:12:09.672)
Stairwell has the backend that Pasquale should hope to have. Stairwell's got the scope that VT should have had. And VT has the infrastructure, the files, and everything to do everything everybody else is doing, and they just don't. They just fucking choose not to, right? It's a fucking bizarre space.

Ryan Naraine (02:12:13.497)
So somebody's gonna acquire somebody.

Ryan Naraine (02:12:25.209)
and all the...

Ryan Naraine (02:12:31.501)
And that's the round answer to why we haven't seen competitors pop up all over the place. It's just a deep complex thing. All right, guys, we're about two hours and 15 minutes in. Costin, can we please close the show with some shout outs? You got anything this week?

JAGS (02:12:45.299)
You

Costin Raiu (02:12:46.849)
Well of course, shoutouts to our good friend Mark who was at the Bucharest Cyber Security Summit. I wish there were more conferences to meet up with the old friends, people who've been in the industry and they have so many amazing stories and I wish there were more presentations about old stories, paleontology and kind of things which may otherwise get forgotten if you want.

I think one knows what I'm talking about and hopefully there will be some interesting presentations. I heard that actually a fantastic presentation proposal was rejected by a state of statecraft which makes no sense in my opinion. I wish they would somehow reconsider or perhaps they didn't know what that story was about but it was... of course we know but we're not gonna blow it.

Ryan Naraine (02:13:39.481)
Do we know which one it is? We're familiar with what the talk is, right?

Costin Raiu (02:13:45.093)
We, we, think we're familiar. It's something we've been waiting for a long time. Yes,

Ryan Naraine (02:13:47.299)
Nice.

JAGS (02:13:47.635)
Kostin! Kostin, you should be glad that that didn't happen because they're not recording the talks and you and I can't be there. So...

Costin Raiu (02:13:55.167)
we can't be there. I got it. Okay, next time.

Ryan Naraine (02:13:58.421)
Alright, you guys are not gonna be at Matonus' state of state craft because of binding hook which is compa-der-

Costin Raiu (02:14:03.647)
Correct.

JAGS (02:14:04.136)
I mean, we would have to essentially like haul ass out of Binding Hook and like get on a two hour train to try to make the conference like the next morning. And I just, I don't know that that's really, the last time I tried to rush coasting onto a train, we both fell. we like, dude, we almost, we had presented Equation and Sophacy to Apple at Apple headquarters back in the day and like,

Costin Raiu (02:14:23.056)

god, no.

Ryan Naraine (02:14:32.057)
I had to make it to San Francisco, right?

JAGS (02:14:33.903)
Yeah, and like we had to make it so everything was like the train was about to leave. Kostin had bought an iPad like for his wife. Like we had all this. I bought like these like Japanese ceramics that they sold at the thing and we're grabbing all this shit and I just see the train starting to go and I'm like, Kostin, we could make it. We fucking rushed. We both fall on the steps. All of our shit is like broken. It was a fucking mess. So I know better than to try to rush Kostin onto a train. was an undignified way to go. So we'll stick with Binding Hook.

Costin Raiu (02:14:43.012)
beautiful.

Ryan Naraine (02:14:48.642)
You

it

Costin Raiu (02:14:57.023)
You

Ryan Naraine (02:14:59.705)
Shout out to Max Smitz and all the speakers at Binding Hook Live. saw the agenda was posted, looks solid as usual. State of state craft also happens.

JAGS (02:15:08.317)
Dude, the venue looks amazing.

Costin Raiu (02:15:11.172)
with a rotating stage or something like this, like a circular

JAGS (02:15:13.651)
Yeah, it's a road like you're in this. You're in the center of the circle like this. Like it's it's cool. It's going to be cool. Sorry, Ryan.

Ryan Naraine (02:15:20.237)
Conferences are not easy to run. They're a pain in the ass. So my, my shout out to all the organizers grinding through getting those. hopefully you have a very, very smooth conference. Anything from you Juanito?

Costin Raiu (02:15:20.766)

Whoa.

JAGS (02:15:31.431)
Well, I mean, I cut you off before giving a shout out to State of Statecraft, which is also our friends. Our buddy Maton is putting this together. It actually looks amazing. I'm glad some of the labs guys will be there. I won't be able to make it, but I will be there in spirit and actually quite jealous of missing some of the talks. So.

Ryan Naraine (02:15:50.753)
No recordings, no recordings, no publication, no journalists, no nothing. So that's one of those dark conferences. think there's a little Dave Itelber raised this on his Daily Dave newsletter this week. He did some light coverage of offensive AI con. And one of the things he said was, you know, a lot of these invite only conferences put the right set of people in the right place to talk comfortably and confidently about things in a trusted environment, blah, blah. But on the flip side of that, we're all talking to the same set of fucking people over and over and over again.

JAGS (02:16:19.795)
Yeah.

Ryan Naraine (02:16:20.696)
if we're just inviting our friends and our friends, right? We're not really expanding it and we're leaving a lot of folks out, a lot of folks who are early in their career that don't have their networks and so on. So there's a little bit of a balance that needs to happen here. I'm not a big fan of these dark conferences. I feel like if you want to do a dark conference, don't even fucking publicize it. Just go in your corner and do your conference.

JAGS (02:16:33.831)
well.

JAGS (02:16:40.613)
Well, let's be honest about why this is happening. Let's put the fucking onus where the onus belongs, right? Most of these conferences are becoming like even ours, which is not like we, know, LabsCon is supposed to be recorded and we push out the videos. We actually just put pushed out our first video this week, which is Martin, Martin Wendiginson's talk with Brad, like the folks from from Dreadnought. Great talk. So go watch that. But

Costin Raiu (02:17:01.534)
Mm-hmm.

JAGS (02:17:07.495)
we put half of the talks on the keynote day were off the record. And it's not because like some of them had legitimate like law enforcement ongoing, blah, blah. But a lot of them was just like, I don't want to get in trouble with this vendor or like my employer is going to give me a hard fucking time. So really what you're describing, Ryan, is true. We are well, yeah, it's it's becoming

Ryan Naraine (02:17:27.448)
Conferences are going away. That's what I'm saying. Real conferences are going away.

JAGS (02:17:32.455)
they're becoming kind of like, you know, work like industry workshops for insiders, which I'm happy to have. And I'm I'm supporting and I'm helping to build and I'm glad our friends are doing it. But the format is a response to the industry and the way that that vendors are treating their employees, not really to the sensitivity of the material per se. And for anybody who claims that we need to scale up the industry and

Ryan Naraine (02:17:55.722)
I agree. It's just a...

JAGS (02:18:01.352)
You know, we need so many more people to be able to join and blah, blah. I don't see any legitimate mechanisms by which that's being fomented. If anything, we are making it incredibly hard to get into this space. And we're doing so at a time when there's another very, very, very, very hot area. So if you're going to go learn and cut your teeth and try to get into a space and you look at it it's like, it's going to be hard securities here, hard as fuck, hard to get into.

Not that hot as far as like the hiring goes. AI is over here. Whatever the fuck happens, if I spend any time learning AI, I'm going to make a shit ton of money. Anybody who's trying to get into a new industry is going to end up over.

Ryan Naraine (02:18:44.898)
You know, for these invite-only conferences talking to ourselves, like, we need to talk to the industry as a whole.

Costin Raiu (02:18:49.679)
Yes, I know the perfect event countermeasure conference which is just coming up with less than a month away Well less than a month away countermeasure in Ottawa. All three of us will be there. Hopefully everybody's got tickets booked and visas all booked

Ryan Naraine (02:18:53.793)
yes, can you give the pitch quickly?

JAGS (02:18:54.355)
I see.

Ryan Naraine (02:19:03.734)
Everybody's got tickets and all booked

JAGS (02:19:06.895)

Everything, we're there. It's happening.

Ryan Naraine (02:19:08.568)
Oh, we're looking out for our Canadian friends as well. Costin and Vitaly, you guys are doing some training, some paid training there ahead of time.

Costin Raiu (02:19:14.109)
I am afraid so Vitaly's training I think I got it get canceled, but I still have a few seats available for my iOS forensics and malware hunting training. So if you're worried about all this Apple warnings and meta warnings that you don't know how to start a an Apple forensics program to protect your CEO or at least to try to determine when they get hit.

Ryan Naraine (02:19:19.16)
Uh-huh.

JAGS (02:19:19.443)
No.

Costin Raiu (02:19:42.087)
do look into the trainings that I will be providing at countermeasure a bit of shameless self promotion yeah come come come come

JAGS (02:19:48.147)
Suffer motion. Good.

Ryan Naraine (02:19:49.528)
And that's the weekend of November 7th, believe. Juanito, you and I are gonna sneak in and get some free training there, at least get the...

JAGS (02:19:56.34)
I think we might be a little too late to really get anything out of it. Like I said, like Kostan's gonna teach the dedicated smart man's way of doing it and then you and I are gonna be in the back like, well, maybe if we just pay for this one service and we try this other thing, we can have the cheap man's version. Let's see.

Ryan Naraine (02:19:59.605)
Might be late.

Ryan Naraine (02:20:16.247)
All right, let me close the show with one last shout out to Tavis Armandy who announced last night that he's leaving Google project zero after 20 years there. Very much, very much an early influencer of how disclosure happened and had a really, really unique approach to things. Over the years targeted AV vendors a lot specifically and forced us to

Costin Raiu (02:20:17.116)
possible.

Costin Raiu (02:20:22.46)
Mmm.

Costin Raiu (02:20:35.292)
You

JAGS (02:20:36.665)
End of an era, man.

Ryan Naraine (02:20:44.833)
take things a lot more seriously. Tabas, in my book, I have a conflicting relationship with Tabas. Back in the day when he used to drop Microsoft Zero Days, I was a blogger at ZDNet writing about cybersecurity issues. And I was somewhat critical of him saying he is the arbiter of what the threat landscape looked like. So he decided, you know what, I think someone else will find this, so fuck it, I'm just gonna drop all day here. Turns out he was right.

Costin Raiu (02:20:45.062)
How is he in your book?

Costin Raiu (02:20:53.66)
Fill us.

Costin Raiu (02:20:58.187)
Ooh, okay.

Ryan Naraine (02:21:13.751)
Uh, his approach and, and, and over the years I've come to record, respect his work. And I got, I got a little story I want to tell here on September 4th, September 4th, 2015. If you go check, you'll find that that was a Friday evening at 7 45 in the evening. Davies dropped a tweet CCing me saying, okay, the first Kaspersky exploit is finished. It works great on 15 and 16. I'll mail the report after dinner. CC Ryan around with a screenshot of him popping calc, right?

Costin Raiu (02:21:21.5)
Tell us.

Ryan Naraine (02:21:42.485)
This is Friday night, 7 45 PM about a few minutes late. says, by the way, it's remote zero interaction system exploit and default config. So about as bad as it gets. And he tags me again. So this is a Friday night. I'm scrambling to call Costian. It is three in the morning there. We're trying to figure out if this is worth it. Turns out we worked over the weekend on this and I'll give

the point of the story is the Russians who were responsible for this on the product side at Kaspersky.

Wanted to get on the phone with Tavis because the back and forth over email and the time zones were, and they wanted to treat it with a sense of urgency. And they wanted to get on the phone with Tavis to kind of just like walk through the exploit and what he found. Tavis said to me, Ryan, I don't get on the phone with anyone. This is a disaster waiting to happen. We are going to stick to email. And it took a lot of back and forth with me basically saying to Tavis, please trust me on this. These guys need want to work on it. They want to work on it. He actually got on the phone with the Russians. He broke his policy.

got on the phone with the Russians and actually included me in all the back and forth going all the way through to when all the patches were issued. So on this day when we're doing shout outs, I want to shout out Tabis for being a net positive in general and being okay in my book. And I wish him all the best with whatever he does. Is he okay in your book, Costin?

Costin Raiu (02:23:02.236)
Absolutely, I mean, I remember we fixed that vulnerability and like record the record time. He actually I think he wrote he said nobody ever fixed a vulnerability as fast as the guys from Kaspersky that right.

Ryan Naraine (02:23:09.845)
He did.

Ryan Naraine (02:23:14.935)
That is correct. That is correct. I believe I got 10 % bonus for that. So thank you for.

JAGS (02:23:20.9)
Hahaha

Costin Raiu (02:23:21.051)
It's always either plus 10 % or minus 10%. This time it was plus.

JAGS (02:23:24.659)
mine. 8even's out.

Ryan Naraine (02:23:26.871)
Absolutely. Godspeed to Tavis. And with that, we'll catch you guys next week. Thanks everyone.

Costin Raiu (02:23:32.068)
Ciao.

JAGS (02:23:32.371)
Thanks guys.