Episode 75: The Three Buddy Problem

APTs pounce on React2Shell; BRICKSTORM backdoors; .gov surveillance

NOTE: The transcript is auto-generated by an AI tool, with obvious misspellings and errors. This doc is open for copy-editing via **Suggesting** mode. <3

Cast:

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

WATCH YouTube Livestream

https://www.youtube.com/watch?v=7IkmOXujJTY

Listen everywhere

https://episodes.fm/1414525622

JAGS (00:00.62)

I took the fucking red eye just to like make sure I'd get out of SF as soon as possible and then like make it for this recording. But I haven't slept like at all. Like I've slept like three hours I think. So this is good. Yeah. Yeah. My apologies to you whoever the fuck I piss off today. We're gonna have a great time.

Ryan Naraine (00:13.317)
This is the best one, Ito.

Ryan Naraine (00:21.073)
Why the wake Juanito is the best Juanito. Hello everyone, this is Episode 75 of the Three Buddy Problem. We're back with a new episode on the, what is this? Saturday, December 6th. So heading into the holiday season, but of course we have an explosion on our hands. At least we have a big story to get to today. Before I get to this, uh, before I get to the news, just a quick check in with Costin, how are things in Europe?

JAGS (00:23.532)
Yeah.

Costin Raiu (00:44.702)
It's the end of the year like today is this St. Nicholas. I don't know if you celebrate it in the States. It's like a day when children It's a day when children well nice very nice behaving children they get some kind of gifts like chocolate candies and whatever and the not very nice kids the not nice kids

JAGS (00:52.462)
the fuck is that?

JAGS (01:08.117)
MSN Day.

Ryan Naraine (01:10.501)
like a pre-christmas?

Costin Raiu (01:12.272)
It's like a pre-Christmas exactly and yeah, it's St. Nicholas Day in theory. yeah, it's on December 5th and kids which are not nice, they get coal and yeah, sticks for beating.

JAGS (01:20.11)
Fuckins.

Fucking socialists.

JAGS (01:29.154)

fucking socialists look at how many holidays right it's not one Christmas it's got to be pre Christmas then Christmas then post Christmas Orthodox Christmas

Costin Raiu (01:37.49)
the end but like you're next with all this like St. Valentine's Day

JAGS (01:43.486)
I remember you remember KL like the it was fascinating, right? Because most companies in the US will just stop doing any fucking work whatsoever in December. But the Russians would do that in January. So there was like two months where nobody was doing shit. Like we're just working and you're like, I think everybody else died.

Ryan Naraine (01:44.571)
Happy.

Costin Raiu (01:49.584)
March 1st.

Costin Raiu (01:54.235)
Hmm. Seems in January, correct.

Ryan Naraine (01:58.929)
Probably still is.

Costin Raiu (02:02.717)
January was the best, most productive month because you could finally get back to all your projects and work on them without anyone bothering you, without your boss bothering you. Everything was fine.

JAGS (02:07.399)
It was amazing.

JAGS (02:12.928)
we could we get a January hiatus just enforced at all companies just just recenter yourself take a little time hit your stride again.

Ryan Naraine (02:22.5)
Before we get to the show Juanito you mentioned just jumping off a flight. Where were you? How were things in your life?

JAGS (02:27.47)
I was in San Francisco, I had to go to the office, Mountain View, see some friends from Singapore, amazing folks, and get to check in on Gabe and St. Meyers, Cyber Dad. So just planning, you we've got a lot of stuff happening at Labs and a lot of change for the better, for

really interesting work that we're doing. And there's no point trying to fight people on publications in December, so everybody can just knock themselves out.

This December is the Friday of months, right? It's when you like publish your stories that you don't want anybody whatever dirt people have been sitting on all year. Now's the time.

Ryan Naraine (03:07.728)
doesn't feel like that this week though. I feel like there was a bunch of dumps this week. In addition to the React stuff, there was a bunch of big important threat intel reports, surveillance reports that just kind of dropped.

JAGS (03:12.269)
Yeah.

JAGS (03:18.222)
Well, now through next week is when you publish. After that, if you have a competent PR person in your team, they'll tell you to go fuck yourself if you want to publish something like what, at Christmas? You think that this is what people are going to talk about?

Ryan Naraine (03:23.341)
I see.

Ryan Naraine (03:33.073)
Before we get to the news, I want to do a quick bit of house cleaning if the audience would allow. I wanted to say thanks to Material Security for the sponsorship last month. They sponsored the entire month of December. Good partner to have, they'll return again in 2026. This episode is sponsored by ThreatLocker. Costin, I think you said you were able to look at the website. You looked at the website and it a pretty interesting product. We'll talk a little bit about ThreatLocker in the future episodes, but ThreatLocker is going to be sponsoring the show for the duration of this month.

And then we have Haroon Mir thinks Canary has signed a contract to sponsor some episodes in the new year. have TLP Black officially on board as presenting sponsor. So very happy to have all these sponsors aboard. This is not an easy show to sponsor because we talk a lot of shit. appreciate the support. Appreciate the support from those folks. And if you guys in the audience are in need of products in these categories, I want to say we'd be happy if you'd show some support for them.

JAGS (04:16.782)
Took a lot of shit.

Costin Raiu (04:20.527)
Thank you.

Ryan Naraine (04:33.454)
With that out of the way, Kostin, I'll start with you. Have you re-downloaded Chrome? Last episode you mentioned you don't use Chrome anymore because it has this ESET anti-virus engine in it built into it that automatically does a scan. Billy Leonard from Google Tag, who's a global head of state-sponsored hacking and threats over there said, hey, Kostin, what up? Cleanup tool was removed from Chrome almost three years ago. Happy to have you back. So have you downloaded Chrome since? Are you happy now that...

JAGS (04:33.742)
actually love it, man.

Ryan Naraine (05:02.662)
all as well.

Costin Raiu (05:03.97)
no, mean I have Chrome installed. I never said that I don't have it installed. have it exactly. And I think the most important thing is always to be unpredictable. like for a long time I've been using Chrome with the Firefox user agent, Firefox with the Chrome user agent. So whenever like some...

Ryan Naraine (05:07.876)
You just don't use it.

JAGS (05:21.846)
motherfuckers on opera this week.

Costin Raiu (05:24.316)
I wouldn't say yeah to be honest Opera I don't use a lot but Vivaldi is interesting as well I mean all chromium based browsers are pretty interesting to play with and yeah thanks to Billy I didn't know that they got rid of the ESET engine from Chrome it doesn't even say and actually we had to check

Ryan Naraine (05:41.872)
But doesn't mention the ESET engine, he linked to an article. He linked to an article that says that the Chrome cleanup tool was removed, right? And that there...

Costin Raiu (05:49.5)
And we had to check like because they don't say we removed the ESET engine and I was like, okay, you removed the Chrome cleanup tool, but did you remove the ESET engine? Apparently the Chrome cleanup tool was the ESET engine according to ESET's website and on ESET's website, I don't think they say anything about this, seizing of this partnership in 2023, I think it was, yeah, 2023.

Ryan Naraine (06:01.648)

Apparently,

JAGS (06:11.79)
got against ESED bro. They're you know they're good folks. They're good people.

Costin Raiu (06:19.107)
So, yeah.

Ryan Naraine (06:19.952)
But there's a bigger issue here though, Where there's, let me just frame it in this way. There's not a bigger issue, but a larger discussion point here around a vendor having something problematic in there. Someone says, hey, it's not from me. I'm going to go in another direction. say, it's been removed. You're welcome to come back now. It feels like we're supposed to just kind of, I know it's not a big, I'm not making it into a big thing, but the idea that, okay, it was bad and now it's removed and you're welcome back. just feels like.

Costin Raiu (06:25.516)
Mm. Mm.

JAGS (06:40.686)
Nah.

Ryan Naraine (06:49.988)
Big company energy.

JAGS (06:50.99)
No, don't don't. No, no, no, come on. Don't don't problematize that because actually I think Billy is being pretty cool and coming in and say and saying that no, no, but I'm saying like I think Billy's being cool because if he doesn't mention ESET, I'm assuming he may not even like he may not even be in a position to mention them. But he is coming out and saying, hey, hey, like, no, don't worry about it. And like, frankly, I like it because

Ryan Naraine (06:57.912)
No, this is nothing against Billy, personally.

JAGS (07:20.46)
What's the alternative, right? Like the, we, we crucify them forever because they once had this thing in there, right? Like someone fixed it, somebody or somebody decided, you know, the contract was over, right? Like something, something changed, hopefully for the better. Who knows, right? so sorry, my, my cat just walked out and turned off the monitor. That's great. Thanks, man. something changed for the better, right? So you can't just kind of keep, keep Adam, right?

Ryan Naraine (07:50.384)

Fair enough, fair enough. But let me, let me, let me plant a, let me plant another conversation piece in here. After our last episode, I got a lot of incoming privately in the background around Microsoft's SFI secure futures initiative that has put all these check boxes in place and they're now so much better and security is the number one thing. And I keep getting all this shit PR shit into my head. Right. And the idea is that after the CSRB

JAGS (07:50.722)
That said, I'm...

Ryan Naraine (08:15.747)
They hired a new CISO, they restructured into 10 deputy CISOs or six deputy CISOs and they're doing all of these things. And you're saying, hey, let's sit back and scratch our noses and give them a chance because, and I'm like, at what point does the milk just continue to get spilled, the dirty milk?

JAGS (08:30.624)
saying give Microsoft, I'm sorry, sir, I'm not giving Microsoft a chance. said Google, like Billy coming out and saying some like telling us like a fun tidbit is something that I would like to encourage. I would like to hear I would like to hear from Billy Leonard every day of my life if I could. love the dude. But like I that is does not translate into somehow being cool with like Microsoft in the new layer of like bullshit bureaucracy that they've

Ryan Naraine (08:43.961)
same.

Ryan Naraine (08:48.334)
Fair enough.

Ryan Naraine (08:57.027)
But I like the people that are whispering in my ear that the SFI is moving in the right direction and Microsoft is massively improving and so on. These are my friends. These are people I like who are inside Microsoft and trying to make things right. So I throw it back to you is like, we being played by our friends?

JAGS (09:06.84)
They're telling you SFIs, they're telling you SFIs working well.

JAGS (09:17.046)
I don't know. This motherf- I'm sorry, I just landed and the cat is going wild. Bro.

Ryan Naraine (09:21.113)
Custed this guy and his cat. want to just close this on the Google Chrome thing with you

JAGS (09:25.238)

No, look, I'm trying not I'm not trying not to talk about the Microsoft thing, but I feel like you're you're almost baiting me like we are all hearing from people at Microsoft and we're hearing completely divergent fucking stories about a bunch of different shit.

Ryan Naraine (09:39.939)
When do I ever beat you? Stop it.

JAGS (09:41.9)
What the?

Ryan Naraine (09:45.262)
No, but you get the point, right? You get the point. It's like, there's a lot of, there's a lot of marketing and PR about how much better we've gotten. Chrome is no better because the Chrome, the cleanup tool is removed. And I get your point. This is Billy basically saying, listen, we didn't even like it inside here. You know, it was one of those business things. And that's how I read it there. Costi, you says, we say in Romania, once you get burned with milk, you blow into the sour cream too. And that's the point I'm making is like, at what point are we just blowing on sour cream all the time?

JAGS (10:15.426)
This is, this is, this is.

Costin Raiu (10:15.928)
I don't know man, but physically this happened to me like when I was little I absolutely got burned with the hot milk and then I was blowing into yogurt, sour cream, So I don't know, it's a power of habit. It's when people, I think when people see one kind of thing that they don't like, then it takes like a lot of effort to change that perception. I mean,

I think Chrome is doing some amazing things in terms of security to improve security to make it more resistant to exploitation. It's probably kind of ages ahead of other browsers from this point of view. And at the same time, I feel that you are the product with companies that essentially give you free stuff. You are the product. And then it means that

you need to pay with your telemetry, need to pay with your data. So they just have to find ways in order to compensate and to balance that product. And I think that what they even say this in the blog when they say goodbye to Chrome clean up that this got actually was replaced by things like, you know, checking your downloads whenever you download the file that is being checked against Google.

security backend services and I think the nice thing there is that you can actually turn it off. yeah, this safe browsing in Chrome. Yeah, can, like, while Defender, it's extremely difficult to turn it off. And I also like this, I don't think we talked enough and we talked a lot about this enhanced protection that Google offers. And I do have friends who actually, they reached out and they enabled.

Ryan Naraine (11:46.359)
unlike your defender experience,

Costin Raiu (12:06.571)
this enhanced protection. By the way, do you guys have this enhanced protection enabled in Chrome?

Ryan Naraine (12:12.783)
I didn't even know. I don't.

It's not something that they evangelize.

JAGS (12:16.568)
Wait, now I feel truant, yeah, like am I, what the fuck?

Costin Raiu (12:19.05)
mm-hmm mm-hmm yeah so what does what does enhanced protection do like the the fastest the strongest level of protection against dangerous sites real-time URL checks so like I like your thinking I like I like your thing more advanced more advanced vision based vision detection

Ryan Naraine (12:21.593)
Terrible security people.

Ryan Naraine (12:31.023)
So there's some business analytics happening in the background is what you're saying.

JAGS (12:33.816)
mean, real time URL checks is, that sounds like safe browser. This sounds like, this is just safe browser shit.

Ryan Naraine (12:37.391)
Busted.

Wait, this is not safe browser shit. This is business analytics intelligence collection.

Costin Raiu (12:47.849)
Vision-based fishing detection. Yes, client-side. Client-side vision-based fishing detection. Interesting. Interesting, interesting.

JAGS (12:48.344)
Vision-based.

Okay, okay. shit, my, okay. Yeah, I've had my shit off. What am I doing here?

Ryan Naraine (12:57.369)
But the point you're making, Costin, is that although the clone cleanup removal tool was removed, the intelligence collection hasn't stopped. It's been replaced with something else and you're still, you're still the product. And in this case, you are this business analytics data collection thing in the bag.

Costin Raiu (13:01.559)
Mm-hmm.

Costin Raiu (13:12.248)
I'm saying like Google is, I think they're struggling and they are like really doing an amazing thing, providing a security solution, something that tries to protect people, right? And this may actually be very good and very, very well suitable for the vast majority of people out there. But I think that, I don't know, for security researchers, for paranoid people like myself and maybe others who run a...

Pie hole servers with block list firewalls to try to block telemetry and so on because why because we have NDAs and because we honor TLP black style Data that we receive from others and we don't want that data being leaked through telemetry through defender and through other mechanisms So that's why people like myself. I may be a bit more paranoid So in no way I was trying to say that Google Chrome is is not an awesome browser like

Probably the safest out there and by the way I've seen cases in the past when people were running other things like brave, know Chrome chromium based browser and they still got owned with zero days So it doesn't necessarily mean that if you use a chromium based browser You are more secure than running Chrome itself. Actually Chrome itself is probably a pretty nice ecosystem the way it works

JAGS (14:36.376)
Yeah, that's an interesting... So I think of Chromium like democracy. It's like the only thing worse than a Chrome based browser is a non-Chrome based browser. In the sense of like I feel uncomfortable about all the stuff that's shoved into it. The malware removal tool, I don't even know that that was like my primary concern just because the entire architecture of Chrome is...

like a very strange, very like all encompassing. If you look at it as from like a behavioral log perspective, it does everything that you don't think an application should do. Like it's a heuristic nightmare for a lot of detection stuff, just because it does all kinds of weird shit. It has like persistent update mechanisms and like all kinds of things that just, you know, are running in the background.

Interesting thing right now that you mentioned this enhanced protection and I was like I went looking I'm like, you know, I feel like I fucked up right I should have turned on whatever the enhanced protection is and then you go look at it and you go well actually When you turn on

enhanced protection like Look at they're putting it right on the tin, but that is where it's sending URLs that you visited small samples of page content downloads extension activity system information

Costin Raiu (15:38.678)
Hmm.

JAGS (16:03.362)
for to Google safe browsing, right, which would be the broader sort of checks on that kind of stuff. It talks about in depth scans of suspicious downloads like you're basically saying turn on the AV component of Chrome. Chrome component. Yeah.

Ryan Naraine (16:19.598)
which was the problematic thing in the first place, because Costin has no problem with ESET. It's just this AV component of the browser,

JAGS (16:27.724)
I just, dude, you know what I was thinking about? Like I was praising Google DeepMind last episode about the whole alpha fold thing and then, you know, being willing to do all this protein folding stuff and then just put that out into the world so that everybody could use it. I would feel so much happier, so much more comfortable if like I knew that all of the samples collected from safe browsing and from the internet scraping and from, you know,

the VT sharing and whatnot, if that was somehow going into like a collection for the world, you know what I mean? Like if Google had instead decided, instead of like trying to make paltry money out of like, what is paltry money for Google out of VirusTotal? If they decided like, you know what, this is gonna be like a research tool for like all researchers who look into malware and we can just have one ginormous database with the one.

company that knows how to handle ginormous scale data on earth. would have been, it would be like a service to humanity. I mean, a much more niche one, but I would feel, I say that not, it's like a weird tangent, cause I just, I'm not speaking as smoothly with so little sleep, but like it would make me feel a lot better about shit like this. Like, you know, this internals, the file explorer, the,

task manager replacement that they have, it will automatically send samples to VT. Just, you know, if you set it as like the task manager replacement and stuff like that. Cool. Like, I mean, in a sense for some people, right? Like you're checking side loaded DLLs as to whether they're signed, whether it's the right hash and like sending stuff. Okay. If you were telling me that that stuff is going to the same repo that we all work off of.

and we all work off of it and it's not like a price thing, it's not a, can you afford to use VT? I would find it less objectionable. I'd just be like, well, we're all contributing to the same fucking place, right?

Ryan Naraine (18:38.712)
My beef with Chrome is like, can you get fucking search to work? Like they're using this AI generated search result at the top and it's all trash. It's in many cases just completely incorrect because I tested things that I actually know. It is so bad. And the same experience I'm having a great experience with Gemini, testing Gemini as an AI tool to do some stuff. The experience is great, but Google can't use it for their own search. That's crazy to me. And then the other thing just to close the loop on this from my side is,

Costin Raiu (18:41.076)
.

Costin Raiu (18:54.58)
you

JAGS (19:04.033)
Duh.

Ryan Naraine (19:08.93)
The way the two vendors deliberately not make each other's services work on their Chromium Brace browsers, like Google like affecting if you log into a Microsoft service or you go on to my, you know what I mean? Like they're just kind of like making things a little wonky. The calendar doesn't quite look right and all this shit is like, come on guys, but what are we doing?

JAGS (19:24.994)
Meh.

You ever tried to use Google Docs on Safari? This shit doesn't even work. Yeah.

Costin Raiu (19:30.498)
you

Ryan Naraine (19:31.022)
This is my point.

Anyway, let's move on to the big news of the week. is early December and it had shades of log for Shell. is React to Shell. React to Shell is a React unauthenticated remote code execution, CVSS 10 out of 10 reported to the Facebook team on November 29 by Lachlan Davidson by the Meta Bug Bounty program. Apache was a CVE 2025 55182 Apache shipped on December 3rd. Pretty impressive timeline.

Costin Raiu (19:58.644)
. you

Ryan Naraine (20:04.926)
to get a big patch like this out. Obviously everyone's hair on your neck is on edge. Kostin, why is this a big story?

Costin Raiu (20:14.803)
It's a big story because it's a very dangerous thing which has the potential to affect more than half of the internet. The reason is that this React project became incredibly popular. I was thinking that pretty much everybody nowadays they use React or one of the kind of connected projects that are

Also vulnerable like of course another example is next.js They're just almost everywhere they used to everyone die actually I know people who got owned already as of yesterday who got owned so this Exploitation is already happening out there on the on the internet on a massive scale So there's like random scans going on against pretty much anyone so assume that if you have one of the vulnerable versions

for CV 2025 55182 there's a pretty good chance that at least someone poked you to try to see if you're vulnerable at least if not they already tried to exploit it and I've seen for instance in one case the attackers they first tried to see if there's like a PowerShell available trying to run PowerShell seeing obviously was a Linux system moved on to running WGAT things like that

to download and run cryptocurrency mining software, obviously the cyber criminal side of things, but also APT groups have already been starting to exploit this bug. And it's pretty straightforward in a way, it doesn't take a lot of effort to exploit it and since POCs are already available, I think...

yeah this will be pretty pretty big it will be in the same category as previous cases

Ryan Naraine (22:13.965)
Let me give a little bit of background. The vulnerability is present in versions 19.0, 19.1.0, 19.1.1, and 19.2.0. I mentioned report it to method. is React was actually created by Facebook when it was Facebook by the method team and it's adopted widely across the tech ecosystem. It's kind of like.

Costin Raiu (22:32.708)
Meta, Netflix, Discard, Shopify,

Ryan Naraine (22:36.009)
All kinds of internal enterprise dashboards, SaaS platforms, widely, widely deployed. Quick question. Do we know if it's easy to patch? Cause sometimes these things are not easy to patch.

Costin Raiu (22:43.794)

no, this is a I would say it's a pain in the ass to patch. it won't I think we won't get patched automatically. So here's the deal with other things. Imagine that you have like a Linux installation like Ubuntu and you have unattended updates installed and that basically takes care of all big vulnerabilities automatically. It will download and patch things automatically for you.

Ryan Naraine (22:50.422)
Really?

Costin Raiu (23:12.614)
So you have the kind of the peace of mind. Now, because this is a kind of an ecosystem inside of an ecosystem, it will not be patched automatically. Even if you have all these things like automatic updates on because the vulnerability is in the framework that you use to develop your website, your front ends, whatever, then you need to do the patching like

manually need to rebuild your project you need to fetch the new versions which are not vulnerable and then to rebuild and deploy the project that's that's one I think that to There was also an interesting cloud flare outage which happened Yesterday

Ryan Naraine (23:55.438)
Correct, they had a 30 minute outage, 30 minute outage yesterday and according to the Cloudflare status update, it was tied to this. They were in maintenance mode, probably doing some manual patching, the same kind of things you're talking about.

Costin Raiu (24:04.812)
Exactly.

And this is what I mean because the possibility to block these attacks, I mean, these can be also blocked by some kind of web application firewall. if you can't patch easily, like I think that yesterday a lot of people simply put their websites offline because they couldn't patch in time. So it's better just to take it offline. I think it's the right decision.

Ryan Naraine (24:33.132)
Bye.

Costin Raiu (24:35.063)
And until you figure out how to patch it, then you patch it, you redeploy, that's fine. But if you have a web application firewall, then probably that can work as a kind of intermediary solution until you manage to patch the code. yeah, it's kind of crazy how, you know, things are being built in other things. Ecosystems within ecosystems is the new danger nowadays.

Ryan Naraine (25:02.783)
Yeah, this is the kind of software supply chain complexity we talk about, right? It's like ecosystems within ecosystems and little tiny computers running inside tiny computers inside an operating system. And each has their own unique way of being patched or even updated. And it

becomes crazy. You mentioned APTs have already pounced. And before we get into what we know about the APTs pouncing, is there a way for us to know if this was ever...

exploited and compromised prior to this guy's discovery. Because that's always an issue for me is that, you know, bug discovery collision, it, will we or could we possibly ever know that someone's already exploiting this prior to, because the bug was there.

Costin Raiu (25:42.673)
What I can tell is from what I have seen. So I looked for signs of exploitation or I looked in the logs, in logs for the honeypots that are available to us and websites that I manage. So I looked for signs of exploitation. And although it looks to me that the vast majority of poking begins on December

Ryan Naraine (25:50.445)
How?

Costin Raiu (26:11.697)
and spikes absolutely like crazy on December the 4th. There's another incident that I see on November 24th which may or may have not been related to this but considering that also it could also be

Ryan Naraine (26:23.564)
Mmm.

Ryan Naraine (26:27.796)
It might've been Lackland doing his research. Cause he reported it on November 29th, by the Meta Bug Bounty Program.

Costin Raiu (26:35.92)
possible on what on october what on november what 29 okay so it may be i i can't tell you for sure what it was but it looks like yeah there was another poke on november 24th which seems related then the algorithm that i that i was using to try to identify this exploitation applying it for the entire year it yields hits

Ryan Naraine (26:38.77)
November 29th, so five days later than your November 24th.

Costin Raiu (27:04.616)
one hit on 24th, one on the 2nd of December and then a lot on the 4th, beginning on the 4th. So it would be good to know but unfortunately due to how this bug gets exploited it doesn't leave a lot in the server logs because it happens through the headers if you don't log the headers in your server logs it will be hard, essentially hard to catch it.

Ryan Naraine (27:11.232)

Right, that's when the patch dropped on the third.

Costin Raiu (27:33.807)
And the other thing is that we've seen like the entire exploitation process here can be very, very silent. It might not even, you know, produce any kind of file artifacts on disk whatsoever. So it can be almost invisible from the point of view of server auditing logs and so on. So it depends. I think it depends on what logging you have in your own.

react app if that app actually logs more requests then you can be lucky and try to to dig through there and otherwise if you haven't patched until today December the 5th I would very the 6 actually I would very much say yeah consider consider yourself at least owned by at least one thing if not multiple things

Ryan Naraine (28:21.398)
yourself on right.

JAGS (28:26.542)
What makes this whole react situation so interesting is actually the well, the amount of vibe coding platforms that essentially default to react in the products they create. So one of the one of the folks that has been most like active on Twitter are the people from Versel. They they have this platform V zero, which is

Costin Raiu (28:40.425)
Use React.

JAGS (28:53.826)
fucking phenomenal at just like spinning up front ends. Like if you want a front end, you just go on VZero and go, hey, make me a Splunk-like interface that does this, that, and the other, and like spins up in 35 seconds, and you can just click a button. All of those applications tend to use React like quite heavily. And interestingly, I mean, they've been extremely proactive about...

Ryan Naraine (29:06.198)
they use these libraries, right?

JAGS (29:18.338)
Like I've gotten like emails and emails from all these different things. And like, I don't use anymore. I just tested them at some point. Just being like, you have to patch this and that. So it's cool that they're engaged at the same time. This is.

Ryan Naraine (29:33.772)
This AI death really...

JAGS (29:34.038)

I guess the earliest, yeah, this is one of the earlier incidents of AI, well, of AI promoted technical debt. Because think about it, right? Like the AI didn't necessarily do anything wrong. It's just using a component. But it's enabling somebody to create something in a snapshot where they don't, and chances are they don't have the skills themselves to monitor it or patch it. So.

Ryan Naraine (29:48.395)
No, no, no.

JAGS (30:01.844)
Yeah, you hopefully you still have your deployment kind of tied to this thing and you can go back in and just tell it, hey, you know, please update react. but I'm thinking about all the people who got vibe coded applications that they bought off of some dude on Fiverr, or some other gig site. like, those shits are never going to get looked at again, unless, you know, there's some kind of management deal that is coming with this. So I think it's interesting. I've been thinking a lot about sort of like a accumulated technical.

Ryan Naraine (30:20.652)
Yeah, you're fucked.

JAGS (30:31.576)
debt. We were doing sort of like predictions articles, you know, it's like the end of the year, you have to kind of come out with some predictions thing. And one of the bigger points that kind of stayed with me was from this podcast, a couple of episodes ago, we were talking about what happens when the yeah, what happens when the internet becomes unforgiving, right? Like what happens when you anything that can be exploited gets automatically exploited as quickly as possible. It's

Ryan Naraine (30:46.708)
Yeah, technical debt that'll come down the pike, right?

JAGS (31:00.319)
the dynamics of technical debt are getting really interesting.

Ryan Naraine (31:04.074)
Yeah. And the idea of Cloudflare as decentralized monoculture on its own, that every time Cloudflare has a little bit of a blip of something, the whole world feels it. That's crazy pants to me that we're here. Let's jump quickly to Costin, mentioned APTs have already bounced. Our friends at Amazon. Amazon threat Intel team has actually been churning out stuff with IOCs. So shout out to...

JAGS (31:15.939)
Hey.

Costin Raiu (31:21.901)

Thank

JAGS (31:24.556)
Yeah, yeah, yeah, they're on it.

Ryan Naraine (31:27.542)
Shout out to Amazon, I know I gave them shit but here we are, they're on it. They said within hours of the public's disclosure of this reactor shell thing on December 3rd, Amazon threat intel teams observed active exploitation attempts by multiple Chinese Nexus threat groups, including Earthlamia and Jackpot Panda. I hate these fucking names. Who are these people costing?

JAGS (31:45.39)
Jackpot Panda.

Costin Raiu (31:52.205)
I knew you were going to ask me like who are these peoples? Who are these peoples? Well Earthlamia obviously that's a Trend Micro name for a Chinese APT group. Luckily Trend Micro is one of the companies that actually publish a lot of stuff so they do publish a lot of blogs with the IOCs and you can find a lot of materials.

Ryan Naraine (31:52.49)
Who are these jackpot panda people?

JAGS (31:59.66)
These motherfuckers. Who are these monsters?

JAGS (32:09.996)
Obviously.

Ryan Naraine (32:21.216)
can connect things.

Costin Raiu (32:22.454)
Yeah, about their naming. Jackpot Panda on the other hand, I think there's very very little information available on the internet. I think you can find Jackpot Panda I think on the CrowdStrike website, but there isn't a lot of information, at least as far as I know about Jackpot Panda. So I may be wrong here obviously, but I think you can find a lot more about Earthlamia.

Ryan Naraine (32:31.5)
two different groups.

Costin Raiu (32:51.384)
CheckPortBond I think yeah, that's probably worth more investigations.

Ryan Naraine (32:57.184)
I know we don't fact check, but it's worth mentioning that Amazon says this doesn't affect AWS services at all. They're just sharing threat intelligence to help people figure out, figuring out the response. And what did we find in the blog? Any, any, any valuable, IOX, any sort of tools that can help flag this thing?

JAGS (33:03.918)
They're just being cool as fuck.

Costin Raiu (33:13.103)
yeah. So actually they have like four, there's four IP addresses in there as well as very, very super valuable indicators for me. They do actually say what to search for within HTTP post requests. So this next dash action or RC dash action ID request bodies with dollar, dollar at request bodies with status resolve model. So I thought I was like,

exactly the thing that people needed if they wanted to look a bit in their networks. I took the IP addresses they're sharing. I also looked for this across our honeypot. So me personally, I haven't seen these IPs hitting the infrastructure that I have access to. But I've seen a lot of other IPs from similar ranges, similar IP ranges, like some of these cloud providers that are

for one reason or another, they're like super friendly or preferred by Chinese APT groups like Vulture, like Chupa, Single Hop, these kind of things. There is a lot of stuff coming from there, but there's like four IP addresses you can search in your logs. One of them, I think it's associated with the VPN and one is associated with an unantibuted Pratt cluster.

and all these indicators which to me they were like super useful to spot the first signs of testing or attempted compromise against the honeypots that we have access to.

Ryan Naraine (34:53.013)
You mentioned earlier that a lot of the infections are seamless, so you might not even be able to spot it. Amazon mentions here that you can also check for unexpected process execution or file modifications on application servers. So there are some artifacts and traces that might help you. So shout out to the Amazon team. Juanito, you got anything good out of this?

JAGS (35:12.686)
yeah. I mean, look, I, I'm actually quite happy seeing this come out of Amazon. And this is a thing that this is one of those where you can see that, the, they met them. Yeah. I mean, they're doing their own honey potting and look, this is the kind of thing where when you do shit, right. Product placement doesn't feel shitty, you know,

Ryan Naraine (35:23.573)
Where do they get this kind of visibility from? know they mentioned this AWS mod pod honey pod.

Costin Raiu (35:26.878)
Mad, Madbot, right?

JAGS (35:40.59)
When you do shit where you're just like, hey, we happen to be doing this thing. Look at all that we know anyways, would you like to buy whatever? I don't give a fuck. I'm happy. Look, I'm happy because what did you do with it? Well, within the first 45 seconds while everybody's running with their hair on fire, you came out and gave us something useful. Thank you. Also good luck with your product, right? Like I think that's the right way to do it. So shout out to our Amazon friends, man. They, know, it's, it's a, we've made.

Ryan Naraine (35:47.211)
And here we are promoting AWS SmartBot, right? Yeah.

JAGS (36:09.982)
very big progress very quickly and I'm proud of those dudes.

Ryan Naraine (36:14.751)
Who alongside that we got a coordinated notice from the NSA CISA, this all of these multi-agency press release and advisory on BrickStorm backdoor that coincided with a threat intel report from CrowdStrike around Warp Panda. Warp Panda is a threat actor that's been targeting VMware vCenter environments. If you go to the CISA kev, the non-exploited vulnerabilities catalog and you type in VMware vCenter, there's like a massive list of

old exploitation so we can see what's been happening. Warp Pandas maintain long-term persistent access to networks in one of the intrusions gaining initial access in late 2003. CrowdStrike goes on to say...

Ryan Naraine (37:05.435)
There was a point I wanted to make and I had a specific question. Let me ask Costin first. You got your good IOCs from this one as well?

JAGS (37:08.364)
Yada yada yada.

Costin Raiu (37:13.003)
Yeah, I mean this there's a pretty pretty thorough report with a lot of indicators inside like hashes Also like information about how the malware works about the capabilities of course we're talking here about The brick storm that we discussed before I think we talked about it in the past several times because it's not the first time that brick storm

is in the news, especially with their tool set that allows them to communicate between virtual machines to do exfiltration through the hypervisor by building tunnels between the VM and the

hypervisor. So it's good to have this report. There's Yara rules as well that I haven't been able to fully test to be honest, but they look okay.

I say I mean they have a meta section you know me They have a meta section. They have a last modified they put the date they have hashes in there They have a description and the strings they use seem seem solid but I haven't been able to test them yet because I've been busy more with this other Emergency if you want that was happening in parallel so

Ryan Naraine (38:39.787)
Brickstorm we believe is used by multiple Chinese Nexus threat actors. And I think CrowdStrike is making the point here that Warp Panda, this group that they're tracking here, is the only one that's been observed using Brickstorm. There's another one called Guest Conduit and Junction. So there's like, they're trying to figure out the overlapping use tools and so on. What did we get out of this report, Juanito?

Costin Raiu (38:40.063)
Yeah.

JAGS (39:01.55)
I mean, honestly, I mostly was like sitting around looking at a lot of the VMware stuff and trying to figure out whether, like I was curious, right? We started talking about vCenter sort of being used all over the place. And, you know, there's been a lot of movement and acquisition for VMware in the recent past. I just kept wondering if we were seeing sort of a decay of its maintenance, but it's not being end of life. It's still being supported. It's just kind of.

Ryan Naraine (39:30.229)
Pretty actively patching big things too. mean, the VMware security response team has been pretty active. I see things at least twice a month. Flagging things, flagging exploited things, updating vulnerabilities when things are relevant. We don't get IOCs, you don't get stuff, but at least we know. Anything else to to WarpPander?

JAGS (39:30.336)
you know, good fodder, right? Yeah.

JAGS (39:47.404)
It's just crazy to think of VMware as like so much smaller. Sorry, like I'm just, I'm thinking about what, what VMware was five years ago and now like it's insane. But anyways, sorry. Yeah, this, this is interesting. It's interesting that we keep seeing folks kind of returning to this brick storm thing. It just kind of keeps popping up. And you're getting a lot of disclosures from before it was what like this European agency that came out with a, with a report.

Ryan Naraine (39:51.849)
Yeah, it's crazy.

JAGS (40:15.438)
Obviously our friends at Mandiant and now NSA folks and like it's all really well substantiated in detail. So it's like, makes me wonder what it is about this one that seems to really be getting people kind of aligned and fired up on it.

Ryan Naraine (40:29.258)
You've probably seen Brickstorm in a bunch of like really, really important places because there's an adjoining technical, like really in-depth technical report on the Brickstorm backdoor dated December 4 by CISA, NSA and our friends at the Canadian Center for Cybersecurity. there must be some significant thing happening in North America that they wanted to flag this and get people focused on looking at this.

JAGS (40:48.974)
It's probably credit to Mandiant as well, I'm going to assume. I'm completely assuming. But when you see sort of a high level of like technical acumen across the different publications and stuff, to me, it usually suggests like the original reporter, the person who's actually doing the connective tissue work is leaning into providing that technical.

Acumen in the first place, but that's a total guess, a complete guess.

Ryan Naraine (41:22.09)
From that report, it said, at the victim organization that SISA conducted this incident response, these Chinese actors gained long-term access to the organization internal network in April, 2024 and upload the brick storm to an internal vCenter server. They also gained access to two domain controllers and an active directory federal services, ADFS server, and then successfully compromised that ADFS server and exported cryptographic keys. So there's like a lot of.

nitty-gritty warnings and heads up happening here about what these guys are up to at Brickstorm. Kostin, you were going to make a point.

Costin Raiu (41:54.77)
Yeah, more along the lines that I thought was interesting that CrowdStrike kind of coordinated on this release, but not other companies. So we saw this come out of the CISA, NSA, the Cyber Center and CrowdStrike at the same time. So it failed that CrowdStrike had some kind of heads up, so they knew that this was coming. So they prepared something to...

push their name out there for this, right? Warp Panda. At the same time, I thought it it's weird, so let's kind of nitpick a bit on the report from CSI and the NSA, where they talk a lot about the Brickstorm, but they don't talk, I think, about the previous actor names that have been used a lot. So that would make it, in my opinion,

Ryan Naraine (42:24.276)
their name.

Costin Raiu (42:50.184)
you need to connect it somehow to existing stories otherwise you're just like spinning out new threads uncontrollably so would have been nice if they dropped something like ANC 5221 which is the name that we have seen I don't necessarily know more you were saying that there's probably several actors using this I know what I have seen before so what has been published before especially by our friends from Googlemandy and

Ryan Naraine (43:04.805)
a custom nose more.

Costin Raiu (43:19.843)
about Ankh5221, I think that's the most thorough blogs and the best available information with the RROs, with IOCs, with pretty much everything about BrickStorm. Okay. So I thought it would have been nice to point to that name because that's what, let's say the vast majority of our information out there comes from Google Mandiant. And again, BrickStorm is their name.

This is a name that Google Menden gave to this malware family. So I think it would have been nice to say that, but I don't like how they're trying to avoid using any vendor names for the actor or maybe more along the lines of we don't know which actor it is because we don't have the same visibility. So maybe it is.

Ryan Naraine (43:56.148)
to have heard from my djentu.

Costin Raiu (44:12.359)
We don't know if UNG-5221 is the same as Warp Panda or Silk Typhoon, maybe they just different clusters which overlap. I think would be, I don't know, would put a bit more order into

the chaos if these reports would reference existing research on these topics in a more systematic way.

Ryan Naraine (44:34.812)
It's fascinating to me that all these Chinese threat warnings are landing at a time when the reporting is that there's going to be no more, there's going to be no sanctions over salt typhoon intrusions against the Chinese because of the truce, the truce around tariffs. And it's fascinating to me how tariff negotiations play into these big giant cyber security stories that happening here. The administration also wanting to drop the national security strategy.

Yesterday 33 page document. actually have it printed. got a flight tomorrow. I'll give it a read on the flight tomorrow, but I took a look at it and the word cyber is in there just four times. three times it's just about like thwarting cyber espionage from China and some other places. But there's one point in there where it says, the administration must move to more deregulation to enable private sector companies to assist in cyber cyber operations.

JAGS (45:07.81)
Whoa. Yeah.

Ryan Naraine (45:30.908)
including offensive cyber operations, which comes back to your point from last week that regulation is a dirty word here. We see it actually referenced in the strategy document here. You got a chance to pick at this at all? Any thoughts on where this is?

JAGS (45:43.618)
Yeah. Well, you know, it's not a cyber strategy, right? It's just an, you know, it's a national, it's more a national security strategy. And in that, I'd be really curious to hear from folks who are more knowledgeable about how these things are usually put together and how they get put out. Cause my sense is that this is a

Ryan Naraine (45:47.847)
At all. No.

JAGS (46:09.046)
very, very, very different document than what you would normally expect from the US government. So I think it, you you mentioned, the whole thing, the whole thing is totally different. It's espousing a different worldview. It's like, it's basically a testament to like post Bretton Woods thinking. It's like, you know, everybody do their fair share. We're not going to impose our values on you. People should have the other nation should have the right to like look out for their own values.

Ryan Naraine (46:17.458)
It reads differently, reads kind of.

JAGS (46:39.01)
we will do the same and hopefully we'll find like things in the middle. like, you know, it's just fascinating to read from a US like policy history, whatever perspective, right? Cause it's, again, it's the not so quiet part being not even out loud, but like telegraphed vividly to all other nations. Like this is how we're going to operate. And...

Ryan Naraine (46:50.218)
official government policy.

Ryan Naraine (47:06.314)
There's a big European component in there. think Austin should pay attention to clearly because there's a massive kind of, need to help correct Europe's path.

JAGS (47:09.09)
massive.

JAGS (47:14.594)
Yeah. Well, I think the idea being we need to, it's weird, right? Because the way that it's being phrased is not so much we need to help correct anyone's path as much as we need to correct our path such that everybody else kind of acts in their own, you know, in their own capacity. Look, you're seeing it spelled out.

I've been calling, not, I at no point do I say that I agree or disagree with it. Like I really want to take kind of like an intelligence analysts detachment to these things and just look at sort of what they're trying to do. Cause it's not about, I think falling into the partisan trap and just saying, you know, well, I hate the left or I hate the right. It just puts everything into such a narrow focus that we can't.

We don't actually evaluate whether things are having good outcomes or not. We're obviously not in a place to be able to say what parts of what is changing, what the effects of this are, and if they're going to be positive or negative. But what we like the one thing I will say unabashedly, because we were saying it a year ago and two years ago is, well, the shit from before was not working.

on in cyber, in internet, in tech, it just wasn't working. So I didn't have as much of a vested interest in, well, we need to keep this system functioning. At the same time.

Ryan Naraine (48:47.347)
Yeah, you've been, I've been accusing you of being a free for all kind of...

JAGS (48:51.53)
Yeah, because I was just saying that this shit doesn't work, right? you know, so I'm not going to complain about somebody tearing, like deciding to kind of shake up the thing that was there that wasn't really working. At the same time, I know better than to just be a, you know, idealistic

revolutionary, thinking that, well, the other shit doesn't work. So tear it down. And surely what comes is better. Right.

That's how that's what you get.

Ryan Naraine (49:22.185)
But some sort of pivoting was necessary in your opinion.

JAGS (49:25.012)
Well, think that, so what I saw, what I got to see in the US government and in trying to support some of these things in whatever small capacity was a system that knew it was broken or it was not fit for purpose in cyber and tech, but also knew that it could not change in any way whatsoever. Right? So like

The minute the conversation goes into like, but that's classification, you're like, this is over. Like this whole thing is over because we will never, ever, ever fix the classification system, period. And that kind of intransigence, like when everybody's sitting in a room going, this doesn't work and it can never change, let's find ways to sort of squirrel our way around to trying to do the mission, then.

I don't think that that's necessarily a organizational mechanism that we should enthusiastically defend now. Does that mean that what we're going to do now is better? I'm not going that far, right? I'm just saying, if, let's put it this way, right? Let's assume that this Trump administration is just a four year thing, which

I have no reason to believe that it is or that it isn't. I have no fucking clue. I'm not saying that it should or it shouldn't be. I'm just saying. Let's assume there's this term, that we still have term limits and we're, you know, we're going to stick to this four years, right?

If all we got in cyber was like no progress, no big changes, but they kind of throw out the whole US classification system and start and give people an opportunity to start over in a more reasonable capacity. I would take that as a win. Obviously that's not, that's not what seems to be on the table, but

Ryan Naraine (51:21.235)
You'll take that as a win.

JAGS (51:31.712)
It would be a change that it would be like nuking something from orbit and at least letting people like rebuild. It will still look like a fucking fallout for you. Like, you know, attempted dystopia, but it isn't sort of the thing that's been stuck and it's going to be stuck and it makes no sense to anybody. And it's it's a system that's stronger than all of us, even as it sort of chokes us all to death. I don't know, man, like.

I'm not, look, look at the kind of pieces that we're getting from like, no, no, no, I.

Ryan Naraine (52:01.981)
Mr. America is starting to hedge a little bit, Costin.

Costin Raiu (52:02.179)
No, on the contrary. No, no, I was looking through the policy and I thought it was fascinating. I think it's very well written and it says the kind of things that people expect these to have. So even if you look where they talk about like, what do we want? And

JAGS (52:08.334)
Go ahead, Kostasar.

Costin Raiu (52:27.723)
I can't but just notice that it says we want the world's most advanced, most innovative, most profitable technology sector, which undergirds our economy, provides a quality of action, our military strengthens our global influence, and that comes ahead of having the world's most powerful and capable military. So the fact that technology is a

essentially number 4 here. Political system, innovative economy, leading financial system, most advanced innovative profitable technology sector. They get it. mean the US gets it. is the most important thing here. Technology is more important than many many other things and even in Romania I saw a bunch of numbers today where they were talking about the fact that economy slows down.

and the contribution to the country's GDP from different sectors like tourism, very small growth, agriculture, very small growth, but technology, the growth in technology was insane, like 15 % growth year over year. And I was thinking this is where you need to focus, like if they understand how the world moves nowadays, this is...

This is where you need to focus. You need to focus on technology. You need to understand technology. need to understand that, you know, things like AI, biotech, quantum, exactly what they say here. We want to ensure that the US technology and the US standards, particularly in AI, biotech and quantum computing, drive the world forward. So, yeah, it's fascinating to read this, especially where they poke

when they poke Europe a bit about going into the wrong direction, like restoring Europe's civilizational self-confidence and Western identity. Which is not bad, I mean, look, we need our Western identity back, like we need to get rid of this shit. We need our Western identity back, please.

Ryan Naraine (54:28.945)
Yeah.

JAGS (54:29.912)
That part, I'm like, no, but dude, that's a dog whistle.

Ryan Naraine (54:31.772)
That's a little dark.

JAGS (54:39.758)
the bottle cap. So to me, those are little dog whistles that I'm not thrilled about because to me those feel like signals to the more like authoritarian turned European countries where I'm like, like this is, you know, in a lot of those countries in Europe, the kind that are using this sort of language about sovereignty and whatnot, it

A lot of it is coming with the kind of populist uprisings that historically in Europe are not necessarily like the most, you know, savory.

Ryan Naraine (55:14.928)
what Costin is telling you. And what is very clear from my conversations with Costin is that it's resonating with Europeans. It's resonating with especially younger people, right, Costin? Like this kind of nationalistic, know, save our civilization.

JAGS (55:21.484)
Yeah, yeah,

JAGS (55:30.04)
Chen Xi's a bunch of little fascists is what it is.

Ryan Naraine (55:32.084)
Hehehe

Costin Raiu (55:33.8)
I think the best example is this, most recent happening of all is that the European Commission has fined Axe, Twitter Axe, like 140 million euros for some reason, let's say, because they don't like Elon Musk or because they don't like Axe or because they don't have control over it and they want to have more control without diving into the reasons for that. So obviously that created like a lot of tensions and

Costin Raiu (56:09.725)
I think even JD Vance wrote on X before this fine happened saying that I hear some rumors that the Europeans want to impose which in my opinion is a huge fine, $140 million because of blue checkmark is now deceiving or

disciple or whatever. It's absurd, like it's stupid. just, yeah, it's wrong. And I was thinking that there's a lot of confusion regarding what the European Union is and what are the values of the European Union. Then there's like all these different organizations or bodies. And I'll give you an

example. There's the European Commission. Then there's the European Council. And then there's the Council of Europe.

And all these three, there are like three different things with three different... And then there's the European Parliament as well. And like each one...

JAGS (57:04.738)
What the fuck is this?

Ryan Naraine (57:11.496)
But they all form part of the European Union. The Union has all of these kinds of bureaucratic units that does different things. You're making this sound like it's some crazy pants.

Costin Raiu (57:17.62)
Now here's the issue. Here's the issue. Like if, yeah, I mean, in theory, what people complain about is that we elect some people who in turn they choose other people to run all these commissions and committees and councils and whatever. And then they just go ahead. They go ahead and then they start doing things that we don't want in the first place. Like.

JAGS (57:19.35)
Europeans love bureaucracy, come on.

JAGS (57:34.082)
Did you read the bullshit jobs book we were we were

Ryan Naraine (57:34.568)
This was part of the Brexit justification,

Costin Raiu (57:44.702)
Nobody wants for instance chat control but they are pushing like crazy for this chat control thingy which started under the previous commissioners mandate.

Ryan Naraine (57:53.618)
Well, you can't say nobody wants it when they're pushing for it. Those are conflicting things.

Costin Raiu (57:56.905)
Like there's a huge amount of people in the European Union. I think that the vast majority of people who know what they're talking about, they don't want this. Obviously, there are some reasons why they're pushing it. Doesn't necessarily mean that we want it like we as Europe or there's a European Union. Obviously, we don't want, I mean, people like me who survived through the communism.

JAGS (57:57.527)
Well

Costin Raiu (58:23.86)
where Securitate was opening all the letters coming in and out to check them for subversive materials. you're going back to this shit again. This is equivalent. You're going to check all the messages for subversive materials or like some sorts of materials just like the Securitate was doing back in Ceausescu's communist times. And the people who are pushing for this, they don't have good explanations. They're all trying to give stupid explanations that people should just accept. Like

Ryan Naraine (58:31.218)
That's the equivalent of it. You feel the same.

Costin Raiu (58:53.584)
we're doing that to protect the kids. it's because criminals are using it. So we need to backdoor it. And because like law abiding citizens don't use encryption, only criminals use encryption and know, bullshit like this, which again, it comes from all these different organizations, which don't necessarily come from people that you or I voted for in the first place. So yeah.

Ryan Naraine (59:19.709)
This is the justification for Brexit. are we, why are a bunch of bureaucrats in Brussels making decisions for me in Wales? Like I don't know who these people are, making these weird decisions leaving bottle caps on.

JAGS (59:27.438)
you

JAGS (59:31.96)
Well, I understand that and I agree with that, but I don't know that there was anything about Brexit that was genuinely in the interest of the UK. Going to the UK post-Brexit is a sobering and sad example of how much a population is willing to shoot themselves in the foot.

London was like the de facto quality, the actual capital of Europe, whatever people said. You can say whatever you want about Berlin and like Germany having the money and whatever you want. But like the banks were all in London. The, you know, the people, if you were going to meet people, you were meeting them in London and it was this amazing, vibrant place. And you go now and it is not that. Dude, I was walking down Bond Street and like somebody from the Burberry shop pulled me aside and was like, hey, you really should cover.

Ryan Naraine (01:00:09.925)
It was still London, right?

Ryan Naraine (01:00:20.22)
Really?

JAGS (01:00:28.512)
your watch because I was walking around with my jacket rolled up and I'm like in Bond Street in old fucking Bond Street like Savile Row down the street. I can't like are you fucking kidding me? But but he was saying it because somebody had already snatched the watch earlier that day. So you go it's just what the fuck happened right like to.

Ryan Naraine (01:00:50.119)
Yeah, but that's not that. You think that's Brexit related or that's just crime and economy?

JAGS (01:00:53.044)
I think it, but that's my point. Crime in the economy, very Brexit related. You let that economic vibrancy leave. A lot of the people, a lot of companies moved out of there. The banks stopped working out of London and you just don't have the same amount of money flowing. You're not part of a larger economic block like the UK kind bought itself an irrelevance that you don't easily compensate for.

So I'm not saying it's all Brexit, there's no way that like there is no version of the universe where we say that Brexit helped the economy or helped the position of the UK. So.

Ryan Naraine (01:01:34.888)
Yeah, it's not. This surveillance thing is not limited to Europe or thing. I mean, I saw there was a reporting this week on India having an order requiring smartphone companies to pre-install a government cybersecurity app. If they subsequently walk back the order and it can be removed and there's some things there. So we know governments all over the world wants to do this. I'll mention also that half of the US now requires users to upload an ID.

Costin Raiu (01:01:48.389)
Mm-hmm.

Ryan Naraine (01:01:59.078)
validate age before accessing porn sites, sexually explicit websites, 25 states, it's now this age verification law is in place. And there's a feeling that if VPNs are the circumvention tool, they're gonna come for VPNs too, and at some point we'll have a flavor of chat control here that requires this. I mean, it just feels like we're heading in that direction, am I wrong?

JAGS (01:02:23.758)
How?

Costin Raiu (01:02:24.316)
question is, how serious of a problem that is? Is it for real such a huge problem that minors are accessing porn sites? Is that the issue? Or is the issue deeper? Is issue about control? Is it about creating an obedient society? About implementing mechanisms and levers that allow them to

spy on people and suppress dissent and things like that. So that is the question I guess. Which one is it?

JAGS (01:03:04.033)
This is our Joe Rogan-iest episode ever. It feels very, like I feel like we went, we're in it for our right-wing friends today.

Ryan Naraine (01:03:04.359)
What's the latest on chat control? It feels alright.

Costin Raiu (01:03:07.431)
Hahaha!

Costin Raiu (01:03:14.427)
No, I mean in Europe, I tell you one more thing, which is that it feels that whoever is running within the councils and the commissions and the parliaments and the groups and I don't know, whatever, they just like stretching themselves thin into all sorts of different directions. As like a bunch of people, we need to help Ukraine, Russia is the big problem. Then there's another group.

Ryan Naraine (01:03:25.265)
missions.

Costin Raiu (01:03:43.089)
We need to get rid of cars that use fuel. We need to replace everything with electric cars. And there's actually a target to stop selling anything that is not electric cars by 2036, if I'm not mistaken. And even like recently, Germany was like, whoa, whoa, whoa, guys, we need we need some kind of an exception. We can't do that. Like we're going to destroy our economy. We're going to crash.

And I feel them, mean, yeah, there's like pushes in all sorts of directions like chat control and instead of let's say focusing on one thing that really matters, there's just like pushing in all sorts of different directions which create a feeling of chaos and people are just like not united. I think that is the issue. They're not united by a common goal and instead they're like fighting towards different concepts, different directions.

against imaginary adversaries like don't know, chat control. Chat control? No, I said chat control. I didn't say the war.

Ryan Naraine (01:04:45.415)
Well is it really imaginary? Is it really imaginary when you're at war?

No, no, no, I'm talking about the ability to surveil and look for its wartime. I'm playing devil's advocate.

Costin Raiu (01:04:57.307)
I'm all about focusing on war if that is the issue, but then forget the electric cars. Yeah.

JAGS (01:04:57.454)
They're not even pretending it's for war. They're not even pretending it's for war. That's the thing though, Ryan. If they were even half as competent as the people we were dealing with back in the Bush era, and we were talking about Patriot Act adjacent things, then you at least would make an argument tied to the things that are happening in front of you. But look at the question you just asked.

Well, it wouldn't be good for like wartime like well, but that's not what they're talking about. They're talking about children and a bunch of bullshit issues around like sort of decency and it. Yeah, and you're like, OK, sure, but that like this seems like overkill for that same as in like in the US, like having a moral panic about pornography is like just old school shit, right? Like it's that moral panics are.

Ryan Naraine (01:05:38.759)
This is a material kind thing as well.

JAGS (01:05:56.418)
the pornography of conservative religious people. That's all it is. It's all it's always been. That's their favorite conspiracy is sort of that kind of, well, the Satanists are coming for you on Signal. So yeah, it's a bunch of fucking, we know it's all bullshit. What I'm interested in is, okay, we're in this anti-regulatory heaven for corporations right now.

Ryan Naraine (01:06:11.843)
for your kids.

JAGS (01:06:24.918)
You know how much money is in pornography? Like where the fuck are the lobbyists for the porn industry there if anyone's gonna save us? Actually, like the more I think about this, if anybody's gonna fucking save us, dude, yeah, where's if Pornhub? Exactly, dude, if Pornhub like this is this is your time to shine as like the defenders of like internet free speech, essentially.

Ryan Naraine (01:06:36.023)
VPN industry is filling that slot.

Ryan Naraine (01:06:51.087)
If they don't spy on you through legal means, they'll eventually spy on you. We have a coordinated release of a bunch of reports around Intellexa and Intellectuals corporate web. Shout out to Julian from Recorded Future, Google Cloud. Google also had a report out and then there's some reporting about this Intellexa form that's owned by an ex Intel officer in Israeli. Still active amid US sanctions and the Recorded Future actually

documents this global corporate web of, know, even within the sanctions, they're still aware. On tandem with that, Apple sending a fresh batch of spyware notifications to about users in 84 countries. So we know that Apple has got another batch going out. There's more reporting on French NGO, Reporters Without Borders targeted by Callisto in a recent campaign.

There's just a lot of new reports and activity around commercial spyware. The Intellectual Report stood out to me, Kostin, because it really goes out and documents this web of corporate thing and kind of the kind of reporting we are hoping to see. Did we learn anything new at all from this?

Costin Raiu (01:08:01.98)
Well, there's a bunch of new IOCs in there. If you ask me, the Recorded Future report that Julian wrote is the most thorough of all. It has like the most IOCs, it has like the most interesting information in there. To me, at least, it was definitely the best. It was also the first that I read. And in addition to this, like you were saying, there's one from Google and there's one from Amnesty.

Ryan Naraine (01:08:31.417)
I'm nasty as well,

Costin Raiu (01:08:31.515)
I think it was kind of weird, maybe I misread or maybe the story changed since I read it but it was kind of strange in the sense that one of the reports said that they're thanking Google and Amnesty and then in the Google report they were saying we thank Amnesty but not the other guys.

Ryan Naraine (01:08:52.41)
They don't tank anyone. Recorded future.

Costin Raiu (01:08:57.429)
I thought that was like strange and now I see that the thanks to Google has disappeared from that report so I don't know what happened.

Ryan Naraine (01:09:03.514)
from the recorded future one, it's just pointing only to Amnesty now. So we know that there's some beef there, or some hiccup there,

JAGS (01:09:05.902)
Wow.

Costin Raiu (01:09:06.171)
I find it anymore.

don't know what happened there. Something may have happened. like if you ask me of all the reports, the recorded future one is the most interesting because it has the most comprehensive IOCs and description of everything. The amnesty one has like, they're like dropping, I think, two IOCs to domains throughout the report. And I kind of hate it that they don't have it like at the end in a pretty standard...

industry technique, I don't know, like everybody does it to just have an IOC section at the end. Yeah, I don't know.

JAGS (01:09:47.15)
Amnesty doesn't give a shit about sharing stuff. Like at this point, both Amnesty and Citizen Lab, like they have no interest whatsoever in sharing shit with anybody. Like they, I'm glad they do the work they do and they do cool stuff and then, you know, they're, they're the ones that the coal face with the activists, but it also is starting to feel like they're almost

trying to elbow anybody else away from helping activists. They're like, this is our fucking lane. You're like, all right, you guys need to calm down. You need to remember that this is supposed to be about protecting people that are being targeted and not about marking your territory and peeing all over like the, oh, this part of the mobile implant business is ours kid. Like what the fuck is going on?

Ryan Naraine (01:10:33.51)
Shout out to Julian Ferdinand, we had him at LABS con Juanito, you remember?

JAGS (01:10:35.992)
Dude, I love Julian and this fucking kills me because you know, I really don't like recorded future like personally as a company, like I have some mild history with it. I just don't. never liked the way they operated back in the day. That's like a, whatever. But but Julian does great work. And like I have to, you know, have to give him credit and, you know, did a great talk. He's done. We've done collabs.

Ryan Naraine (01:10:57.83)
Shout out to Julian,

JAGS (01:11:03.59)
with Sentinel Labs, Alex Malinkowski and Julian have done great work together. dude, I need to be a bigger person. honestly, the quality of the research is big enough where they're giving Julian a platform. I got to put my feelings aside and, you know.

Ryan Naraine (01:11:06.596)
He was a speaker at the last lab scan. did this camofay thing, really, really interesting talk.

Ryan Naraine (01:11:25.316)

In addition to this big intellect exposure, we also saw revelations on a group called group 78, a secret U S task force that fights cyber criminals. And this was related to, this was, Lamond French newspaper, pretty detailed documentation of this kind of outing of this black buster ransomware group. How is this any different from, the, the, the leaking of,

Dook lab dook fegin. Costin is this, you know what I'm saying? Is this any different?

Costin Raiu (01:11:56.825)
Mmm.

are you asking me specifically if it's the same people behind LabDuctagon or like if the idea is the same more or less? Right.

Ryan Naraine (01:12:04.728)
No, no, no, that's not what I'm asking you. This is being held up. This is being held up. This, the story I read in Lamont, it's being held up as the U S has a secret offensive team looking to out some ransomware actors. Things we've been asking for. Like these ransomware assholes have been doing their own thing and we've been on this podcast for the last year saying, why aren't we doing more? Why aren't we being more aggressive? What should it look like?

Costin Raiu (01:12:23.737)
Hmm.

Costin Raiu (01:12:29.625)
Mm.

Ryan Naraine (01:12:29.668)
This is actually what it looks like. Is this kind of exposing them, leaking stuff to select journalists, dropping details and doxxing these ransomware assholes. It's affecting some European investigations apparently, and there's like some friction around how the US is approaching it and the existence of this group 78, quote unquote, group 78 as this secret US task force. I'm asking the question, is this just not one of those leak and expose operation? Why is it any different?

Costin Raiu (01:12:57.889)
I don't think it's necessarily any different and I don't think that the focus

Ryan Naraine (01:13:01.572)
And why did you think I was asking if they were the same thing?

Costin Raiu (01:13:04.856)
because we know there's a lot of kind of fake leak operations going on. There's a lot of these so titled and titled hacktivists leaking information, which in reality they're not truly hacktivists, but they are like other, I don't know, group 79, group 80, group 81, and so on and so on. What is interesting here, I think with this story is that

Ryan Naraine (01:13:23.462)
strategic.

Costin Raiu (01:13:31.532)
Probably they didn't want this story to come out. I don't think that they are probably very happy that this story came out in particular when they talk about that the American guerrilla style things were kind of creating a deep rift between the European and the US investigators. And to quote multiple sources said European officials were stunned. I mean,

I don't know, like to me, sure, go for it. If this is what they need to do in order to draw these people out of Russia and to arrest them, please do it. I mean, yeah, they're going to put pressure on them to make them like to annoy, to make their life difficult. And then they say like, you know, I'm done with this shit. Let's just go to Thailand for a vacation. They go to Thailand for vacation. And what do you know who is waiting for them in Thailand?

Ryan Naraine (01:14:06.992)
More of this.

Costin Raiu (01:14:28.344)
is group 78 member of FBI and if this is like I'm okay this is okay in my book absolutely

Ryan Naraine (01:14:38.544)
The legal system in Europe is worried about interference of investigations going on, tainting of evidence, legal, blah, blah. Juanito, you're rolling your eyes. Why?

JAGS (01:14:51.854)
I don't know how to talk about this story, like at all. I don't know how to talk about any of it. None of it sits well with me. None of it, all of it sounds weird to me. First of all, like, what the fuck are we talking about? Like, what the fuck? Yes.

Costin Raiu (01:15:08.791)
Can I quote something? I have never seen anything like this, said a veteran Europol cyber officer. Committing crimes to damage an ecosystem is extremely unusual, even for the FBI.

Ryan Naraine (01:15:27.75)
You

JAGS (01:15:27.79)
What the fuck? Like everyone is displaying their worst qualities right now.

Costin Raiu (01:15:29.719)
What is going

Ryan Naraine (01:15:38.128)
The other shit here is someone comes in and privately shares an operation that's happening around a hack and leak operation and then they drop it into a Lamond private report. It's like... I don't know.

JAGS (01:15:51.232)
I look, okay, okay, let's engage just a little bit, right? So I don't know what the fuck is going on. This isn't how the FBI normally.

Operates in anything but also like if this is really what's happening Why would they say it like that? And then if they do have this privileged data like clearly it wasn't data sourced by the FBI Because if they had been sourced by them You wouldn't get some cutout that's giving it to journalists like you you know Ryan like I my thinking did not go to lab do to gun or anything like that because you know

That's just you don't usually have someone in a meeting somewhere saying we're gonna we're gonna play these tricks with the whatever and then somebody else goes and talks to a journalist like this is It's totally ass backwards. It's just not how you would do it But most importantly if that data has to make it to people on the outside It cannot have been sourced from the inside like it cannot have come If it's if it's been handed

to some FBI whatever or like it's part of the IC's collection mechanisms. It's exactly what we were talking about 20 minutes ago, right? Like you'll never in the history of men, like the age of the universe will decay before you declassify that shit. So nothing about this sounds, I don't even know what the right term is. It all sounds very fucking weird. And I'm not, I don't think that it's being made up.

I don't think that the Europeans are making up that something was said, but this sounds like a game of really unreliable telephone and somebody getting excited and saying some shit they shouldn't have and then somebody flying off the handle and doing some stuff they weren't supposed to do and everyone's confused and everybody's kind of weirded out. And the European reaction makes me roll my eyes because this is the kind of shit that like, if you were doing them a favor, if you are helping them in whatever.

JAGS (01:18:00.782)
They'll take it happily if you do it quietly. The minute you say something publicly, they all have a conscience. And oh my God, the privacy of it all is like, oh God, okay, we fucking get it. that reaction alone doesn't do anything to me or for me, but the discussion of what this group 78 thing is supposedly doing makes no fucking sense, right?

If this is how you're gonna do it, if this is how you are trying to do it, that's not how you do this. Like that's not how you're successful at this. If anything, you...

Ryan Naraine (01:18:38.991)

This is normal though, this kind of hack and leak disruption extra legal kind of this has become a normal part. I mean, we're starting to see it with the kitten busters leaked. I'm just talking to generally the.

JAGS (01:18:48.152)
But not in the... But dude, you're talking about a US law enforcement officer walking into a government, a multilateral forum and saying that. There's nothing normal about that at all. Like what? Like that's that maybe...

Ryan Naraine (01:19:03.279)
the FBI goes to conferences and privately TLP Black says that we've been doing this thing in the back. Come on, this happened.

JAGS (01:19:08.258)
No,

JAGS (01:19:11.96)
They, you are equating things that kinda kinda look the same, but that things that aren't the same, right? Like when a law enforcement officer in a multilateral forum says some shit, it's, you know, there is a certain amount of like vetting and whatever. It's one thing if you tell me that some FBI officer went on a private stage in a private threat intel conference and said, here's a few things we found that you things might, you guys might wanna work on. You're like, okay, cool.

This is actionable and you're trying your best to make it work. That's not what this is. Somebody walked into a multilateral meeting and said, we're doing some like badass cowboy shit. And everybody went, what the fuck are you talking about? You are the cops. You are the fucking law enforcement officers. You can't be like, yo, fuck the law, right? Like it doesn't come off right. But then again, there's the

There's just so many, this sounds like there's just a web of fucking telephone happening and probably a lot of bluster and a lot of, you know, making things seem a thousand feet tall when they're in, you know, probably in a molehill.

Ryan Naraine (01:20:25.816)
Group 78, keep that in mind. Keep that in your notebooks. Kostin, you remember when Dave Vitell was on the show, you asked him if Aardvark was capable of doing smart contract auditing, security auditing and so on. was fascinated, questions stayed in my head. Anthropic drops a report that says, hey, we're doing this. On contracts exploited after the latest knowledge cut off March 2025, Cloud, Opus 4.5, Sonnet 4.5, and GT5.

Costin Raiu (01:20:35.12)
Right.

Ryan Naraine (01:20:53.369)
collectively worth $4.6 million, establishing a concrete lower bound for the economic harm world. So they're saying they're tinkering here and playing with this and there's some big value in what did you make of this report as your AI magic money correspondent?

JAGS (01:21:09.58)
I did. Kostin Kostin. Come on, Lay it on us.

Ryan Naraine (01:21:12.013)
What are they saying?

Costin Raiu (01:21:15.807)
making like a drama pause. I mean, you guys were asking like a lot of theoretical questions and I was like more on the practical side with Dave. I mean, how do you use this thing in practice? Like, I'm interested about the practical use of AI about the practical use of models that can actually make your code safer in the end, like making

Ryan Naraine (01:21:18.479)
Ta-da!

Costin Raiu (01:21:42.42)
We already know that AI is making your code unsafe. this is like, you know, it's a given thing that AI will introduce bugs in your code. It will make it from some points of view safer, but at the same time introducing unexpected pathways, things that will happen and eventually, you know, will turn into discovered vulnerabilities. So.

From the point of view of finding bugs, was thinking that these tools like Artvark, like this system should be able to catch vulnerabilities in smart contracts pretty easily. They should be very good at this. And why? Because this is a pretty big market. There's a lot of companies out there. I think we were talking about Trail of Bits, right? In the past that is doing smart contracts, auditing, like pen testing, if you want in this sphere.

finding bugs before you know the North Koreans come and with their collective minds they hack the shit out of it and then they sell hundreds of millions of your money or other people's money who trusted those smart contracts in the first place. So it's good to see that actually it works. It's good to see that people put it to good work. yeah, we just saw the

deployment of a new version on the Ethereum ecosystem just a few days ago and it's good that nothing wrong happened, nothing bad happened. I think it's important that if you care about cybersecurity in the blockchain sphere, it's important that you do auditing of smart contracts and having the right tools, you know, it

it helps and makes the difference between getting owned and not getting owned.

Ryan Naraine (01:23:37.273)
And the research paper from Antropic Fellows Program is that in a nutshell, they were able to prove that the AI agents find about 4.6 million in blockchain smart contract exploits. This is the kind of like no-brainer places you should be pushing this AI research one.

JAGS (01:23:55.016)
I mean, absolutely. Absolutely. Because the AI smart, the smart contract side of the house, like the fact that people are willing to trust this stuff with money, like real money of some sort is insane to me. But what I'm curious about is like, is this just like a scoped project that they put some energy into?

because obviously there's money, it's flashy, you can basically use it as a good proof of the value of what you're supposedly doing. Or are smart contracts particularly exploitable? Because like, why is that the thing that these things are excelling at creating, like popping out O days for and not like, not as much these other, I mean, look, big sleep is coming out, like there was like some iOS.

stuff reported by Big Sleep recently. Obviously, Aardvark's finding stuff. Like, you have people that are finding bugs, but this is...

The sense I'm getting is much more talk of like a proper exploit sort of being popped out of these. Kosen is that right? Like I went through the report, but are we this isn't like, we found like a double free, right? Like you left a little bug in there, bro. You should go fix it. Like it sounds like it's like the thing is borked, right?

Costin Raiu (01:25:17.682)
Mm-hmm.

Costin Raiu (01:25:26.524)
Yeah, I guess it's more in the sense that, yeah, here's a confirmation that AI is getting better at everything and in particular, if you know how to prompt it, it's definitely getting better at finding bugs in smart contracts. And I think, of course, the other side of the coin here would be to understand how much the North Korean Lazarus Blue Norov guys are using AI to

to find bugs and exploit smart contracts? How much of that they are doing at the moment? mean like right now? Probe? I think yeah, for sure. If according to entropy the Chinese are using AI to automate their intrusions, I would say that it's highly unlikely that the North Koreans are not using AI to try to exploit smart contracts.

Ryan Naraine (01:26:01.662)
No, but they have to be doing that, right? mean, this is their wheelhouse.

Costin Raiu (01:26:24.477)

And I mean, yeah, there's news of smart contracts being exploited all the time. At some point, you don't even know exactly how it was done, how the bug was found. But like the amount of news in that field is typically pretty significant.

Ryan Naraine (01:26:29.348)
Yeah, it's...

Ryan Naraine (01:26:41.506)
Yeah, in tandem with news that Lazarus North Korea did a $30 million theft from South Korea's largest crypto exchanges. Upbit, had our buddy Song Soo tweeting about Upbit conforming a major security breach. $39 million in Solana based assets. These things are so dime a dozen these days that it barely registers as a blip, right? Question for you though, right? When you talk about AI doing smart contract auditing, are you looking to the AI to think

Costin Raiu (01:27:01.371)
small pocket money.

Ryan Naraine (01:27:11.31)
differently and approach it completely in a new way that humans aren't capable of thinking of? is that the ability to scale and do things faster and do things more? Help me understand what you're hoping that the AI brings to the table.

Costin Raiu (01:27:25.061)
I think you just, well, assuming that the bad guys are using AI already to find bugs in smart contracts, it makes sense to first use AI on your side to find all the bugs, at least to fix and patch all the bugs that the AI can find. the, you know, the low hanging fruit is suddenly no longer available to the bad guys. So that's

kind of establishing if you want establishing a baseline beyond the baseline considering that as I say you put a lot of time resources tokens whatever analyzing smart contracts you even I think would be nice to have some kind of a certification mechanism like I don't know we we use this model and spend this many tokens to try to

ensure that it operates as expected and there are no hidden pathways, that alone by itself probably would help raise confidence in this technology, which to me is important. So the expectations from my side would be more in the line of raising the baseline, making smart contracts safer by default, and potentially creating some kind of

seals or certifications or things that people can uh you know for transparency reasons and reports they can show on their websites whatever and that they i want the badge i want the pledge and the badge uh but not like this fake one where like the seesaw cuts the queue and gets in front for a photo

Ryan Naraine (01:28:57.325)

You want a badge? You want a pledge and a badge?

Costin Raiu (01:29:11.365)
but I want the one that is driven by AI and it's got like the signature from the AI whatever that yeah, they spent 5 million tokens and everything that was found was patched and this is what they found.

Ryan Naraine (01:29:25.816)
Hey, there's some folks planting a flag in the ground. The folks at Expo, is a hotshot AI security company that has Nico Weissman as their CISO. Just this week saying, listen, we're willing to put a plant or flag in the ground and say, use our product. If we don't find something, you don't pay anything. I feel there's like, there might be some fine print there. There might be some fine print there, but those guys have nailed the marketing. They nailed the marketing and getting on the HAKA 1 leaderboard. again, this is kind of like.

Costin Raiu (01:29:31.953)
Mm.

JAGS (01:29:42.156)
genius genius shit genius shit

Ryan Naraine (01:29:52.802)
Here's a, here's a use it for free. And I guarantee you that our AI is going to find some Dave. They're they're dabbling in the web app space. Why do you think it's genius?

JAGS (01:30:02.046)
I it's fucking brilliant, man. you're, you have to, so, okay. From the perspective of a consumer, there's no reason that you really would decide to go for a newfangled AI pen testing company as opposed to a well-known existing red teaming shop, right? Like, okay, you're doing it with the AI. It just sounds like it's cheaper for you and experimental.

Why, you know, cutting edge isn't necessarily the most desirable thing in that like checkbox ticking exercise. But when somebody gives you a financial incentive to try, like they took all the risk out of the fucking equation. Just, you know, give us a try. like, it's the same thing as like when Halvar and Sean Heelan had optimized. And my understanding of this, just...

Ryan Naraine (01:30:59.329)
Yeah, I love that business model.

JAGS (01:31:01.238)
Yeah, I just heard it through the grapevine. was like, we'll take a portion of like the money we save you. Fucking genius. Genius.

Ryan Naraine (01:31:05.347)

whatever we save for you. Yeah, that was the original pitch that I really loved. I mean, they had to move away from it because it was difficult, but the idea was use our product. I guarantee you we'll save you a million dollars. Give us half of that. So you take, you even take, you take 500,000, give me the other 500,000. I guarantee you I'll save you a million dollars, which was fascinating to me. I, I.

Costin Raiu (01:31:17.295)
Thank

JAGS (01:31:26.412)
Yeah, so I love seeing it because this is the kind of stuff that people are missing in order to make shit impactful. Like the traditionalist mindset around products is not vibing well with AI as a powerful force undergirding the system. Because if what you're telling people is this makes things cheaper, but you don't translate that into the business model, then why do people

buy your version as opposed to buying the tried and true one that they are already comfortable with. But if you tell me that it's cheaper for you, which means that you make it not just cheaper for me, but that you radically shift the quality or the output that I'm getting, or you use the money that it's saving you or the automation that you've built to then translate that into a different kind of transaction altogether.

then you have a motivation to actually pick this up. So I think this shit is genius. I wish Nico all the best with this and look, we'll see, right? This is putting your money where your mouth is.

Ryan Naraine (01:32:37.251)
They're in the VC cauldron so best of luck to those guys. Let's close the show quickly with some shout out to our hour a half Mark, Costin has to get out of here. Costin you wanna go first?

Costin Raiu (01:32:48.395)
I mean sure, I think this week we found out that a good friend of mine, Vasily Ivanov, out of Bulgaria, is going through a tough period of his life, he's been diagnosed with cancer, so sending all the possible good vibes to Vas, I'm still positive about this because my father-in-law

Ryan Naraine (01:33:02.147)
aggressive prostate cancer, right?

Costin Raiu (01:33:16.078)
has been going through something similar and with the right treatment his cancers got much better and a doctor actually said that you know he will he'll pass away eventually but not because of the cancer itself so for Vess I just want to send like some strong strong thoughts of support some good vibes and

Ryan Naraine (01:33:38.209)

For members of the audience that don't know who Vess is, it's an old school antivirus guy. I I met him at virus bulletin conferences many, years ago. He's a little bit of a curmudgeon, but a deep roots in our AV industry from the old days, right, Costin?

JAGS (01:33:49.034)
Little bit.

Costin Raiu (01:33:56.576)
Yeah, I mean, he's been around since the beginning, very beginning and the guy has always been very tough on mistakes. One thing he couldn't tolerate, couldn't tolerate idiots and morons. He had like a very low tolerance for that, very low tolerance for bureaucracy.

Ryan Naraine (01:34:17.197)
well, that's what I was going to mention. A good point you made here because he wrote a big long essay about his current circumstances and it describes months and months of like misdiagnosis, bureaucratic days, conflicting medical advice, some therapy that may not work. And he wrote it in a very, it wasn't dark. It wasn't too dark. was, it was tough to read. Obviously it was tough to read.

Costin Raiu (01:34:34.772)
Easy way, Mm-hmm.

JAGS (01:34:39.16)
It's tough to read. I wouldn't, you know.

Ryan Naraine (01:34:41.601)
It was kind of heartbreaking and he keeps caring for his real mother and there's not many people in his life and so on and navigating this system. But it comes across as a very, very human document to leave behind. I don't know. just, it, it, I never got to know him personally. I know about him and I know I've read all his work and kind of followed him over the years. So I mean, I double what Costin is saying. Best of luck and you know, the best of vibes.

JAGS (01:35:06.67)
I never met Vest, but to me, when I kicked off in the industry, he was one of those guys on Twitter that you just like, if he like so much as like smiled your way, you're like, my God, I fucking made it in my career because if you fucked up, if you fucked up even by like a fucking inch, like Vest was gonna just come in and like, yeah, he was right. It's fine. Like it was like this kind of forcing function of that old school.

Ryan Naraine (01:35:15.07)
Hehehehe

Ryan Naraine (01:35:22.829)
He was tough. Yeah.

JAGS (01:35:36.13)
So, yeah, I don't know, man. I think we've all had family members who've dealt with prostate cancer. Cancer itself is kind of this terrifying, awful thing, but prostate cancer is pretty manageable. A lot of people, like my grandfather included, you can take care of it and hopefully continue to enjoy life and stay here with us. So all the best to our... Well, I wanted to say our friend. I've never met the man, but I have a lot of respect for him.

Ryan Naraine (01:36:06.114)
Shout out to Vess. And the other thing I noticed this week is Halvar. You mentioned Halvar. Halvar and a bunch of old school hackers wrote an old beta eulogy to an old school hacker and Frac staff member, Sebastian. Hacker Handel Stealth that passed away, apparently passed away this week. Again, I didn't know of him, I knew of him. I had heard and seen photos and stuff over the years. He was a close friend to a lot of people who I consider friends. And that's another.

passage of time kind of thing for all of us as we get older, I guess. don't know. some shout outs from your side. into sorry, Kostyngo.

Costin Raiu (01:36:40.254)
And by the way, just wanted to say there's a fantastic story about how Stealth was doing like an SSH man in the middle at a conference. When people are trying to do SSH, he was like just hijacking the connection, forcing the protocol down to V1 and doing this man in the middle to essentially steal people's things, secrets. And this...

Resonates with me so well, especially when there's people who talk about like you don't need the VPN like when you're at the wherever like use a public Wi-Fi stop Stop worrying about the VPNs. Just go if you hear any of those things just go and read this story because It tells you so much. Like I said, I've seen so many people got on that conferences using public Wi-Fi without VPNs So I thought it was a fantastic story

Ryan Naraine (01:37:36.236)
Shout out to Stealth, shout out to his family, shout out to all his friends dealing with this.

JAGS (01:37:41.678)
Since we're on this topic and I don't know, I don't want it to be on Couth, but there's an amazing book by the late Ernst Becker called The Denial of Death. And it's a phenomenal tour de force by somebody who is actually late stage cancer, who had been a psychoanalyst and a Buddhist. And he's kind of just facing face first, you know, this notion of inevitable.

death, which as for those of us who've ever enjoyed Heidegger, it's at least considered that like when a human being considers their mortality is the time when they're engaging with authenticity as opposed to anything else in our lives, right? Like that idea that we're going to be

here forever is like the heart of inauthentic thinking. So it's a phenomenal book and a good reminder to use what life we've got to do meaningful things.

with treading water.

Ryan Naraine (01:38:42.274)
Let me just end the show on a more lighter note. Juanito, noticed a Spotify wrapped drop this week for Spotify users and we've had a bunch of Spotify users post their minutes and how much time they've been listening to the show. It's been pretty fascinating, but I must mention you've been selling Apple and China books because the number one books read by the entire Three Body Problem audience on Spotify, their next

JAGS (01:38:48.044)
you

JAGS (01:38:53.934)
my god.

Costin Raiu (01:38:54.95)
Hmm.

Costin Raiu (01:38:58.751)
Hmm.

JAGS (01:39:00.503)
in-same.

Ryan Naraine (01:39:11.586)
bet their next highest red thing was Apple in China. now that you mentioned a new book, the denial of death, might, you might be selling some products there. My shout out is to all the Spotify audience. We have an active life, pretty significant audience in Spotify that I did not know about. They don't share. Spotify doesn't share numbers, but apparently over the last year we've grown what 366 % year over year, 1.1 million minutes. Listen.

JAGS (01:39:26.604)
We didn't know the numbers. We didn't know.

Ryan Naraine (01:39:39.968)
I don't know how these people expect to get those minutes back, but here we are. My shout out is to the audience all over and all platforms, YouTube. We have a bunch of people growing on YouTube, on Apple podcasts, on Spotify, wherever you listen to the show, shout out to you. Thank you for listening to us during the course of the year. Next year promises to be even more fun. Last words guys.

JAGS (01:39:59.534)
Yo, we're gonna start a fucking book club. It's gonna be our Oprah version where we just put the sticker on it.

Ryan Naraine (01:40:02.902)
Yeah, that's also coming.

Costin Raiu (01:40:09.578)
Let us know if you want us to give you more book recommendations like what one has been reading this week, things like that, let us know in the comments.

JAGS (01:40:16.94)
my god.

Ryan Naraine (01:40:19.058)
Absolutely. And with that, that's our show for this week. Thanks everyone. Have yourselves a great week guys. We'll talk next week.

JAGS (01:40:24.75)
Take care, guys.

Costin Raiu (01:40:25.706)
Ciao.
