Episode 38: Three Buddy Problem

A half-dozen Microsoft zero-days, Juniper router backdoors, advanced bootkit hunting

LISTEN:
https://securityconversations.com/episode/a-half-dozen-microsoft-zero-days-juniper-router-backdoors-advanced-bootkit-hunting/

WATCH:
https://www.youtube.com/watch?v=VSpUgA-ZaT4&t=4730s&ab_channel=ThreeBuddyProblem

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

JAGS (00:00.103)
There's a lot of bullshit in these stories that I don't quite know how to handle, even on the crypto attack side of it.

Ryan Naraine (00:10.068)
I will get to the crypto things later on. Hello everyone.

JAGS (00:11.939)
Just let's just not talk about I was about to say let's not talk about CSA for fucking 45 minutes, but you know since we're already at it

Ryan Naraine (00:14.774)
Hello everyone.

Ryan Naraine (00:20.246)

We will not, but I have some questions for you guys on the CISA news this week. This is the three body problem. We are up to episode 38. I'm here with my buddy, Costin Rayou, checking in from Romania. How are you, my

JAGS (00:24.644)
SudNews.

COSTIN (00:31.454)
Good, good, good. Maybe you've heard that the most famous candidate, Galen Gheorgheescu, in the history of Romania was banned by the Supreme Constitutional Court simply because he said, yeah, he's not eligible. So now Romania is back to square one. Like, who do we vote with?

Ryan Naraine (00:54.166)
Very great news coming out of Romania. Juanito, you look like you're shacked up in a hotel room again. What is going on with you?

JAGS (01:00.217)
I am shacked up. got summoned to the wonderful land of Mountain View this week. I'm now, yeah, yeah, actually really exciting work stuff, but not something to talk about on the podcast, but good, interesting days for Sentinel One. Yeah, and I actually found the one nice hotel in San Francisco for today. So we are recording out of an.

Ryan Naraine (01:09.301)
work stuff.

Ryan Naraine (01:19.424)
Good, good, good.

JAGS (01:28.015)
uncharacteristically nice place for San Francisco.

Ryan Naraine (01:31.254)
Thank you for welcoming me to your fancy microphone stand and everything. Commitment for the people.

JAGS (01:33.989)
I travel with the whole fucking arm now.

COSTIN (01:38.158)
Clam chowder, clam chowder, don't miss it.

JAGS (01:40.703)
yeah, the wharf. We'll go to the wharf. Sorry.

Ryan Naraine (01:43.934)
Let's jump into the news this week. It's Friday, March 14th around 9.30 in the morning here on the West Coast. We'll kick it off with this week was Patch Tuesday. Usually Patch Tuesday is a bunch of vendors dropping very important patches and people in the back backing mines just kind of humming their vulnerability management engines and doing things. But this week was particularly special for the just a sheer number of in the wild exploited zero days that have been covered. And I'll start with Microsoft. Microsoft

JAGS (02:00.166)
I didn't get that.

Ryan Naraine (02:13.642)
patched 57 vulnerabilities across the Windows ecosystem. And this week we got six new ODEs out of Microsoft.

JAGS (02:21.05)
Bro, you're the only one keeping track of these fucking old days, man. Like, they're just patching shit at random. People, maybe they're applying the patches. You're the only person paying attention.

Ryan Naraine (02:28.138)
Correct, they just say-

Ryan Naraine (02:33.204)
And I feel like every week we say Microsoft just kind of give you a bare bones bulletin advisory. No IOX, no nothing. You're kind of like, but Costin help me understand. There are IOX being shared in this map program. When O-days like this land, six O-days in a one big Microsoft patch Tuesday batch. What do you, what does the AV and the security vendors get? How long ahead of time help explain with map? Like why, when we're complaining about the absence of O-days.

COSTIN (02:56.206)
Mm-hmm. Mm.

Ryan Naraine (03:01.632)
the test detection, it's not really true because they've already shared it.

COSTIN (03:05.378)
Yeah, that's true. mean, this is probably one of the reasons why map was founded because whenever a patch like this was coming, vendors were complaining like, can you share some details? Can you please give us some kind of information that we can use to protect our clients, especially to allow us to protect the people who didn't install that patch because back in the days...

maybe for some systems like for some servers it may not be possible to install the patch immediately because it requires a reboot right and we've seen by the way many keys in the past when although a patch was available for some unknown magic reason it wasn't getting installed and downloaded so it was pretty big with that was super big with WannaCry I knew of people who had automatic updates enabled but there was essentially no patch being installed

So when MAP was founded, yeah, this is what Microsoft wanted to do to share information in advance. And typically what we were getting was POCs. In some cases, I think we got like a shell code. We got source codes, examples of the attack, like fragments, samples. So there was good information. I mean, it used to be very useful.

Ryan Naraine (04:21.59)
What are you using that information for? And just just to back up again, MAP is this Microsoft Active Protections Program. It's a program available for defenders mostly, right? It's just defensive focused security firms like EDR. believe Juanito, your team must be in MAP as well,

COSTIN (04:25.166)
Mm.

COSTIN (04:33.281)
Ideally.

JAGS (04:37.53)
Yeah, mean, most of the most of the defensive companies are though that that said, and I'll admit this readily, I try not to look at any of the map stuff because of the amount of like this kind of work that we do, where, you know, they're very strict about the rules sort of like maintaining certain levels of like, confidentiality on what comes in and out of map. yeah.

Ryan Naraine (05:01.024)
Good reason. mean, they've had leaks in the past. They've kicked out some Chinese companies in the past for like examples of like leaking information either deliberately or not. But we've had some issues in the past with it.

JAGS (05:10.106)
Yeah.

Yeah, so I keep myself kind of, I'm not saying I keep myself too ignorant of it, but I don't really kind of like pick up on it too readily. That, the kind of stuff that goes into map, I don't think is that encouraged for threat hunting as much as it is for like patching and maintaining of like your systems and kind of having a sense of what's going on there. But you know, that might be me kind of over-correcting a little bit. There's just been so many incidents of like people kind of taking, you

Ryan Naraine (05:29.77)

Detections, yeah.

JAGS (05:40.678)
using things out of map and using them in context that they were not supposed to. I just kind of bow out.

Ryan Naraine (05:46.656)
Right. One of the just as an intellectual exercise, like you mentioned Juanito, I'm the only one who care about this stuff. But one of the things I like to kind of poke through and look at the credits and who found which ones and so on. This week, it was fascinating to me of the six here days, four of them were reported quote unquote anonymously. What do you think that means?

COSTIN (06:03.862)
Anonymously. We talked about this in the past and we were like speculating it may be some intelligence agency. I does it mean they want to stay anonymous or the fact that like there's let's say some kind of a drop box, you vulnerability at Microsoft com or secure at Microsoft com and like anonymously an email appears. Here's the vulnerability. Can you guys patch it?

Everyone said, sure, we'll patch it. We don't care who report it. That's what I mean. If you ask me personally, I think it was maybe a government or an intelligence agency who spotted this. So either they're burning their queue, like as we discussed before about the NSA, every now and then patching some of the vulnerabilities they know about.

Ryan Naraine (06:34.73)
You think that happens? You think it really just drops randomly anonymously?

I'm asking what do you think, what do you think is at play?

COSTIN (07:02.986)
or simply catching somebody else using them. In particular, I thought that these vulnerabilities are interesting because they're all related to file systems and they can be exploited through USB sticks. Now I remember there was a very interesting zero day back in the days that was being exploited through an USB stick. So essentially all you had to do was to plug a stick with the malformed

file system and that would result in kernel mode code execution. And I think we build detection for that and we actually found one case when someone was trying to exploit it. I think it was a government organization that was being targeted with that. And I also was kind of thinking that these are some very, very interesting types of vulnerabilities.

that don't require any kind of clicking or interaction, all you have to do is to plug the stick and you'd be surprised how often that happens that people who find the stick they just plug it and that's all it takes if you have one of these zero days.

Ryan Naraine (08:10.866)
Also, we've found some of them were repredicted to ESET, which suggests they were also funding malicious campaigns. It's also possible that some of the elevation of privilege things happening alongside some ransomware campaigns to write it not necessarily directly government or nation state.

COSTIN (08:15.086)
Mm.

COSTIN (08:20.558)
Mm-hmm. Mm-hmm.

Yeah, so the anonymous ones were mostly like file system related, right? So somebody poking at the file system or fat, fast fat, while the one that is had found that Filip Jurkaczko, sorry if I mispronounced that, it. How would you pronounce that? How would you pronounce it? Filip Jurkaczko.

Ryan Naraine (08:32.882)
NTFS fast fat file system driver yeah

JAGS (08:45.062)
Is that how it's pronounced? I don't know. I have no idea. I have no idea. Come on.

Ryan Naraine (08:46.506)
That's amazing.

Jurzako, I would say it's your kacho.

COSTIN (08:54.06)
we're terrible now so

Ryan Naraine (08:56.147)
Sorry, this is terrible.

JAGS (08:57.008)
This is worse, it's only getting worse.

Ryan Naraine (09:00.064)
Philip, Philip from ESET.

JAGS (09:01.094)
Philip, Philip who does great research.

COSTIN (09:04.184)

Grzegorz Brzeczkiewicz.

Ryan Naraine (09:05.93)
Philip is pretty active, I've seen his name popped up in a bunch of discoveries before. So shout out to Philip, sorry for messing up your name.

COSTIN (09:12.738)
Sorry about that. But yeah, that's different. That's clearly one that, let's say, is a favorite of pretty much every kind of thread actor that needs to poke a Windows system because they need to escalate privileges. And this, like for instance, if you're on a domain controller, this is like a gold mine. Something like this that gives you system on a domain controller is amazing. But even without, let's say, a domain controller, it's

JAGS (09:14.405)
guys

COSTIN (09:40.408)
It helps a lot to gain privileges and to escalate so you can run better access code if you want.

Ryan Naraine (09:51.51)
There's a Microsoft Access remote code execution vulnerability that Microsoft says was discovered by a quote unquote website called unpatched.ai. Unpatched.ai is a very cryptic website that just lists, there's a listing of their vulnerability reports and they have been pretty active reporting Microsoft Access vulnerabilities. This is not the only CVE credited.

JAGS (10:02.446)
Yeah.

Ryan Naraine (10:17.386)
to this unpatched AI, in itself doesn't, the website doesn't say much about who it is, what it is, but Costin, we believe this is an AI powered thing. Is this one of those AI use cases that you've been talking about?

JAGS (10:21.286)
We made it. We finally did it.

COSTIN (10:26.67)
You

So, well, are you saying like this is the gen AI, like the general AI running a website by itself?

Ryan Naraine (10:31.892)
What is unpatched AI?

Ryan Naraine (10:36.788)
I don't know you tell me what is unpatched AI.

JAGS (10:38.67)
running a website it's not a company it's just the AI on its own

COSTIN (10:42.538)
Exactly. Please, please.

Ryan Naraine (10:43.274)
There's an about page. Let me read from the about page. find on patches using software to help customers better identify and manage cyber risks. Many issues are unknown or silently fixed by vendors hiding the true risk profile. With the help of AI, we are developing an automated platform to help find and analyze these issues for our customers. So they're selling some sort of feed against, if you look at the reports, they're promising some pretty significant things. But what stood out to me was how many CVEs they've had already applied the things they have found.

All listed as remote code execution. there's up there. They're up to something. Are these just crashes or we think this is just a fuzz or what do think is happening here?

COSTIN (11:22.574)
I read before the show I spent some time trying to dig who is behind that, know, with all sorts of tools, like looking at the domain which is unpatched.ai. There was almost nothing. mean, it's whoever made it really, really tried hard to stay anonymous. Correct. Correct. There's like some Reddit posts which you may be associated with them by a user. I think

Ryan Naraine (11:40.82)
went to great lengths to keep it quiet,

COSTIN (11:53.15)
That is not let's say a lot. It's not very much But to me what I was thinking about this website the fact that they claim We work with the US and US ally countries for the first impression was like this is China for sure because Because like if you're in China and you want to sell your your things then you need to say something like this because otherwise people was it's China

JAGS (12:10.719)
No... No way...

Ryan Naraine (12:17.162)
You just say that.

I don't think so.

COSTIN (12:23.104)

Yeah, probably not. But yeah, it looks like someone...

JAGS (12:25.178)
No, that's the kind of bullshit you get from any would-be US defense contractor, desiring subprime, right? We hired a bunch of NSA, FBI, CIA, former geniuses, none of them are listed on our website, and we're going to sell some stuff to DOD.

COSTIN (12:31.502)
Could be,

COSTIN (12:47.212)
I mean, looking just at what they found so far. I think it's maybe not necessarily fuzzing, but maybe looking at the library that access uses to parse databases. Like this is a database, think Microsoft bought it. Yeah, it's a database that they bought way, I think it was way before MS SQL. So it's kind of a database that

Ryan Naraine (13:00.48)
What is Microsoft Access, by the way?

JAGS (13:05.018)
Good question.

COSTIN (13:15.726)
predates MSSQL, which was used a lot, especially in accounting programs. So we were using this like, I don't know, 20 years ago. And what was interesting with Access, it was they were not relying on the OLEF format. Pretty much all the other Microsoft tools like PowerPoint, Office, Excel, they were using this object linking and embedding format.

Ryan Naraine (13:21.302)
Ugh.

COSTIN (13:42.762)
Access had their own format was like a different file format, which was kind of tricky to parse, but they think unlike Ole, it was fully documented. So back in the days, we had to write scanners to search for viruses in this file formats Ole, we had to reverse engineer. I think access was way easier, much, much easier because the documentation was available. So what I think they're doing is they're going through the

parsers, the libraries that access uses to parse this format, which is quite different again from the old jelly and embedding and trying to find branches that can result in buffer overflows, know, anything you can turn into exploits.

Ryan Naraine (14:28.95)
and they're using AI, you think it's all automated.

JAGS (14:30.278)
The name claims it.

COSTIN (14:31.758)
I would suspect they're using AIs to find those paths that can allow vulnerability exploitation.

Ryan Naraine (14:41.366)
Which is an amazing offensive use case. We've talked in the past about use cases for AI, some real life use cases. If this is accurate, and you can imagine these are not the only guys doing it. It must be powering a lot of the Bugbunty ecosystem as well. The guys who are searching for crashes there. Are you impressed by this Juanito?

JAGS (14:41.723)
mean,

JAGS (15:01.414)
I I think we're reading a lot into very little. Which is, it's not to say that it's not happening. It's just like we're not being shown anything, right? Like if you give us like some kind of blog or technical paper, basically saying, look, we're using these models, we're doing this X, Y, and Z, and it's working, then like we could genuinely start to evaluate that. That said, if they have figured it out,

Ryan Naraine (15:05.993)
We're guessing and speculating, yeah.

JAGS (15:30.2)
This is precisely what I would expect to see, which is to say you make some reports, you get some bugs patched, you don't tell anybody how you're doing any of it. And then you show up at DoD and say, Hey, we're the guys that just got these past like five bugs patched by Microsoft, Apple, and so on. And we're doing it with AI, be that true or not. you know, you buy shit from us. And,

Ryan Naraine (15:55.67)
Or VCs, or you go to VCs and say, hey, give me a lot of money so I can scale this. It's easy to raise when you can prove these CVEs,

JAGS (16:00.219)
bruh

COSTIN (16:02.306)
Mm-hmm.

JAGS (16:03.43)

Look, to be fair, A, I don't know that if folks figure this out, I expect them to tell everybody else how they did it. And B, I'm not even sure that I want them to. Like, looking at the situation right now, like we are back in a Cold War, like technological escalation type tit for tat with the Chinese. And they have benefited greatly from

The Chinese have benefited greatly from the transparency with which we have been putting things out without necessarily, well, I'm not going to say without reciprocating, right? Like they're contributing as well. But I don't know, man. Like once you get into this whole area of like, this is how we're automating like zero day finding. To what extent this, no, it's, it's, it's, and it's almost certainly already here to some degree.

COSTIN (16:52.558)
Mm.

Ryan Naraine (16:54.23)
It's coming, I mean it's here.

JAGS (17:00.324)
Like I think that the problem we're having right now, right? Like I don't want to sound super naive. So I personally believe that there's a certain amount of AI that is working for bug discovery in specific use cases. Like I think this is very, and like, would love to hear from Dave Itell, probably not on the podcast, but like to what extent that is working in what types of problems. Cause that's the real thing here. I think everybody expects like AI.

for bug discovery to work the same way as AI in general, where you go, hey, here's this use case, here's 10 use cases, and it's good for everything. And I think when it comes to bug discovery, what we're going to see instead is we have figured out how to instrument AI to be really good at finding this type of bug. Now we're going to work on a use case where it gets really good at finding this other type of bug.

you're going to start looking at it addressing sort of classes of problems the same way that Google's zero project zero has been worked has been talking about since the Ben Hawks days, like six years ago saying like we're trying to eliminate certain classes of bugs because there are certain kind of intellectual exercise. There are certain kind of like chain of thought that leads to certain kinds of bugs.

[AUDIO TROUBLE BREAK, HENCE NEW TIMESTAMP BELOW]

Ryan Naraine (00:01.71)
A story that I didn't put on the list, but I wanted to bring up quickly is OpenAI calling DeepSeek state controlled and calling for bans on PRC produced models. It's kind of related to what Juanito was just talking about this competition with China. This is an official policy proposal from AI describing DeepSeq as state subsidized, state controlled and recommending that US government consider banning these models. We talked about this on the...

COSTIN (00:15.502)
Hmm.

JAGS (00:18.989)
That's so funny.

JAGS (00:31.077)
Banning them from what? Banning them from where?

COSTIN (00:31.415)
Yeah, we talked and I said it's coming. I said it's coming. Remember?

Ryan Naraine (00:33.004)
We talked about this in the deep sick model.

JAGS (00:37.059)
the fuck are you banning them from? I'm sorry, this is like the funniest shit ever. I can't like, I cannot take OpenAI. Look, I am a huge OpenAI fanboy. I stan OpenAI all day long. And I think that there, if anyone's gonna win this race, at least in the people that are currently competing, it's OpenAI or someone we just haven't heard from yet. But like it's OpenAI is to lose. That said, when they try to get into this sanctimonious bullshit,

like trying to engage regulators, trying to do X, Y, and Z with like, you know, the involving the sort of patriotic sentiment. That's when they lose me. And I find this shit hilarious. Cause I'm like, you guys have been, you know, you've given no fucks about intellectual property. Originally you didn't want to have anything to do with the gov now. And now like, you know, the U S national supremacy represented by open AI is needs to be protected and protected from what open source.

Ryan Naraine (01:36.46)
Is there a little bit of a pandering to the protectionist nature of the new administration? what do you expect? What do they expect? This is an actual, so the Trump administration supposedly has an AI action plan and this was open AI submission. It's like, listen, these people are state controlled. We need to ban them from competing here. It feels like there's genuine fear around what DeepSeek and the open source models could present to them.

JAGS (01:36.504)
Right? Like what the

JAGS (01:43.085)
A little bit? It's the whole fucking argument.

JAGS (02:02.573)

I don't know if there's genuine look, maybe there is fear. That said, I don't think it's a good look for open AI. Not because of any of what I was just saying, but actually because the whole point with open AI is they've been saying, look, they came up with reasoning models. Like they're the first ones that show up with like O1 and O1 Pro and they're fucking awesome. I still, I love them to this day. I think they're great. And they were extremely confident.

as they were kind of even behind the scenes, right? Like I remember being at a CTF in Vegas and somebody actually asked somebody coming up and asking who had created the CTF because their internal model that had not been released yet was not able to solve one of the questions. And that was apparently very impressive. So they were like so confident in what they have internally.

and, rightly so, right? Like when we get deep research and you, and that's the only way that you can hit supposedly that you can hit the O3 model, not O3 mini, but like the actual hardcore expensive O3 model. what we were getting out of it was phenomenal. I think they've been tweaking that lately. I get the sense that they're trying to rebuild deep research with O3 mini, because I've made it too expensive because I think I'm the only asshole on earth. That's like hitting a hundred deep.

research queries a month. I'm trying to get my money's worth. and I love it, but no, no, no, no, no, no. No, I just, think that my guess is that I don't know. I, well, I got to like, got to 99 and I bitched about it on blue sky. It gave me a little thing. It was like, you have five queries left until like March 12th. And then I like started metering it, but then like in March 11th, I was like, fuck this. Like I started hitting it to see what happened.

Ryan Naraine (03:31.918)
Did they ban you?

Ryan Naraine (03:37.176)
What happens when you reach your limit? What do they tell you? No more deep research for you?

Ryan Naraine (03:44.824)
How do you know? Is there a counter somewhere?

JAGS (03:56.306)
No more complaints. So like I bitched about it on blue sky and they, you know, I don't, no, I don't think it was that. I think it just so happened to match up with the time when they gave 10 deep research queries to the people that pay $20 a month. And my guess is that's because they have somehow changed what's happening in the background to now use 03 mini instead of the full 03.

Ryan Naraine (04:02.606)
So you think you get referential treatment.

JAGS (04:24.311)
And I say that because the output is not as good anymore. We're starting to get output that doesn't fit. If you tell it what you want it to look like, seldom fails. It seldom produces what you're asking it to produce. So if you tell it, hey, I want three tables and visualizations and a four paragraph breakdown, that's it. I don't want 5,000 words. It still produces 5,000 words. it's, it's no longer following instructions that well in that sort of like wrap up.

process and I'm guessing that's because they've involved some cheaper model in the production of this sort of like well-harnessed deep research thing, which really bums me out because 03 was phenomenal. the whole this diatribe before like getting into the specifics about OpenAI, my point was they looked 10 feet tall because their tech is always like just one paradigm ahead or two paradigms ahead and they're like, we're fucking

We're cooking so fast and like making such cool shit that no one is gonna reach us. We don't care what the other people do. And then to all of a sudden be like losing your mind because somebody came up with an open source version of your O1 mini, which is supposed to be the distilled small version of your old, old model. And you're gonna act like the world is ending. It makes you look small. Like open AI should just be like,

walking it and not trying to play this kind of dumb ass game.

Ryan Naraine (05:56.012)
really good powerful open source model is an existential threat to them though right I mean in theory. Costin do you think what do you... No?

JAGS (06:02.211)
No. Sorry, Kosa, go ahead. Sorry.

COSTIN (06:05.369)
I would start by saying that yeah, it's probably time to make AI great again, like part of the new administration strategy to bring everything back at home. And I kind of I saw it coming like I mentioned it before, there will be a time when this will be banned like AIs from China, from Russia, wherever.

simply because the risk, I think the risk comes from integrating with them. Like when you start integrating building on top of that and you start putting them into your projects. With that, yeah.

Ryan Naraine (06:40.696)
Like you have an entire startup ecosystem. Let's say you have a venture capital startup ecosystem built integrating with these open source models from China and they're so embedded and now they're like, you know, filtering out into all kinds of other integration technologies. And now you can't rip it out. It becomes difficult to rip.

COSTIN (06:53.209)
Sure, yeah, the information, you can't, you can't, I, that's, what I think. And this is a reason why I think it's, it's not that surprising that some old man is calling for it.

JAGS (06:56.665)
Well...

JAGS (07:04.869)
But what's the problem? What like I'm saying in the sense of like, we need to make an important distinction here, right? Like, are we talking about Chinese open-sourced models or are we talking about sending queries via API to Chinese companies that are running those models? Because

Ryan Naraine (07:24.674)
I think we're talking also about anything, any sort of open source modeling or anything coming out of China that is connected to Chinese labs that are owned and operated by big massive Chinese multinational companies, right? Like anything that gives data puts.

JAGS (07:40.294)
I'm sorry, but like how much of our normal open source stack is currently being either partially maintained or massively contributed to by Chinese open source developers? How much of the fucking Android stack or Linux kernel is being contributed to by Chinese? And I asked that genuinely.

Ryan Naraine (08:00.526)
Then we just have this podcast, and we talked about this recently about Linux driver developers from Russia being kicked out. Yeah.

JAGS (08:03.855)
But like-

COSTIN (08:05.623)
Yeah, yeah, like Russian developers. Correct, Well,

JAGS (08:08.301)
Yeah. do even to like Ghidra. Somebody was where we were at reverse. We were like running a deep research query. We were like, Hey, so, can we get in? Can we profile all of the contributors to Ghidra in like the issues tracker and GitHub and be like, how many of these are from Chinese companies, Russian companies? Can you tell if any of them are from sanctioned companies? And yeah.

Ryan Naraine (08:27.15)

There's a documented case of the NSA responding to positive technologies support request for Ghidra and getting tech support from the NSA back to positive technologies. This is documented.

JAGS (08:36.441)
Tech support, man.

The vector 35 guys are just like eating their heart out, know, like killing it on an, that's an actual American solution being built and whatnot. That's being undermined by a government funded project. know,

Ryan Naraine (08:53.356)
Right, but when we consider the TikTok conversations we've had in the past, what Costing is referencing here, I think he's right. think eventually coming down the pike, you're going to just have to ban these things. Juan, you don't see a big risk involved, but I think there's an embedded supply chain kind of ecosystem threat that is real.

JAGS (09:04.588)
No, no.

JAGS (09:08.741)
Yes.

JAGS (09:13.081)
Yes, within measure. that's why I like, that's why I'm trying to like put some, I want us to define what we mean a little more specifically. And it's not because I don't know that we're doing anything wrong. I just think that these sorts of claims and asks are purposefully vague in ways that.

are not helpful, right? Like, and maybe even on purpose, right? If OpenAI is calling for the banning of these Chinese models, maybe they're hoping that somebody is gonna overreact and overreach towards something that's even unthinkable because look, the idea that we should ban the use and integration of Chinese companies hosting models or even foreign companies hosting models, I think is reasonable.

you're sending out an API request. It's hidden away behind some LLM wrapper, right? Like you, you, we start a company called, you know, food.ai and, and it, people get to the Pentagon. People get to order their food through our little interface. It turns out it's just a wrapper and we're sending our requests to deep seek in China to resolve all that data and send back the result. Okay. Totally understand why you don't want to do that. You're literally sending information from

US whatever, without people knowing to a Chinese company to analyze, without anybody knowing and you're relying on their output that they're sending. So I can understand why that's a use case that you want to avoid. At the same time, we should not overreach in the sense of saying, you should not be using these open source models in ways that you host in the US that you're hosting as a company yourself.

because frankly, open AI is not contributing shit to the open source ecosystem. And that's where the real innovation is going to come from. Right? So like, if you guys are so worried about the Chinese, you know, infiltrating American innovation with a reasoning model. Well, the only reason anybody cares about that is because no American company has released a reasoning model as an open source. Anything. If I could use.

JAGS (11:28.491)
Meta like Facebook's thinking llama as a model 32B whatever then I would use Facebook's thinking llama instead of using Quen QWQ32 or DeepSeq R1 but no American company has open sourced a chain of thought models. So what the fuck are you talking about? You're just telling companies to sit it out the technology sitting there and you're just gonna be like, no, no for America for the flag.

who are just not gonna use this Chinese shit, like on my Chinese built computer with my Chinese contributed to software. Like what the fuck, man?

Ryan Naraine (12:05.688)
cost didn't before. Go ahead.

COSTIN (12:05.817)
Look, look, I think it's important just to maybe balance the discussion because I see what Juan is saying here. It's to me is very, very surprising because Juan was always Mr. America. So I would have expected him to, yeah, with the make AI great again, but I see, I see the risk.

JAGS (12:21.295)
Come on.

JAGS (12:27.333)
Stay unpredictable, man. Stay unpredictable.

COSTIN (12:32.792)
coming from integrating this open source model from China in the sense that just to give you an example, you leverage the model to write reports. And let's say in particular, this model, the way it writes the reports, it subconsciously encourages a certain narrative in the report. So from that moment on, your reports will be pushing subconsciously, maybe it's not immediately obvious, a certain narrative about false flags, about attribution perhaps.

about naming adversaries, about blaming China if you want and then this is everywhere like you integrate you don't know how it gets integrated in pretty much everything from maybe smart TVs to to pretty much everything you can imagine in your life and then suddenly you realize at some point that the news that

Washington Post is showing or New York Times, they're like flagged as disinformation by your smart TV because it relies on reports which have been produced with this open source model. So this is the of thing, the kind of risk and this may not even come from the first generation of those models. What will happen most likely you will integrate and they say like, yeah, from now on we use only open source DeepSeq. And then let's say R2 will come.

R2 will be vastly superior and R3 and R4 and so on and at some point these models will begin to have a bias for one reason or another they'll be biased in a certain direction and you'll have to update your model if you want to be better if you want to have more parameters so better knowledge more recent knowledge and I think that's where the risk comes from going into that streamline like with that

direction for the future and the models that will come in the future.

JAGS (14:26.421)
You see, don't disagree with that at all, except that I don't think it's a future problem. I think it's a problem we have had for two years now. the notion that like, I'm glad the Chinese have introduced paranoia into a space that should have evoked paranoia.

from the very beginning, right? Like the issue here is you have, like, and we've had AI ethicists bitching about this nonstop forever, since before it made any sense to discuss. But the whole point of these models is that they are lossy compression systems that essentially reflect human bias at a variety of levels.

COSTIN (14:55.257)
from the beginning.

JAGS (15:24.517)
And moreover, that bias is even present in the prompt engineering that we do. Half of the problems that we get are people don't understand that they're asking leading questions just by virtue of just the way that you formulate the question, right? Like, Kostin, the other day you run that query, right? Like, who's the smartest of the three? Like, who's the most intelligent? You're like, look, I was like, look, man, just by saying who is like intelligent in itself.

Ryan Naraine (15:52.29)
Who was?

JAGS (15:53.542)
It's a whole lot of bias that you're pumping into it as to like, what's a valuable feature as opposed to, you know, it's sort of like having to iterate on its own perceptions. And that's us introducing bias. And then the model itself between the training data, the way that it's refined and fine-tuned, like it is bias stacked upon bias. And I am not in any way so...

trusting or excited to accept the bias of American companies, particularly at a time when American companies are serving as like robber barons and don't give a flying fuck about anything, not regulation, not this country and not any and not employees, not the health of the economy. They don't care about anything or anyone. They're just gunning through.

Ryan Naraine (16:38.988)
DeepSec doesn't either. mean, the folks behind DeepSec you think are paying attention to IP laws?

JAGS (16:42.329)
But no, no, no, my point is not, my point is not at all that like American things suck and therefore the Chinese things are fine. My point is this is a problem with the fact that we are now taking some fucking, like we call them models and we call it AI and that makes it novel, but we're just taking software and having it spit out evaluations at us without clear criteria because the criteria itself is not observable.

And the whole point of it is that we shouldn't trust any of it. And the problem that you have is simply what is it gonna mean to consume the output of generative AI regardless of where it comes from and have guardrails and a sense of evaluation and a sense of like what the reasoning is behind some of these choices.

And that's a bigger problem. is a technical problem of like observability in models, which is not a solved problem. go, well, how do we know if this thing has been manipulated or if it's been pushed in a certain direction or if a bias has been artificially introduced, right? Like that is observability into what is essentially a giant matrix of statistical probabilities for arbitrary tokens, right? Like that's not an easy thing to discuss. And then

You also have this notion of regardless of whether the model itself is biased, is the prompt introducing a kind of bias? Is the wrapper introducing a kind of bias? Is the system prompt that you don't see introducing a kind of bias? Then what bias is the user putting into it?

And finally, none of it matters because what is happening with that output and how are people going to consume it? And we're right back to, okay, now you have an infinite amount of sources of shitty content trying to push you in different directions. But you know, five years ago, this was a discussion around Fox News. They're fucking, it's peddling lies all day long at Boomers with no discernment. What do we do tonight at nine?

JAGS (18:53.027)
Right? Like no fucking clue. And the real issue is a lack of like education and discernment general like anything. And our world is now being run by people who are proud of dropping out of school. And it shows. Right. It's just.

Ryan Naraine (19:07.992)
Kostin is there anything else to talk about with the unpatched AI?

JAGS (19:11.541)
Ha

COSTIN (19:11.801)
Okay, I was thinking that any

Ryan Naraine (19:15.362)
get us off that tangent. Just quickly, is there any? Yeah.

COSTIN (19:21.497)
Any kind of bias, just keep this in mind. It's very much similar to disinformation ops against elections and whatever. You don't need to do like the 50 % obvious bias. All you need is the 5 % bias and that 5 % bias which is invisible, like no matter you can apply whatever

tests you want, they will not catch the 5 % or 1.5 % bias. However, its cumulative effect over the years will be felt. So I do think that yes, probably you need to be careful and you also probably need to balance like run several models, Western models, Chinese models, Arabic models, Taiwanese models.

Japanese models and try to make the best from them. Run another model which just distills the output from all of them and draws a conclusion. And you may actually have to do that. I think I mentioned it before that I was asking some questions about the elections from this podcast with Eric Weinstein and Google's Gemini didn't want to digest it, didn't want to give me a summary. They cannot talk about the elections. So had to use DeepSeq for that.

JAGS (20:44.933)
fuck

COSTIN (20:45.186)
And it's funny. I use the Chinese model to discuss the US elections.

Ryan Naraine (20:46.03)
We'll use the Chinese models to figure out what's happening in the US.

JAGS (20:47.397)
That's some dumb, that's some dumb ass Google bullshit. That's the typical over, that's how you end up with a model that makes, what was it like black Nazis and Asian, you know, like stormtroopers from World War II, right? Like it was just like, what, that's somebody thinking ahead into like thinking that they can actually, well, yeah, over-correcting by thinking that they can just enhance the guardrails in the system prompt to have like,

COSTIN (21:01.389)
Yeah, right, right.

Ryan Naraine (21:09.59)
overcorrecting it.

JAGS (21:16.629)
extreme inclusivity as if that's what solves these problems. I think, Kostin, you're hitting on an interesting and actually important idea here, which is there's a certain laziness right now into agentic workflows and this notion of, what is it, chain of experts and that kind of chain of thought model in that whenever you're talking about these solutions,

What's happening is there's a certain amount of orchestration and harnessing around a single model. And what you say is like, Ryan asks me a question. I spawn a version of the LLM that's like an overall like orchestrator, like a orchestra conductor, but like this, this person who evaluates that question and says, what, what kind of experts are needed to answer this question? And then you spawn.

multiple iterations of the same model with a prompt that tells them to act as if they are this expert. And then their output is synthesized. But there's a laziness in that in that it's the same model under the hood for these different personas, because they're general purpose frontier models. I think to some extent, if we want to fight algorithmic bias,

you're kind of going to have to fight it with an algorithmic solution, which is to say, what does it look like to have these chain of thought models and these like multiple panels of experts and agentic workflows where there are multiple models being used for the multiple opinions that are supposed to come? And that just like honestly, right now it's an arbitrary flavoring kind of thing. Like is it R1 or is it QWQ or is it O1? But in the future, hopefully,

what it's going to be is, is specialized models, right? Like this Harvey AI thing where it's like, we we've been fine tuning a model to just be really good at like legal advice and, and, know, helping lawyers and that, like, that would be the true version of a panel of experts is we have fine tuned models to be specifically good at this, that, and the other. And I think that's, that's, that's not too far out in the horizon. And at that point,

JAGS (23:39.213)
we can have different discussions about what it means to actually have expert models on spec that are talking about things with each other rather than have generalized valuable models trying to cosplay and LARP as experts in this, that, and the other.

Ryan Naraine (23:57.144)
This week's Patch Tuesday also dropped us iOS.

JAGS (23:59.302)
You

Ryan Naraine (24:02.318)
iOS 18.3.2 with a WebKit 0D that's marked as exploited. The language from Apple is that this may have been exploited in an extremely sophisticated attack against specific targeted individuals. And they the exploit worked on versions of iOS before iOS 17.2. This is the same language we just heard about with the USB bypass. The tethering.

COSTIN (24:08.022)
you

Ryan Naraine (24:31.05)
exploit from I believe a month ago or maybe a few weeks ago. Again looking through the credits here it says credit Apple. What do you think happened here Costin? You think this is just them figuring out something based on an old investigation or this is something fresh?

COSTIN (24:33.209)
Mm-hmm.

COSTIN (24:46.553)
So I looked a bit into this story because they actually they say this is a supplementary fix for an attack that was blocked in iOS 17.2 So immediately I wanted to see which attack What are they talking about? Like this is a supplementary fix for which specific attack? so I looked a bit at iOS 17.2 and

It actually patched a couple of webkit vulnerabilities, I think most of them were reported by Chinese researchers, but it wasn't somehow connected to something big or if you remember the language that Apple uses, Apple is aware that this may have been massively exploited, that language is not in 17.2, however, that language is I think in 17.0.2.

And in particular, that is related to Predator, the Predator chain, is way more interesting in particular. I wonder if it's a mistake and they mean 17.02 or like, are we missing something here? Because that chain, the one that CitizenLab wrote about in 2023 and Google Tag also wrote about, so that was a pretty big discovery of

Ryan Naraine (25:45.646)
Yeah.

JAGS (25:49.349)
Was that a mistake?

COSTIN (26:10.073)
Predator using being deployed in Egypt through man in the middle Which is exactly the same reason why you have to use VPNs because your ISP can Deploy and they have deployed Predator with three zero days on to people's iPhones through man in the middle attacks happening At your telecom provider and this is exactly the kind of attacks that VPNs defeat

So I was wondering, yeah, maybe it's related to that. Unfortunately, no information, but it would make sense to be 17.0.2 that patch, not 17.2.

JAGS (26:47.173)
Pardon me, but the other alternative being that three zero days are deployed through the VPN service, right?

COSTIN (26:58.239)
Yes, but then it wouldn't be your government. Like, who do you worry about? Do you worry about your government who can put you in prison for advocating for deep sick instead of open AI? Or do you worry about your, you know, friends, your friends from a different government, like maybe from Guatemala or what was it? Lesotho? Have you ever heard of this country? Lesotho?

Ryan Naraine (27:01.944)
Yeah.

JAGS (27:01.965)
I'll...

Ryan Naraine (27:11.842)
Yeah

JAGS (27:25.347)
No, there's what? Are you serious? What?

Ryan Naraine (27:25.612)
Yes, yes, it's an African country, it's a small African country, yes.

COSTIN (27:29.334)
Deploying the Zero Data Area. I'm just making a, making fun of you.

JAGS (27:31.974)
but, that's my point. Like, no, no, no, no. Okay. At least it's expensive to set up a fucking telco. It's expensive to get in an ISP. It's expensive to do this. Like my issue with the, with the VPN thing is, is always like who it's the same discussion we keep having who owns this fucking VPN. And does that person still own the VPN tomorrow and the day after versus somebody walking up being like walk away.

COSTIN (27:41.611)
It is.

Ryan Naraine (27:49.527)

Wants it

COSTIN (27:58.329)
Let me meet you right there in the middle, like deploy your own VPN, like bio VPS, cheap VPS, a digital ocean, wherever, host it in Germany or I don't know, in Singapore and deploy your own VPN and then you'll be fine. I think against these kinds of attacks.

JAGS (27:59.674)
Here's 30 million dollars. Fuck off, right? Right.

Ryan Naraine (28:00.054)
or who is the other person who's owned it, right?

JAGS (28:18.277)
Just tail scale that bitch.

Ryan Naraine (28:22.766)
Quick question, quick question. Why are people still on iOS 17.2? Is there like a technical roadblock that blocks people from upgrading to the latest 18.3.2? Is there like all the devices can only get up to 17? What's the?

JAGS (28:22.895)
That's fair, that's good. As long as nobody pops the server.

COSTIN (28:32.537)
Mmm.

COSTIN (28:39.001)
See what they mean here is that it was originally blocked so they did a patch in 17.2 maybe even by mistake this is not clear or 17.02 there was a patch and they did a supplementary fix because it would appear that you know it happens that the patch is not complete like under some special conditions it can still be exploited so we're gonna close it the right way yeah so that could explain it

But to answer your other question, are, for instance, if you have an iPhone X, that one is limited to iOS 16. So you cannot put even 17 on it. You cannot put 18, obviously.

Ryan Naraine (29:18.526)
I see. So some of the older devices, the newer operating system wouldn't get loaded on it. So in some cases where there are these activists and so on, we're guessing that they're running old machines that can't possibly be updated.

COSTIN (29:24.663)
Alright.

Look, an iPhone X is a wonderful device. like, it's still, I've seen people with iPhone X which was beautiful, like the design itself was beautiful and the phone still works excellent. The battery is fine, the phone works very well. It just doesn't get newer iOS versions, unfortunately.

Ryan Naraine (29:50.862)
There's another OD I wanted to just bring up, just to close the loop on the batch of zero days we saw this week was one from FreeType. FreeType is an open source font rendering library, font library. Facebook actually put out an advisory saying, listen, this vulnerability may have already been exploited in the wild. CVSS 8.1 out of 10. It popped up in my head because I've seen FreeType before.

in a Chrome ODE exploit from a couple of years ago and in a Project Zero description of like a threat actor that had multiple ODE's and had access to a whole cache of things. Including in there was a free type ODE that they had held on to for a long time. What do you think is happening here, Kostin? Does this look like ODE here? Do we think it's ransomware? What do you think is happening here?

COSTIN (30:23.437)
Mm-hmm. Mm.

COSTIN (30:36.513)
Look, what bothers me when I say things like this, me and I think a lot of other people not being native English speakers, can you explain what is the difference between this vulnerability may have been exploited, could have been exploited, should have been exploited or might have been exploited? What's the difference between or has been exploited? Well, has is obvious.

Ryan Naraine (30:55.374)
You

or has been exploited.

COSTIN (31:04.313)
What is like may have been? How do you like it means we don't know or we don't know if it wasn't exploited like how do you how do you read it?

Ryan Naraine (31:12.494)
Juanito, you're the native English speaker.

JAGS (31:16.419)
fuck, really? of, You can see why the white nationalists are like up in arms. So, well, I'm kind of sitting here with it where it's like with, when I read may have been exploited, I mostly see it as like, in my view, particularly whenever we're talking about, let's say like Apple advisories, like may have been, like I find those really disingenuous because they know

Ryan Naraine (31:26.582)
It's lawyer speak.

JAGS (31:45.552)
they have been exploited and they're just kind of hedging their bets. I don't know why. honestly, it may very well be even be like a liability thing or like if there is a lawsuit about, know, you know, human rights activists getting targeted by some country that Apple can't perhaps has a way to wiggle out of being in the middle of the situation by saying like, well, we got a report, but it could have been this.

COSTIN (31:46.765)
Mm-hmm. Mm-hmm.

JAGS (32:11.393)
you know, it's reasonable to believe that it may have been this, but we don't know. Like, I think it's more on the lawyer speak side of things. I think you also, and I say that because in those situations, I think it's reasonable, like it is beyond reasonable to believe that it has been exploited because you have discovered it by virtue of somebody reporting an active exploitation in the wild. So the notion that it may have been is

COSTIN (32:36.185)
Mm-hmm.

JAGS (32:38.617)
disingenuous. It has been and we have become aware of it because of that. At the same time, in different situations may have been makes sense, right? Like we found the vulnerability. It's actually not a really hard vulnerability to find and

Other people have exploited vulnerabilities in this area or attacks have happened where we don't know how they happened, but this component was involved and there's an easy vulnerability in it, but we became aware of it because we were doing a code audit and you go, it's possible that these attacks that happen. I'm just saying if you're, if you're asking me to parse the language as if it's in good faith, those are the situations where I would.

Ryan Naraine (33:18.688)
I don't think that's what's happening here, do I? That's a stretch.

COSTIN (33:20.857)
You

Ryan Naraine (33:24.096)
Right, right, right. Fair, fair.

That's not a good faith one though.

JAGS (33:29.155)
Where I would write this may have been, but like it's all, it's.

COSTIN (33:33.091)
How would you write it if you knew this has been exploited? Would you say, we have indications that this may have been exploited, which is different from it may have been exploited.

JAGS (33:37.463)
I would say it has been exploited. wouldn't, you know.

JAGS (33:44.854)
No.

Well, no, no, no. I mean, look, when we see that something's been exploited, you go, this has been exploited, right? Like it did. And that's why I was looking for the situation in which I would write it may have been exploited, which is to say, I know this vulnerability exists in this component. And then I know there was an attack in which this component was exploited, but I don't have the incident response materials to say that this was the exact Oday that was exploited in that component.

COSTIN (33:53.195)
Hmm.

JAGS (34:16.739)
So it may have been this Ode. And that actually I think applies a lot when it comes to these like garbage network appliances, because there are so many exploits and some of them are known and some of them are patched and some of them are unknown and some of them are not patched that it may have been this one, but they had 12 other ones to choose from. So who the fuck knows, right? Like that is a good situation for it may have been this exploit.

There was definitely an exploit, I just don't know which one, right?

Ryan Naraine (34:50.094)
Who typically uses free type? Is it just the browser makers and some apps that like render fonts and I think like who needs to pay attention to this and scramble the patch.

JAGS (35:01.049)
I'm actually not sure. I'm not that familiar with this free type thing. Kostin, do you know?

COSTIN (35:06.201)
I looked a bit into this. It's interesting that in particular this version that is vulnerable has already been replaced with newer versions. So somehow the surface of exposure is not that high. In

particular in the past this has been used to target Android users. So like it's always I think it's very very difficult when you

when you're trying to exploit mobile users that maybe, know, through Chrome sometimes and actually in many cases, it's not necessarily a Chrome exploit that gets you in, but it's one of these things. Like one of those libraries that is like used for some obscure historical reason, it's still in there and it has a vulnerability. It supports this file format that you can deploy fonts from the web.

and the browser renders them. And this is like the reason why these libraries are still embedded into all sorts of products like browsers. And this is why they're a favorite target of thread actors. Now, it would be nice to know who was using this chain before in 2020 when Google found this.

old free type zero day targeting android and i think they said that the same threat actor also had windows and ios change so that's like a full i wonder if was candiru or if it was somebody else probably or one or maybe maybe somebody like dark hotel you know given their google's fondness for catching them but unfortunately there's

Ryan Naraine (36:42.894)
Might have been one of those private sector offensive actor type groups, right?

COSTIN (36:56.735)
no public information as to who was behind the CV 2020-15-999 from 2020.

Ryan Naraine (37:06.926)
I'm just fascinated that all day reports are just dime a dozen these days that we just kind of flip by them as just another quick news story. You remember back in the day when a zero day was a zero day?

COSTIN (37:12.633)
I was looking at the story but like you look at the at the story right for this week it's seven zero days like this is another thing seven zero days other stories say six zero days but it was six in the wild right and there's a seventh one and 57 flows and I was wondering

JAGS (37:21.399)
Old man yells at Patch.

Ryan Naraine (37:23.182)
That's exactly right.

COSTIN (37:41.151)
Aren't those 57 flaws also zero days?

JAGS (37:45.286)

I mean, I guess it depends on whether they're making a distinction between a vulnerability and an exploit. Like that is in itself an important distinction. then, you know, has it been used? I mean, look, the whole point of an O-Day is it's based on the awareness of the code maintainer. So.

Ryan Naraine (37:47.628)
the definition, I think we use zero-day to describe exploited in the wild, yeah.

COSTIN (37:55.224)
Mm-hmm.

JAGS (38:12.781)
I suppose there's some fine argument to be made about whether like, is it a vulnerability versus an exploit? And is it something that came into awareness from the outside versus from the inside? Like, is that, is that a distinction worth making? And all of this is just parsing like legal bullshit. Well, but it's all legal bullshit. There's no reason to really do it other than like, you know, splitting hairs.

COSTIN (38:30.689)
Mm-hmm. Mm-hmm.

Ryan Naraine (38:32.034)
Yeah, it's too inside baseball exactly, mean.

COSTIN (38:36.441)
Worst case.

like worst case or the best case they patched 57 zero days

JAGS (38:47.799)
I don't know man. The fact that there were 57 zero days to patch might be a bigger problem to discuss, right?

COSTIN (38:54.937)
That's what I mean.

Ryan Naraine (38:55.215)
If it's in an end-of-life project, is it still zero-day?

I ask because the next story is Mandiant finding some Chinese actors using custom backdoors on some Juniper routers. I mean, we've had this in the past as well, but this specifically is against end of life software and hardware, end of life routers. But Juniper actually issued a patch yesterday and the same day that Mandiant announced that they found this custom backdoors linked to a Chinese espionage group, Inc 3886.

COSTIN (39:01.641)
It's still a zero day.

JAGS (39:04.301)
It's a forever day.

Ryan Naraine (39:30.764)
Juniper released emergency patches to patch this vulnerability. Again, it's end of life thing. Kostin, have you looked at the IOCs here? We've got a lot of IOCs and telemetry data from the Mandian folks. Who are the folks behind this?

COSTIN (39:43.073)
I looked at this and there's two Yara rules as well and I noticed that those actually the Yara rules they do catch some older stuff that Mendy and wrote about. So I guess this is a kind of an overview blog post which looks at UNC's 3886 activity over the past couple of years.

Ryan Naraine (40:03.105)
Old stuff,

COSTIN (40:08.791)
And I thought at the same time it was really interesting that they do say there that by the way, this UNC targeting old routers, considering everything that's going on, it's not vault Typhoon and it's not salt Typhoon. So this is as far as we can say it's not them, but again, like, yeah, it's pineapples and ananas. So who knows.

Ryan Naraine (40:20.366)
Correct.

Ryan Naraine (40:33.934)
The specific flaw was reported by someone at Amazon, but they made it clear that in at least one instance of malicious exploitation was reported and they made it very clear not at Amazon.

COSTIN (40:46.483)
Mm hmm. Well, I think it's an important it's an important mention there. And I would do the same if I was reporting. I would say that, like, by the way, we don't use any of these old things here. It was never exploited in our infrastructure. So I would do the same because these days people like there's all sorts of podcasts and people jumping to conclusions and speculating and not doing fact checks. So you never know.

Ryan Naraine (41:11.406)
You

Ryan Naraine (41:17.356)

What is tiny shell? My man didn't made a point of like making it clear this is tiny shell based backdoor. Is that a previously known thing that you guys understand what they're trying to say?

COSTIN (41:26.253)
It is.

You wanna talk one about tiny shell?

Ryan Naraine (41:30.53)
Yes.

JAGS (41:32.678)
I mean, it's a... So, it is like sort of like a really bare bones open source, like as the name suggests, right? Like this sort of like minimal set of functionality. And I believe it's more like broad Unix, right? Like they're using it for free BSD, but you basically could just compile this thing out. But what they're saying is you're taking this open source, very minimalistic...

piece of malware and then they're tacking onto it other functionality that they can use. So like for more specific, like you want it to turn into a passive backdoor, it's waiting for a very specific packet to turn it on. It might do like a proxy redirection into that network, right? So you say, hey, I'm gonna come in through this port. If you see this magic number, then activate that.

and redirect me as an internal proxy through that port into the internal network, stuff like that. just the value of open source.

COSTIN (42:37.529)
Some people also might remember it under the name MIPSUN. We used to call it MIPSUN back in the days. think during our yara trainings there was an exercise for one of these variants, one of these backdoors, if you remember it.

JAGS (42:53.893)
It was a specific Chinese campaign though, right? With that MIPSUN. Is that right?

COSTIN (42:58.689)
I think there's been like several over the years. That one was compiled for Solaris, the one that we were looking at back in the days. But I mean, yeah, nowadays there's a lot including for Windows. I've seen it for Windows. What I was thinking here is that it's always interesting like that routers and this kind of hardware, old hardware.

is kind of living in a different world from the rest of the industry. So pretty much every kind of router nowadays, it doesn't get automatic updates. You have to manually, like in some cases, there's not even a button, check for updates, apply updates. Like the most modern things, they have these buttons. But some of the really old things, you need to download the firmware binary file.

JAGS (43:31.77)
Mm-hmm.

COSTIN (43:54.177)
from the vendor site where some cases you cannot download it because you need an account and you cannot get an account unless you pay so you need to download the firmware go to the device manually and upload it and reflash it with the new firmware so i wonder how difficult it will be and what impact this emergency security update will have in the sense that will people actually download and apply it? everyone's running? exactly

JAGS (44:18.119)
everyone's running to do it, right? I'm sure everybody spends all day just staring at that website waiting for the next pad.

COSTIN (44:23.812)
So I...

Ryan Naraine (44:25.87)
Shout out to Juniper though, they've issued a Juniper malware removal tool. Have you looked at that? It's interesting, it's a utility to scan for and remove malware running on Juniper network devices packaged with JunoOS and JunoOS evolved by default. It's similar to antivirus software for desktop except that it runs on a Juniper device. So that might be worth looking at.

COSTIN (44:31.331)
I have not, no.

COSTIN (44:45.433)
Do you need a paid account on the Juniper malware support toolkit portal support site?

JAGS (44:49.613)
Almost... almost certainly.

Ryan Naraine (44:53.25)
They also have an integrity checker. I think that, mean, they must be shipping some signatures in a malware removal tool,

JAGS (44:58.699)
I don't know, bro. Remember the last time we talked about one of these fucking malware removal tools on like one of these appliances. It was literally like restart the thing. So it disinfects itself that upgraded to this, then run the malware removal tool, which will almost certainly not find any malware because you just disinfected the damn thing. And then it turns out it's just like a bunch of like hash checks and you can change the list from inside of the, of the fucking operating system. So it's just like,

Ryan Naraine (45:16.115)
You

JAGS (45:27.041)
It's beyond performative. It's like nineties antivirus bullshit. And you're being given instructions that like, you know, only make the situation worse. which is not this. Why are we shouting out Juniper?

Ryan Naraine (45:37.686)
Hey, shout out to Juniper. I mean, we're yelling at people for releasing a malware removal tool now. Come on.

JAGS (45:45.144)
I were yelling at people. I'm yelling at people for, for having like garbage software stacks and this look, man, like I'm, I don't know what happened under the hood here. I don't know what happened behind the scenes here, but I would be very surprised if like Juniper figured this shit out and called Mandiant to get them involved. This is almost certainly Mandiant figured some shit out, called Juniper and wrangled them into doing something about it.

COSTIN (45:45.227)
No, we're not yelling.

Ryan Naraine (45:48.462)
You

JAGS (46:15.149)
And fine, if they did something good, then great. But I'm just, I'm not ready to shout them out. I'm not ready to shout anybody out,

Ryan Naraine (46:21.58)
I'm just amazed that they actually have a team that shipping updated signatures into a malware removal tool. means that there's...

JAGS (46:26.563)
You mean they have like some software developers still? Cause frankly, I am surprised that there are any engineers left in supporting any of these appliances. Cause as far as we can tell, all the code was written 15 years ago and nobody has, and the patches are literally like, can we change the two lines that address this one specific vulnerability in a land of many of vulnerability, hopefully without disturbing any of the other vulnerabilities. So the Chinese can just keep doing what they're

Ryan Naraine (46:53.23)

It's funny how we can just interchange the names. You can say Juniper, Sonic Wall, Evanti, you can't tell them apart. And nothing changes.

COSTIN (46:54.649)
You know?

JAGS (46:57.963)
I can't tell them apart. cannot tell them apart. Fuck these companies.

COSTIN (47:04.121)
You know what is the biggest challenge for these companies and maybe it's not, think fully appreciated the fact that, and I've seen it for myself when you need to patch a bug in something like that and you don't have the compiler, you don't have the compiler that was used to compile like the original firmware because the modern compilers they'll produce like a huge

fat binary that just doesn't fit in the memory of that device anymore and then you're scrambling to find the compiler from the 1996 that was used to compile that firmware like this I think there's not enough appreciation for like the effort that this company is actually put into keeping all the compilers and the old software needed to rebuild this firmware from paleontology ages

JAGS (47:54.054)
feel like there's a fundamental problem in there though. Right? Like it's not like they're doing us a favor. It's their fucking business. Like it's there. It's literally their business. These appliances don't sell for like 300 bucks or 30 bucks. Right? Like when we're talking about like dealing, you know, these like bullshit TP link routers and you're like, yeah, the margins don't even exist. you know, expectations are super fucking low.

COSTIN (48:06.201)
Hmm.

COSTIN (48:11.747)
Hmm.

JAGS (48:21.571)
but we're not talking about that. I'm assuming these appliances cost like five figures, I'm guessing. And like, I don't know how quickly they're getting end of life. If it's 15 years, okay. But if it's five, I don't know, bro. And like, frankly, you know, if it is something you are actively maintaining, then having a functioning, you know, pipeline for just comp-

piling patches is not like beyond the realm. I'm just saying like I it's not that I don't want to give them credit. It's not that their jobs aren't hard. It's just that it's literally their job. Like it's it is the description of their job to like build and maintain these fucking things. So like expecting the bare minimum of like not having these be Swiss cheese for foreign adversaries to do whatever the fuck they want. Moreover, for ransomware groups to do whatever the fuck they want with them. It's not, I'm not ready to pat them on the back for any of

Ryan Naraine (49:25.48)
Alright, shout out for your malware removal tool. It justifies that you know that there's malware there and you're trying to do something. It's better than nothing.

JAGS (49:33.466)
Bro, I cannot wait to hear the next report where we also find out that it's just a list of hashes. It can be modified on disk and the fucking the attackers, the attackers saw the patch coming in and we're like, no, absolutely not. And just like modified it, right? Like, or there's no way to load it. Like if you go to like put in the firmware, it tells you that it got updated, but it didn't. Like it's stuff, just all kinds of bullshit there.

Ryan Naraine (49:43.694)
It's something man, it's something.

Ryan Naraine (49:48.782)
It's possible.

Ryan Naraine (49:57.301)
It's possible.

Speaking of firmware, want to pivot quickly to our new report out of our friends at Biner. They actually met these guys at the reverse conference in Orlando, Takahiro and Fabio on a pretty deep technical report on their introduction of a new method for detecting UEFI bootkits, analyzing unique code behaviors. Costin, you got a read of the report. What is the big takeaway here? What is the?

COSTIN (50:27.513)
I thought it was a very interesting report and I think it's a kind of cooperation between multiple researchers. I think they mentioned Aleksandr Milankovsky, correct? Correct, correct.

Ryan Naraine (50:36.942)
Yeah, I saw your boy, Alexander Milenkovsky. Got a shout out, yeah.

JAGS (50:41.327)
Yep. Brian Baskin and a few, some of the ESET folks as well.

Ryan Naraine (50:45.966)
Mm-hmm.

COSTIN (50:46.561)

So as I think you said played an important role here because they ran the the other rules that the team developed to to find these new UFI boot kits I thought that this research It seemed very similar to the one that I did I think around 2018-19 when I was trying to find UFI implants not necessarily root kits or boot kits, but just like generic UFI implants, I think

I presented about it a bit at SAS in Singapore, but also at Blue Hat in Israel. And I think that this is a fascinating field. More people could probably look into this because they're... Absolutely, there must be. And like, again, just by looking at the various hints that dropped over the years, looking into those and...

Ryan Naraine (51:28.984)
There's a lot of stuff happening, right? That we just don't know about.

COSTIN (51:42.827)
left and right documents dropped by your favorite leaker or from your favorite three letters agency, you will see that the capabilities to target UFI existed for a very, very long time. And people actually, I've seen people put experience in developing UFI implants into their CVs. So I think that they're probably

deserves more attention I thought was super interesting so I was like you know going like where's the Yara rules give me the Yara rules so can run them on my collection and then I discovered that the Yara rules are not public so I think not or I don't know how

Ryan Naraine (52:25.758)
they didn't release the ARROR rules. How does that help you?

JAGS (52:29.113)
think you can ask them for it though. can, like in this particular case, yeah.

COSTIN (52:31.801)
Can I ask them now? Can I ask now? Can you guys share the other rules with me at least? Thank you. I mean, I would love to run them. I would use them to hunt them on my repository of firmware images. I have a repository of images that I collected over the years from all sorts of different sources.

Ryan Naraine (52:36.45)
Ask on the podcast, they're listening.

JAGS (52:37.829)
Yeah, yeah. Russia, if you're listening.

Ryan Naraine (52:41.73)
What does the Yaro rules help you do?

COSTIN (52:56.959)
So I did that for the research that I showed back in the days. I think I unpacked and parsed about 50,000 firmware images looking for interesting things. And I'd love to see how these Yara rules can potentially find more stuff. I'd love to play with them.

Ryan Naraine (53:20.322)
And the paper is like, have to go beyond existing detection mechanisms using all kinds of different ruling. the paper introduces like discussed about advanced static analysis, semantic detection, ML based clustering techniques. And it's like, it's an introduction of new ways and new ideas for us to go hunting for these things. Juanito, is this something that interests your lab? Like when you guys think about UEFI based boot kit, UEFI boot kits and so on, is this top of mind for you to be able to detect these things?

COSTIN (53:30.467)
Mm-hmm.

JAGS (53:49.55)
Yeah, I look, I personally think this is an area that's getting sort of like tragically under explored and under. It's not it's just not as big a concern as it should be considering that this is one of like the main roots of trust that you're relying on for every other technology like security technology that comes on top. Right. Like there's you're basically saying like this is the

Ryan Naraine (53:59.318)
Invest it just generally.

JAGS (54:18.883)
This is the belief that the ground you set foot on when you get out of bed is solid, right? Like that is, it's just like some foundational root of trust that you need. And of course, some of the higher end folks from some of the three letter agencies have been so, of course they've been invested into UEFI and into like, because what a wonderful way to have persistence beyond even like reinstalling the OS.

to be able to get in from under any security solution no matter what without necessarily being detected. And that's just the kind of technology that requires a certain level of specialization that I would put beyond your average nation state attacker, but that is worth the investment for a truly high end attacker to say, like the gains are so fucking massive. We're gonna persist on these systems forever. We are gonna be able to like undercut any security solution.

And coming from a security solution maintainer, it's something that you're concerned about at all times. There's a reason rootkits and bootkits were always the thing that you worried about because at that point it was a fight for altitude. Who has the greatest altitude in the operating system such that you can trust that the AV or the EDR or the XDR or whatever the fuck you want to call it.

is the thing that has the greatest view visibility and is not under the shadow of a rootkit or a bootkit that is feeding it misinformation or that can shut it down. That's the biggest problem for us, right? Like for any EDR vendor, your biggest concern is something unhooking you, tampering with your detection, removing you, shutting you down, uninstalling you.

And that is the biggest issue for anyone that, and honestly, it's why it's so fucking naive for people who want to create new security solutions. And they say, we're going to build an agent. We're going to build a brand new agent. You're like, bro, you do not understand like how much work goes into just keeping this thing alive, stable, having it not intrude or fuck with people's normal workflows, not take up too much processing power.

JAGS (56:43.269)
not be slow, still be compatible, be compatible after Microsoft decides that like they switched to this new rolling update basis. Now like shit gets changed within Windows 10 and 11 like every three to six months in undocumented ways sometimes. And you still have to maintain this product that isn't shutting the computer down or fucking with people's work, but can't be shut down or fucked with by some other thing.

that suddenly has greater altitude. Again, that's why people were so pissed off about these Microsoft signed, you know, pieces of malware, Microsoft signed rootkits making a comeback because of the new shift in their signing mechanisms. But overall, this is like one of the unexplored areas that we just, a lot of folks in the industry like to pretend is just not a factor. Like we basically put it as our version of out of scope.

because considering it is such a headache and such a potentially catastrophic situation for detection that nobody wants to think about it.

Ryan Naraine (57:50.082)
And now we're relying on smaller third party companies. Kostin, why have more anti-malware vendors invested in doing these level of detection? Shout out to the ESET guys, because they are pretty prominent out front with some of these discoveries.

COSTIN (57:59.065)
Hmm.

JAGS (58:00.121)
Yeah, they've invested into it.

COSTIN (58:04.141)
I think it's a question also of return on investment. I mean, this is quite difficult to achieve in a reliable way. And I know because I've been pushing back on my old job for us to have this capability in our scanner and implementing it in a reliable way, given how many different chipsets there are out there like Intel, AMD motherboards.

older Intel chipsets so doing this in a way that works let's say on as many platforms as possible and then it's stable and you don't crash the operating system is kind of a work of art if you want so I think one of the reasons this is not maybe more popular is because it's very difficult to implement so it requires a huge initial investment and then you run it for years and you don't find anything

And I think that one of the reasons that you don't find anything is because people don't know how these threats look like so Like all your heuristics if you want which are based on code emulation like a behavior blocking even signatures They don't work very well for malware that is designed to to operate at that level

So you need to build different kind of heuristics pretty much what they're talking about in this paper and what I was talking in my own research years ago. You need to develop a different class of heuristics looking for other kind of hints. And again, this is difficult because the amount of publicly available rootkits is just half a dozen. It's just a handful of bootkits, UFI bootkits out there.

Still people don't know how this look like every now and then yes ESET or Kaspersky or others They just find another one in the wild that was used by I don't know ghost emperor or like another APT group but in general these are quite rare and honestly, think that There has to be even more advanced things out there such as SMM rootkits like system management mode rootkits

JAGS (01:00:16.939)
for sure.

COSTIN (01:00:21.401)
which I think that people like the author of black energy was discussing like the Kind of things that Lisa was talking about in the past these have to exist in the world and the problem is that your Even your ring zero antivirus Solution will not find them. You will not be able to catch them. So it's still a question mark How do you go about finding those things in the negative rings?

minus one, minus three and so on, like hypervisor rootkits and system management rootkits or even other kind of hidden places rootkits.

Ryan Naraine (01:01:00.974)
One of the things they mentioned was that even Yara has a limitation, Like even the best possible use of Yara still is somewhat limited. Can you explain that a little bit?

COSTIN (01:01:04.707)
Correct.

COSTIN (01:01:10.157)

Yeah, in the sense that after all, Yara allows you to put kind of certain ideas into a semi-programming language designed to catch traditional malware. And this is what it is about. in hunting for UFI rootkits, sometimes you need to take into account the fact that you're dealing with an ecosystem, like a collection of files. And Yara by...

you know, by the way it was implemented, it works with one file or one block of data that it scans. But in some cases, you need to look across multiple files at the same time and like put them together and correlate them in order to say, yeah, what's happening here is suspicious because there's like this.

a strange bitmap file that potentially has a buffer overflowed which triggers some encrypted shellcode that you wouldn't otherwise get to unless you trigger the vulnerability into the bitmap. So this is what they mean by the fact that even Yara has limitations and for this it's almost like looking at an entire new computer or an entire new file system that

you need to analyze as a whole and every single like individual file from that file system alone by itself might not be sufficient to trigger your heuristics.

Ryan Naraine (01:02:43.212)
So it's Yarrow plus some additional kind of custom rules creation and some like embedded intellectual knowledge of things. The context, right.

COSTIN (01:02:49.715)
and the context.

JAGS (01:02:50.533)
but

Yeah, think that certain amount of like, I think the issue, the limitations with Yara really come in just on virtue of most of the time Yara is being run on files on disk, maybe in memory, depending in what kind of context they're being deployed. Like I love, like Joe Sandbox is something that I admire in large part.

because of implementations of things like this where they're like, yeah, we'll run your YAR rules in memory while the thing is running. But even there, you're basically saying like, we're either looking at a file as it is laid out on disk with its features discernible on disk or as it's laid out in memory with its features in memory. But you're still not talking about the kind of like behavioral.

things that you can do when you hook into a system that understands what those code blocks are supposed to do, how they're following each other, what the control flow of the program is. Like there is, there's still a way in which Yara, I'm not saying it's stuck at the metadata level, it's one level past that, but it's still not an understanding of how that code plays itself out.

self-modifies, how it feeds into itself, how it recurses, it flows in execution. And for something as specialized as UEFI, you like, look, credit to Binerly, right? Like the reason the guys are doing this research at Binerly and they have firmware hunt and stuff is because Binerly has built a whole fucking platform to instrument how these things work and be able to like, and you have massive gains from that. Because if you do understand it and you can process it that way, that means that you,

JAGS (01:04:42.457)
have a much easier time saying, this is the chain of logic that means that something bad is happening. And you can go and sort of process that elsewhere, but Yara is not going to be able to do that for you.

Ryan Naraine (01:04:55.246)
All right, so what's the next steps? Folks just trying to advance this research, get some happy hunting going. Maybe the guys share some Yara rules so that additional people can go hunting. I saw them mention they found some variants of certain things with very poor detections on VT, which suggests that you can go hunting their stuff on VT, right, Costin?

COSTIN (01:05:15.865)
I mean, yeah, I still think that nowadays if you want to inspect your own computer like the UFI neural computer, it's not a very straightforward process. Yeah, sure, you can essentially find all the open source free software to do that. You can find it on GitHub, but it's not kind of straightforward.

I still think would be nice if somebody created a tool that you can just download the run it on your computer it automatically dumps your firmware using let's say the API's and support for multiple platforms it offers to upload it to Firestotal it offers to upload it to

Our friends at BinerLit offers to upload it to our friend Roger Thompson who used to run a website to scan your firmware and so on and so on. So I still think there's a kind of high entry level. It's not straightforward to do that. And I mean, even keep in mind the fact that not everyone runs on just one operating system, Windows, whatever, but there's people out there with the Macs, with the Linux systems.

and so on and so on yeah exactly it's super hard

JAGS (01:06:31.811)
the complexities that come with fetching firmware in all of those types of devices.

I think that that area at the risk of sounding like a little too executive-y, I think the big issue you have with the firmware space is a combination of like accessibility in the way that Cosen is describing and a lack of appropriate awareness and prioritization, which is to say from an expert standpoint, it is absolutely obvious that this is an extremely important area of our security foundation and that any threat that exists there unnoticed, not the fact that there are threats, but the fact that we are not aware of the integrity and security of that space, which is something that gets dismissed very quickly, right? Whenever one of these UEFI bootkits,

you know, shows up like ESET finds a thing. Someone like Dave Weston will come out and say, yeah, but that's from like an old version of like, that's not, that doesn't include a secure boot. That's from like an old thing. And I'm like, yeah, but they found it now and it's been around for eight years and nobody noticed that it was there. So like, I don't give a fuck that there's a new piece of technology that means that that wouldn't work in certain versions. I mind that there have been

50,000 computers that had this in it and none of us could tell because none of our tech is actually engineered in a way where it's checking for that integrity. But that really shows the bigger problem firmware has and it's the uphill battle that Binerly has as a company that's a hard tech company trying to solve this problem, which is there is a weird self-reinforcing loop of ignorance in security products, which says,

JAGS (01:08:32.537)
this is gonna take effort, why should we invest the effort into solving this problem? And you go, well, because it's a big security problem that will undermine the security of everything else. And they go, well, but we haven't seen any of those threats. And you go, well, you haven't seen it because you haven't put the effort into seeing it. And then you go, look, here's an example of a threat. And they go, yeah, but it's just one. And you go, yes, but that's...

Ryan Naraine (01:08:51.113)
Looking, yeah.

JAGS (01:09:00.309)
But here's the example and they go, maybe there were more customers haven't asked for this and you go because they they don't know that they need this and you go, it's a lot of effort and it's like a weird little fucking ignorance loop. It's like a PM problem that is constantly right. Like why would we prioritize this problem, etc. But I think what we need to see and what binary needs to solve in a way is finding that kind of

that way to lower the initial friction into getting more data and showing and creating more awareness more regularly, like tying into other things, tying into how the OS is worked, tying into, let's say these like bullshit appliances, like all these different ways, just finding some way to making it just a little smoother for information to come in and awareness to come out, because right now you're in that

early stage of awareness for a problem kind of akin to when the antiviruses in the late 90s early 2000s were still dealing with that narrative of like viruses aren't really real. Antivirus companies make viruses. They're creating a problem for which they're trying to sell a cure. But like who the fuck is actually dealing with computer viruses? And like now that sounds insane. It sounds completely bat shit crazy. But that was a thing.

that was being argued well into like the mid 2000s, right? Like Rob, what was his name? Rob Rosenberg was like a big figure in that whole like, you guys are just making this shit up. You're like, okay, thanks bro. And like, look, that was a part of the evolution of our awareness of that problem. UEFI and memory threats and GPU threats are things that are still well within that realm of like, we know it's possible. We know, we've seen examples of

Ryan Naraine (01:10:25.71)
Mm-hmm.

JAGS (01:10:52.855)
a lot of these things, not all of them, but a lot of them. We have seen documentation that tells us that the big boys have been playing in that space for a long time. And every once in a while we catch a glimpse of a thing, go, whoa, look at what's been out there. But then we all just go right back to business as usual and go, eh, it's kind of out of scope. There you go. So yeah, rickety foundations, bro.

COSTIN (01:11:13.815)
We go back to Juniper.

Ryan Naraine (01:11:17.998)
And reality is that a world of hurt is happening on the dare that nobody is capable of seeing, is looking for, and we are told that secure boot has solved it all when we get secure boot bypasses at every security conference anyway. Can we do a short segment quickly on magic money? Costian, there's a really fascinating story on a crypto trader who lost $215,000 in a MEV

JAGS (01:11:35.359)
not a short one. This one's good. This one's interesting.

Ryan Naraine (01:11:44.938)
sandwich attack on Uniswap. So let me read this for a second quickly. The Mev bot front-run the transaction, leaving the victim with 98 % losses in just eight seconds. The attack happened on Uniswap v3, USDC, USDT liquidity pool and highlights the dangers of maximum extractable value bots in these. Like, what is this gibberish? Like what, what the hell happened here?

JAGS (01:12:08.079)
Hahaha

COSTIN (01:12:11.737)
I'd love to hear Juan explain it because he said he previously read about this story and he loves his first ever as fascinating and I was thinking this reminds me of the 90s you know in which way

it reminds me of the 90s I don't know how popular these were outside but I mean in the in the Eastern Europe or even like Russia

JAGS (01:12:12.591)
This is your moment, Kostin. This is it.

Ryan Naraine (01:12:14.69)
Please.

Ryan Naraine (01:12:23.042)
and he's fascinated by it.

COSTIN (01:12:40.841)
Everyone kept their money in dollars. So whenever you needed like some cash, you'd go to an exchange, which was usually run by Arabs, Arabs, Israelis, you'd go and come here and go and change your dollars into Romanian lay into rubbles, lever, forints.

Ryan Naraine (01:12:48.056)
I'm be with you.

Ryan Naraine (01:12:56.12)
currency.

Ryan Naraine (01:13:00.984)
You remember us walking around the streets of Moscow looking for cambios to get cash in?

COSTIN (01:13:04.537)
Absolutely, absolutely. Something like this. was in in in Russian. So just to change your your dollars in this attack, it kind of reminds me of that because in a way it's so similar to changing money and you looking at the exchange rate, you see you look up and you see the exchange rate is like one dollar.

200 rubbles you say wow that's a fantastic exchange so you take your dollar out of your pocket and By the time you give it to the to the cashier The exchange rate is one dollar one rubble That's how it works that the guy takes your dollar He looks back into his safe and lo and behold where his safe used to have like I don't two million rubbles There's just one rubble left. That's it

Ryan Naraine (01:13:41.57)
The digits move.

Ryan Naraine (01:13:45.645)
you

COSTIN (01:13:59.449)

and he takes that rubble and it to you and he changes like the change rate is now again 1 $ 1rubble so all the people on the street who have rubbles they are like holy crap I can now change a rubble for a dollar so everyone is rushing back to change a rubble to dollars but lo and behold by the time everyone is queuing in front of the exchange the rate is again back 1 $ 200rubbles so what the hell just happened

Ryan Naraine (01:14:25.228)
and 20.

You've been sandwiched.

COSTIN (01:14:28.983)
So you've been you've been sandwiched. That's what happened. And this is I think how this attacks work. People like front run the exchanges. They empty the safe so that they create a temporary different exchange rate. You get your one rubble for one dollar and then they before other people can rush and exchange their worthless rubbles into dollars again.

You know, they just restore the exchange rate and you can do this, but I think there's a number of prerequisites. I mean, I I've been trying to do this not not in this manner because to do it like at this level of how it was done here. You need some kind of serious resources. So I think the best party you need to read from this story is that the attacker.

JAGS (01:15:18.213)
Mm-hmm.

COSTIN (01:15:23.497)
sent a $200,000 tip to the Ethereum block builder Bob the Builder to prioritize the malicious transaction and the attacker himself kept only $8,000 in profit this is like so typical of these attacks you spend to make a thousand and like who can afford that

Ryan Naraine (01:15:38.99)
You spend 200,000 to make 208,000 right there.

JAGS (01:15:44.218)
Well, yeah, that's that was the part I was hoping you understood or like had some insight into because I'm I can understand why you need somebody kind of ready to very quickly accept or validate your transaction, right? In the way that cryptocurrency works. And I can see why that person would expect a cut. But

200,000 to $8,000 and then saying that the person with the $8,000 is the attacker, but the $200,000 tip receiving is just like an innocent bystander. That right off the bat doesn't make a whole lot of sense to me. And note that like they're saying, like it seems like they're focusing on one attack, but they're saying that that same trader

COSTIN (01:16:22.775)
and Bob the Bill.

JAGS (01:16:41.797)
got screwed over like up to like 700 or something or 500,000, half a million dollars. So A, I feel like we're not seeing like we're not only are we seeing the tip of the iceberg, but I think we're mischaracterizing its shape and its nature. like I think to me as an ignorant bystander, I...

COSTIN (01:16:41.879)
lost half a million half a million half a million

JAGS (01:17:09.365)
I just don't feel like I'm getting the whole story here. B, like they mentioned that this might possibly be a form of like money laundering, would make more, at least it would make a bit more sense. You're saying, we don't mind these losses at all because right, like they're actually, you know, illegal, trans, like we're taking illicit funds and we're somehow washing them and.

And then you get all kinds of advantages, right? The person quote unquote losing money gets to report losses, which means they offset taxes. And the other person that's quote unquote making the money gets to have these like cleaned bills in a way. I still don't think I, A, I don't think I get it. B, I...

I also am immediately reminded of like the flash crashes and dark markets of like earlier stock trading, like high frequency stock trading that you do.

COSTIN (01:18:05.017)
It's the same,

Ryan Naraine (01:18:05.72)
This is what it brought back. Yeah. This is the memory it brought back. This HFT thing that was documented in the book because there's a fascinating story in Forbes on these MEV crews. Apparently it's not illegal either to be doing this kind of front running, get in and getting the price. Exactly.

JAGS (01:18:20.271)
Can't be illegal when there's no regulation and laws nothing like

COSTIN (01:18:24.121)
Why would it be illegal?

JAGS (01:18:26.533)
You

Ryan Naraine (01:18:26.67)

But there are like crews of guys who do this and they target each other as well. it is.

COSTIN (01:18:29.593)
That's awesome It's like the the Olympics right they were saying this is like the Olympics like my mathematician team here We have like a Greek mathematicians Russians, Romanians, Hungarians everybody's like fighting the other MEV team with their mathematicians and like we're Mathcocaine and DDoS. Yeah to DDoS the other MEV bots so that we get to

JAGS (01:18:33.445)
Be illegal, guys.

JAGS (01:18:49.923)
Math and Cocaine.

JAGS (01:18:55.845)
you

COSTIN (01:18:58.841)
rip off people faster than they can actually rip off our people.

JAGS (01:19:04.013)
Ryan, what was the Michael Lewis book? It's like flat. Was it flash flash boys? Yeah. Yeah. Nothing is new under the sun. It's the yeah.

Ryan Naraine (01:19:04.034)
I was just...

Flash boys,

Ryan Naraine (01:19:13.368)
I was just fascinated by the Forbes story. Part of it was like they actually created a loan, an abracadabra collateral for a loan denominated in quote unquote magic internet money. It's actually included. Like we made that up here on this podcast, started calling it magic money. It turns out that it's already part of that ecosystem. So I was wrong there. It also points out how much crime and fraud and malicious activity and kind of like the worst of the worst.

JAGS (01:19:32.345)
But some credit.

JAGS (01:19:40.257)
It's not crime. There's no laws. What's you know? It's not money.

COSTIN (01:19:40.957)

jungle it's a jungle I mean look if you let me put like you go into the jungle and you get eaten by a lion or a snake

Ryan Naraine (01:19:43.522)
There's no money, it's magic, right? How can you steal?

COSTIN (01:19:54.145)
Whose fault is it? The snake, the lion or yours?

JAGS (01:19:54.213)
Go on.

JAGS (01:19:58.412)
It depends, man. If you go into if you think you're going to the jungle and it's Jurassic Park, there is some version of liability. Right. You thought you were going into an amusement park and a fucking clone T-Rex shows up and eats your children. There's usually some discussions of liability. Dude, it is insane. Like it is insane. Like, look, here's the thing that matters. And this is where like the joking turns less funny.

which is the reason we cared about dark markets and flash markets and high frequency trading is they were fucking around. And when finding out phase came, it was like a huge economic disaster that like rocked portions of the economy in ways that were completely unpredictable and unprecedented because you had money being moved around and

insane automated ways and failing in unexpected but massive rippling effects. And that's a discussion we had I think last episode or the episode before where I'm like, who the fuck are these people that can afford to lose $1.5 billion here and $700 million over there and like no problem.

Ryan Naraine (01:21:09.933)
and just blink.

JAGS (01:21:14.565)
No, no issue. They just get up, dust themselves off and move on. We don't even find out who who who who are these fucking people that are losing all this money and don't feel it. And I think we are still in the fuck around phase the same way we were with like CDOs back in 2005. And we haven't we're soon going to reach the find out phase where you go, oh, somewhere in this trillion dollar magic money, crazy mania.

Bullshit phase of robots attacking robots. We actually decimated I don't know however many six hundred billion dollars worth of the economy got shifted around from one place to another Without us accounting for it and next thing, you know, people can't buy Houses or like fucking eggs cost thirteen dollars. I don't know right like shit starts to happen that that we don't know how to account for Yeah, I heard about this. I don't I didn't realize how few eggs I ate

Ryan Naraine (01:22:08.598)
Eggs are expensive.

Ryan Naraine (01:22:14.158)
I want to read the money quote from this Forbes article and I'll put the link in the show description here. It's like they're talking about these two MEV crews and these crews who are going in front running ahead of each other and like mouthing against each other. And one of the guys says, you might be friends with people, but at the end of the day, you're all just trying to bankrupt each other. It feels like that's just such a perfect summation of what this magic money ecosystem looks like. It's just fascinating.

JAGS (01:22:26.917)
fucking nerds.

JAGS (01:22:38.787)
It just do, but it's what I love. What I do love about the magic money ecosystem is that it shows you the depravity of investment bros that you don't get to see because their casinos are like skyscrapers. like you don't get to, if you have hung out with, used to host investment banking movie night at St. Andrews back in the day. And it was cause I loved hanging out with the sociopaths that go into investment banking.

and like seeing the true frothing at the mouth that comes with taking someone's money, making it your own and trying to keep somebody else from taking your money. And like, it's all numbers, right? And you could tell the people who thought they were going into it because it was a career where they were gonna make good money and it was a stable source of income. All of those people flame out of investment banking within six months or a year. They can't stand it.

But the sociopaths, those fucking people, like that is their environment. And it's just like &A and all this shit. You're like just moving money around, crashing things, fucking people over and making money hand over fist with no explanation for where that money came from. Those people thrive. And you can see it naked in the cryptocurrency space. Because no one cares if it's an obvious rug pull. Nobody cares if it's obvious fraud. Nobody cares.

If it makes no sense, it's just a vehicle for moving numbers around. And if you're smarter and take money, awesome. And if you're dumb and you lose it, well, fuck you, right? Like it's, it's just naked.

Ryan Naraine (01:24:11.79)
Kostin, why are you having him go at you like this? This is your world, buddy.

COSTIN (01:24:16.313)
I don't see it like this is not coming at me like I just wanted to to ask you a simple question Do you guys watch UFC? A little bit. Yeah, it's it's fun, right? It's like it's still fun even if people are

blowing their teeth out and like bleeding and kicking the shit out of them, right? This is no different from UFC. This is like UFC for math nerds and sociopaths and yeah Greek mathematicians

JAGS (01:24:19.673)
No, no.

JAGS (01:24:25.093)
a little bit.

Ryan Naraine (01:24:39.266)
You

Ryan Naraine (01:24:42.53)
Rich Creeper.

Ryan Naraine (01:24:47.244)
Any

JAGS (01:24:47.424)
Noooo

COSTIN (01:24:47.498)
It's the same thing.

Ryan Naraine (01:24:49.974)
Listen, if you're playing with magic money again, you need to be putting your wallet, your laptop in a safe somewhere, right? Like this. How do you protect against something like this?

JAGS (01:24:50.149)
I don't know. I don't-

COSTIN (01:24:59.513)
You

So one of the reasons why this attack worked is that because the trader was doing this on a Uniswap V3 exchange that was not the official Uniswap V3 exchange because the official Uniswap has a protection against malicious map bots. So in a way he kind of asked for it.

Ryan Naraine (01:25:15.822)
because of course.

you

Ryan Naraine (01:25:24.835)
He's playing in the mud and he doesn't want dirt on his shoes.

JAGS (01:25:26.553)
Some fucking gambler, bro.

COSTIN (01:25:27.897)
Like instead of exchanging your dollar for rubles at the bank, you went to the back street in Moscow and you thought you were gonna get 300 rubles for a dollar, but instead you got three rubles. And you could have gone to the bank, right? To the Bank of Russia on the main street and get 150 rubles, but no, you wanted the 300.

Ryan Naraine (01:25:42.414)
You get three rubbles for $300.

JAGS (01:25:43.365)
And a bunch of newspaper.

JAGS (01:25:53.808)
Dude, the fact that you're talking about rubbles makes this really hard to take seriously because those fucking things aren't worth the paper that they're printed on, right? Like, the paper is more expensive than the value of the rubble itself. But I take your point. Russia's making a strong comeback, guys. The rubble is gonna come back.

COSTIN (01:26:03.225)
I don't know.

You need to buy the dip. Buy the dip, look at the dynamics.

COSTIN (01:26:16.565)
I look if you know what's happening in the world if you look at what's happening in the world like the US stock market I don't know you're not so magic money into the Tesla stocks and the S &P 500 I don't know like suddenly magic money look very enticing and actually there's a very

JAGS (01:26:18.597)
It's gonna be the next Euro.

JAGS (01:26:29.103)
Oof. Tesla. Everything's computer.

Ryan Naraine (01:26:32.344)
George S. Kuhn.

COSTIN (01:26:42.965)

Interesting interview with Yanis Baroufakis who was the

JAGS (01:26:47.517)
I just listened to his book on the way up here. Techno-feudalism. Yeah, sorry, sorry.

COSTIN (01:26:50.061)
Here's the form. Okay. Very, very interesting guy who was the finance minister of Greece and he talks about Trump's new policies and what he thinks that Trump is trying to do with crashing the economy, devaluating the dollar so that he can buy back the US debt with magic money, with magic money that are not packed to the dollar.

I think that that's interesting because in a way this story that we're talking about someone was trying to swap USDT to USDC. So those are magic money which are packed to the dollar. One dollar is one USDT, a Tether USD. And this works as long as Tether, company behind them and Circle in the other case, they can guarantee and they say like, whenever you come to me with the magic

I'll give you a real dollar for it and We have a vault here that is full of real dollars so whenever we get a magic dollar from you we burn it and we give you the real dollar and This works as long they actually they have as many real dollars in the vault as magic dollars and Just imagine if somebody starts buying the US national debt with magic dollars

and there are not as many magic dollars as real dollars I think that's what Yanis was saying

JAGS (01:28:23.781)
I think our friend, Janis Varoufakis, maybe he wants to see a five-dimensional chess move and people are out here playing like, not checkers, like... are out here eating crayons and this motherfucking things that we're like watching five-dimensional chess happen.

COSTIN (01:28:41.462)
Backgammon. It's backgammon with dice.

JAGS (01:28:52.377)
That may, I would not look, there is a possibility, right? That like Tech Maga, the JD Vans, like Circle, the Peter Thiel and all of, know, Sachs and all these folks are playing this like insane game of 4D chess. And if the magic money somehow becomes a cheat code to removing our national debt, well, I'll fuck, I'll be the first one to build a gold statue of one of these motherfuckers outside of, you know, the White House.

Uh, I would be very surprised if that's the case. I'll be surprised if they had thought about it before Yannis Varoufakis said it, if they had even considered that as a possibility. Um, I, I am genuinely terrified by the eventual follow on effects of what's happening in crypto. I like the, what people don't understand is that we have effectively been playing with virtual money.

for like 30 years or so, maybe more, where banks were starting to effectively play with money that isn't even in circulation. It's just virtual money in between these massive banks and you have these giant like exchanges and notes between them. And that's why we had to have all these attempts at like regulation of banks where you go, hey, you can't just make up.

all of this money, you have to have a certain amount of reserves that match this, because otherwise, like you're playing the role of the Fed by like creating all this virtual value. And you've had the sociopaths in Wall Street, like trying to find different unregulated vehicles to play out their gambling addictions in some way or another. And frankly, we, know, the U.S. consumer and a lot of the world gained value from that, because that's what allowed us to do a lot of like,

refinancing of mortgages and getting all kinds of investment capital and all sorts of great shit. However, we have seen that when you detach the global economy from any indicators of health and any real world indicators of value, not only do you get these massive opportunities for fraud and bullshit and bad decision making and like, essentially like,

JAGS (01:31:09.527)
It's not being like asleep at the wheel. It's like someone being blackout drunk at the wheel driving the entire global economy. We get situations like 2008 and that still was tethered to something that had a regulatory basis. But like we weren't really paying attention the way we should have. What is happening here? What is happening in a trillion dollar crypto market of unregulated shit? Just

just swishing around in a way that we can't immediately feel. Because like what I'm worried about is like you're just that is a whole system that is built around overreach and like survival of the smartest, the fittest, the, you know, most coked out. And when they inevitably lose because someone has to lose and someone has to win in a game where you're all just out to bankrupt each other.

How does that, what happens when the bill comes due? Like what happens when somebody goes to make one of these ridiculous transactions and they realize that like there's no money coming from the other side anymore or like things don't quite work the way they expected to and the bill comes due for everybody else.

COSTIN (01:32:30.145)
I tell you what happens, it happens the magic Tuesday or the magic Monday. It's not the black Monday, it's a magic Monday.

JAGS (01:32:37.689)
Magic Monday.

Crypto Month.

Ryan Naraine (01:32:42.094)

While you guys think about your shoutouts to close this show, just wanted to flag this quick story. A pretty shitty story about what's happening to Reuters journalist Rafael Satter. We all know Rafael, he's been covering this industry for years. Good guy. He's a US journalist that had his Indian government citizenship taken away. What's the story? Rafael, who covers cybersecurity for Reuters in the US, received a letter from India's Ministry of Home Affairs in early December, accusing him of producing work that maliciously targ-

maliciously tarnished India's reputation and informing him that his overseas citizenship of India card has been cancelled. means he's no longer able to travel to India where members of his family live. This is related to the Appian thing. Pretty crappy that a journalist writing about this stuff gets really caught up in accusations of maliciously tarnishing folks and affecting his everyday life. We talked about this in the past about how

Threat researchers, journalists and so on approach these things when they are real life ramifications for.

that usually come down the pike. Does this make you nervous, Juanito?

JAGS (01:33:50.478)
I I don't know about nervous. We were at the center of this with Reuters, right? Like Tom Hagel from my team was doing the follow-up research with the Reuters guys. Our story got taken down also because we received a cease and desist letter from some white shoe law firm representing Rajit Kare. So we've been in it with Reuters to some extent. And yeah, I mean, look, this is a...

And I do not want to minimize the effects on Raphael, because I think that's an important human dimension that is being shown here. It is a, it is a even bigger problem than what is being described here, because this is the equivalent of like a slap suit serving as a form of

unprecedented censorship. I Reuters hasn't had to take down a story. I think it was in like 70 years or something like that. And they had to take the story down for like 10 months because they were being harangued in Indian courts over like, and it's the typical bullshit of like, you get sued and then they don't show up and then they sue you again. And then, you know, there's a claim, but it gets not unsubstantiated and then a different judge gets put in and then whatever. It's like,

Ryan Naraine (01:35:04.974)
It is drugged, see ya.

Ryan Naraine (01:35:10.392)
That's the point of it, right?

JAGS (01:35:11.627)

That's the whole point is 10 months of faffing around for this like billionaire douchebag to pretend that like he's a, I don't know, some like yoga guru now, instead of like having started this company that is well, yeah, it's well fucking documented to have been doing hack for hire. And what Reuters got their hands on was like a lot of original sourcing that not just showed that it was hacked for hire.

Ryan Naraine (01:35:23.896)
Are you gonna get this podcast banned?

JAGS (01:35:36.954)
but that it was interfering with legal cases in Switzerland and the United States. Like there has been actual real world fallout of all these operations. And we've just kind of like been like, whatever bro, like let it, let this shit happen. And in the meantime, what we're seeing are essentially look, what really concerns me about this Raphael situation is I don't mind there being some D bag.

tech bro who's made way too much money doing bad shit who is pissy and wants to find a way to not get

Ryan Naraine (01:36:13.336)
Clearly very powerful and influential too if you can get citizenship revoked.

JAGS (01:36:17.197)
That's my point. And that's where you get like, look, before we were playing in the realm of like, slap suits and like just flashing your money around to try to rewrite history. But now we're talking about them having influence at the level of like the world's largest democracy, apparently, and being able to influence, you know, citizenship decisions and God knows what else. And that is where you...

Ryan Naraine (01:36:43.34)
And not in the background either, but documented that you're maliciously tarnishing the country's reputation, which means it's overt,

JAGS (01:36:48.697)
Yeah, right. like, so there is a sense of the equivalence of right, like it's kind of it's fascinating because essentially the Indian government is tying their reputation to what these companies are doing. And that's where you go, whoa, wait a minute, man. Like there's a lot more to India and it being an actual legitimate important contributor to the global economy and a respectable nation. And when you do shit like this,

Ryan Naraine (01:37:05.548)
Yeah, what's... yeah, so silly,

JAGS (01:37:17.657)

The only person tarnishing the reputation of India as a country is whomever the fuck thinks that it's appropriate to enforce this. you know, shout out to Rafael. He's been like, his integrity has been paramount in all of this. I've gotten to watch how some of the sausages made and, know, him, Chris Bing and some of the other folks involved like have put on real work. And at no point have I seen them act with anything less than like.

complete integrity and devotion to the story, even as things like got pretty hairy for everybody involved. And I hope situation gets better. even for everybody involved, even for the sake of just looking at India as a responsible player in the stage and not just some like bullshit, two bit oligarchy. Yeah, like what the, this is beneath a country like that.

Ryan Naraine (01:38:03.426)
Rogue Nation doing a...

Ryan Naraine (01:38:08.43)
Kostin, have some thoughts on this story at all?

COSTIN (01:38:11.673)
Yeah, it's what can I say it's very it's very sad and worrying and Again, I I don't think that there was anything Wrong in the stories that Raphael they were like very thorough very well written Everything was pristine. Everything was beyond any kind of doubt So not only that but I don't think that at any point when what they're saying is that

he operated without a journalist license or something like this. mean, come on, let's let's be serious. None of that holds water if you want. So I hope that, yeah, I saw there's currently Rafael's lawyers are appealing this decision and there's a very good chance it might be overturned.

Ryan Naraine (01:38:44.558)
Nonsense.

COSTIN (01:39:01.591)
So I hope that that is the case and I couldn't think if the US government shouldn't maybe play a more active role in this story and the reason is that for instance for the Binance exec who was jailed in Nigeria if you know the story just to draw parallel with the magic money the US government intervened and got him out of there essentially helping him and I

Ryan Naraine (01:39:27.022)
Was it Binance or Coinbase? This is the guy who was arrested in Nigeria that Andy Greenberg had been covering and writing closely about, right? Yeah.

COSTIN (01:39:29.645)
Binance, Binance, yeah.

Nigeria.

Exactly, correct, correct. So just imagine Andy Greenberg simply maybe getting a similar treatment because of the stories that he was writing. So I think, you know, that journalists should be protected, that maybe states should care more and governments should get involved more to protect journalists and to take their sides if you want. And that's why I think that that story with Tigran was a nice

a nice, if you want, conclusion.

Ryan Naraine (01:40:11.106)
Yeah, he was released and I think he's backstage side now. Some closing shout outs, Juanito, I'll start with you. Anybody you want to give some shout outs to quickly?

COSTIN (01:40:13.507)
Just back in the states, yeah.

JAGS (01:40:21.989)
that's a good question. I don't know. You ask me this every week and I never prepare for it. Like I never think it through before the time.

Ryan Naraine (01:40:27.042)
Yeah. This is the part of the show where you get to do free plugs for anything you like, anybody you see, any bit of work you've done. Don't make it anything. It shouldn't be too hard.

JAGS (01:40:34.597)
that you're right.

Yeah, I don't know, man. I want to see where things are going from here with all this AI shit. The discussions that we're having about models and stuff, they are sideshows. Technological development is about pushing that boundary forward. I think OpenAI needs to focus on being the...

COSTIN (01:40:38.681)
You

JAGS (01:41:04.661)
ringleader being the the organization that is pushing the boundaries of what is considered possible and and continuing to move that forward rather than playing this bullshit shell game of like trying to get this or that banned yeah they can love

Ryan Naraine (01:41:20.014)
Sir, this is the shout out section. This is not the shell for open AI again.

JAGS (01:41:23.499)
No, my point is to hype them up at doing what they do well. I love their tech. I love what they do. I want to see deep research get better. I want to see more consumer stuff come out. I love that shit. They're doing great work on that front. Focus on that front. And then to everybody else, all of, you know, we actually said we don't want to talk about CESA for too long. We didn't talk about CESA at all. You know, well.

Ryan Naraine (01:41:46.04)
did not do it at all. We'll catch CESA next week. There's a lot of turmoil and a lot of leadership changes and fire rings and not fire rings and red team made laid off and red team wasn't laid off. A lot to get to. We'll get to it next week.

JAGS (01:41:55.545)
Yeah. Well, I think it's not I don't even want to talk about it. I'm just saying like, you know, you have new leadership. It's hopefully.

Ryan Naraine (01:42:02.67)
Hey, this is the US government cyber security agency. should pay attention to what's happening there.

JAGS (01:42:06.949)
Well, yeah, but the whole point of it being like there's new leadership. Congratulations to Sean Planky. It's a new dawn. Show us what your administration is going to be. Tell us what your priorities are. Put your money where your mouth is. And like, I look forward to it, right? Like we're not going to just dismiss that organization out of hand without knowing what it stands for and what it's trying to accomplish. And, you know, we have a vested interest in them succeeding to some capacity, right?

Ryan Naraine (01:42:17.976)
Good one.

Ryan Naraine (01:42:32.11)
Gustin, before I get to you quickly Juanito, let me tee up another shout out for you is LabsCon. Starting to get some folks asking about invites and obviously the next step is call for papers. Any idea when are you starting to ramp up? I see the Twitter account is starting to be active again. It feels like there's some LabsCon energy happening.

JAGS (01:42:49.763)
Yeah. Well, we're getting there, right? think within the next in about a month, we'll probably open the CFP that usually comes hand in hand with us opening the invites, usually to the alum first to try to, you we'll do about half of the invites. We push to the alums first and then we kind of start opening things up little by little. Super excited for this to kind of come around. We are keeping it as tight as it was the year before, which is to say.

You're still looking at about 150, 160 people, including the speakers. So there is a certain level of, you know, I'm not going to say exclusivity as much as self-selection that goes into it. There's room for new folks. We always want to see new great folks as long as they fit into the spirit of the con. And I'm looking forward to see what people bring out. Like for me, the most exciting part is that scary tentative energy.

before and during the CFP where people are trying to figure out like what's a good enough project? What's research that it's not even that meets the bar of the CFP? But even if you get accepted What's a topic that's gonna have lasting value from June all the way to late September, right? So there's a sort of it encourages a certain kind of strategic thinking that I think

Ryan Naraine (01:44:04.323)
Right.

JAGS (01:44:10.351)
tends to be very well rewarded considering the kind of awesome research that we get. So I'm looking forward to seeing what people come up

Ryan Naraine (01:44:16.814)
And the same vein, just quickly a shout out to Kristin Del Rosso and the folks who are planning ChinaCon. I know they've been pushing for folks to submit to their call for papers. Their conference is in September and the call for papers closes on May 31st. So there's like a big giant window in there where there's like an element of staleness, an element of something being lost, something being announced and so on. It's like a tricky, tricky dynamic to manage.

Shout out to those folks and good luck to all those conferences, including PivotCon that's coming up. And Kostin, you get to close the show. Give me some shout outs.

COSTIN (01:44:47.033)
Alright, I'm like Juan, I never think in advance but since we talked about the administration's 4D chess with saving the US national debt I simply can't not mention this chess news Hans Nieman that maybe you've heard his name before is a chess player that has been accused of cheating with all sorts of weird devices

JAGS (01:45:14.039)
Wait, wait, wait, is this the butt plug? Is this the butt plug thing at chess?

Ryan Naraine (01:45:15.128)
just got more drama than anything else.

COSTIN (01:45:16.895)
It is the but it is yes it is so has Neiman after that incident basically nobody wants to invite him to chess tournaments anymore so now he's playing in Russia and in Russia

JAGS (01:45:29.219)
As one does, when one's career goes poorly, one plays in Russia.

COSTIN (01:45:33.049)
He posted photos from from the Red Square and in Russia I actually played 18 games against Daniel Dubov with a fantastic extraordinary strong Russian Grandmaster very young Who's just amazing not just in chess, but I saw him for isn't doing pull-ups with one hand just one hand pull-ups And he played 18 games hasn't even played Daniel Dubov for 18 games and the loser

This is what they were playing on. The loser has to take a lie detector test. And Has Niemann lost one point. He lost one point to Daniel Dubov and now he needs to get a lie detector test where the other or the other guy, Daniel, can ask one question. everyone's everyone's excited like what the question will be. What will the question be?

Ryan Naraine (01:46:08.785)
Ha

Ryan Naraine (01:46:25.368)
This is exciting.

JAGS (01:46:29.733)
Dude, chess is getting sexy out here. Like these dudes are finding ways to like actually make it interesting.

Ryan Naraine (01:46:31.982)
Dude, every month there's a new cheating scandal and there's people wearing the wrong shoes and the wrong jeans. It's like super crazy.

COSTIN (01:46:41.759)
Yeah, not only that, like one of the greatest stories that happened recently, Magnus Carlsen, possibly the greatest chess player of all times, he was playing in the finals of Blitz, Fide, Blitz Championship. And he was playing Jan Nepomniachik, which is a he's a Russian player and

They were playing in the final and at some point, you know, after a couple of draws, Magnus said, listen, like we can play like this forever where we can share the first place. Like, do you agree? Yes, I agree. So they went to Fide and said, like, we want, both of us want the gold medal. And Fide said, sure, like you can both have the gold medal. So just imagine like in UFC, like in the final, they said, hey, you want to fight? Nah, you want a gold medal? Yeah, let's share it.

We both won the gold medal, so there's a lot of funny things happening. if you, if like, this gets me back to my shout outs is to all the people in security and computer security playing chess, shout out to you. Have fun. Yeah. We need to organize a change a championship sometimes. Security chess part two.

Ryan Naraine (01:47:52.16)
a lot of them.

JAGS (01:47:57.231)
Secure HS again.

Ryan Naraine (01:48:00.802)
Thank you gentlemen, to all the CISO folks, we'll get to you next week.

JAGS (01:48:04.703)
god.

Ryan Naraine (01:48:06.062)
Good night.

JAGS (01:48:07.205)
It's everything's computer.

COSTIN (01:48:11.551)
Everything is computer. Wow.