Ep3: The Three Buddy Problem Podcast

Hosts: Ryan Naraine, Juan Andres Guerrero-Saade, Dave Aitel

** Costin Raiu is on vacation.*

Ryan Naraine (00:02.254)
Hello and welcome back to episode three of the Three Buddy Problem podcast. Costin Raiu is on vacation. I believe he's in Santorini having a glass of wine somewhere, but we have a guest host today. Dave, Aitel, CEO of Cordyceps Systems. Dave, how are you? Thank you for filling in today.

Dave Aitel (00:24.598)
Thank you for having me, looking forward to it.

Ryan Naraine (00:26.894)
It is Friday, July 5th, exactly 8:07AM. Juan is back in Miami after a trip to Recon. How are you Juan?

JAG-S (00:35.727)
I've got a little bit of conference flu or something. So I'm struggling a bit, but I'll manage.

Ryan Naraine (00:42.894)
How was the con? Can you spend a second on a quick wrap up of recon.

JAGS (00:47.535)
Man, I mean, I'm sad that you're asking because I'm going to tell you the truth and it's not good. Like I think a lot of us love recon as like the only reverse engineering focused conference in the space. And the organization around it has fallen into disrepair in a way that's like, it's almost like a, it's a slow death. Like to the point where I am a handful of other people had to.

Ryan Naraine (01:08.814)
visible.

JAGS (01:15.471)
run HDMI cables through the audience for the keynote to be able to speak because she had been standing on stage for 30 minutes, no slides, no microphone. Like it's not a good look. So I think a lot of us love the conference. I hope that somebody will buy it or stand in or make an alternative, but I don't know that in good conscience, I would tell people to like spend their money on it right now. Though the content is pretty unique to it.

Dave Aitel (01:43.094)

I know some people who are putting up an alternative, shall we say. So watch that space.

Ryan Naraine (01:43.246)
And div.

Ryan Naraine (01:49.55)
So there are talks about having some sort of replacement. Just before we started recording, you and I were talking about infiltrate and the gap that's been left behind by the more or less the disappearance of infiltrate since the acquisition. What is going on with that?

JAGS (01:49.551)
That'd be good to hear.

Dave Aitel (01:58.902)
There's

Dave Aitel (02:03.766)
Yeah, I think it's kind of a shame. You're not wrong. There's a gap and especially in the sort of domestic United States area. You know, a lot of us are going over to Germany for offensive con, which I think has been carrying the torch. But it's, you know, there's, there's a different crowd there. And I think there needs to be there needs to be an offensive focused conference here in the States as well. I don't know if Miami is still the right place to throw a conference. To be completely honest, I think you might want to move a little further north.

where it's not 1 million degrees and under threat of hurricanes, even in the middle of winter. So I think this is gonna space that's gonna continue to evolve. I think there's room for both of those things in the United States, like reverse engineering conference, which has a slightly different crowd, slightly different focus, and then an offensive conference.

Ryan Naraine (02:45.902)
Right.

Ryan Naraine (02:49.646)
Conference organizing is a full -time job though. Conference organizing is not easy in a lot of respects. It's kind of a voluntary thing where you throw a lot of time behind it. Juan and I are working on LabsCon. You talk about a place not being a million degrees will be a million degrees in September here in Arizona. But the point around these conferences, they peak and then they fade away because it's a lot of work, a lot of sustaining work over time.

Dave Aitel (03:15.478)
It is. We saw like T2 stopped this year. There've been some great conferences where they sort of just ran their course. Enigma, ShmooCon. The conference space is open and I think I did not get as much value out of some of the bigger Vegas cons as I wanted to last year. They're just

too oppressively huge and almost diverse, right? Like there's too much happening. I couldn't focus on anything, right? So...

Ryan Naraine (03:20.201)
Enigma died.

JAGS (03:21.839)
Shmoocon!

Dave Aitel (03:44.342)
I think we're going to see some movement in that space for sure.

JAGS (03:47.183)
I hope so. I mean, even look at what's happening with DEF CON, right? Like this year is going to be weird. Like it's just a weird venue. It very much feels like a convention now. It's not so much a conference as a convention space. And like you said, the sort of the conference space is open. Like I do think somebody has to, well, there's opportunity for folks who might want to try something different even during summer camp, because I don't think folks are quite as into what things have turned into.

Dave Aitel (03:57.494)
Yes.

Dave Aitel (04:15.894)
No, and honestly, the other truth of it is, is it's like, as you say, logistics is hard, getting the right people in the room is hard. But I'm looking forward to the next generation, to be honest, of these conferences. I think they're good. I think they're really valuable.

Ryan Naraine (04:30.574)
All right, enough about conferences. In fairness, there's sometimes too many conferences as well. Can we, I want to pivot to the news of the week. The biggest story this week is obviously the OpenSSH unauthenticated remote code execution vulnerability found by the guys at Qualys. Usually when you put those words together, it's the internet is on fire. She stopped everything and rushed the patch. In this case, there were some circumstances that made it not necessarily a big security risk. Dave, I want to pivot to you first.

Surprise to you that we're still seeing RCEs in OpenSSH.

Dave Aitel (05:06.39)
No, not at all. I mean, maybe if you thought that OpenSSH was secure, you'd be surprised just because something's been looked at a lot doesn't mean it's secure. It's still written in C, still a really dangerous piece of software to have on your system. Always going to be true. I don't know why it hasn't been rewritten in Rust. First one that people know about in a long time. Right? Like, so that's the thing about these things is like...

Ryan Naraine (05:26.286)
First one in a long time though.

JAGS (05:33.903)
Hahaha

Dave Aitel (05:37.682)
Like, I mean, there's a lot. All right. So here's one thing that I think is really, you said that there were like some things that made this not that interesting, which is true, right? Like people are like, well, right now we only have an exploit for 32 bit. You know, there's a lot of complicated stuff in here. I think the Qualys team tipped their hand a little bit with their, with their methodologies for how you go about exploiting remote race conditions in a systematic way. I just think the

public open source research is not as advanced as private research in that area.

JAGS (06:12.559)
So I'm glad to hear you say that because the exploit side of things is so far out of my wheelhouse and I just have kind of a fascination with it. But I have been a little disturbed by how comforted and comfortable we are with this idea that there's a regression. We know there's an exploit. We know there's somebody who's been actively exploiting it, but it's hard to exploit.

So it's unreliable, you're gonna need to hit this thing a thousand times before it works. So it's fine. And I'm like, to me, those are the conditions for what was discovered, sort of the canary in the coal mine. Now you've put every exploit dev out there who actually may be much better at this. You've let them know this thing is out there, it's sitting there.

you know, likely unpatched in many of these other places. You're telling me that there's no way to more reliably hit this thing. You're telling me that there's not a bunch of open SSH running systems that don't have ASLR turned on or like that there isn't an alternative for non 32 bit systems. Like I'm almost dismayed at the level of comfort that we've given ourselves so quickly and easily about this one.

Ryan Naraine (07:26.99)
No, I think what you're describing as comfort is just notes that widespread opportunistic exploitation is unlikely. I think that's the argument is it's not that you shouldn't stop and go look for things to patch or you shouldn't try to put your mitigations in place. It's that this is not going to be one of those warmable widespread things. Is that a fair assessment, Dave?

Dave Aitel (07:44.438)
I totally agree.

Dave Aitel (07:50.134)

I totally agree with where people are feeling on this. I agree with both of you actually. So people are comforted in their own hearts that their personal systems are not being targeted. And then people are also systematically looking at it. They're like, it's not a systematic risk to the internet because it's unlikely to be something that everyone hits. Even though in theory, you could plug this into Mass Scan and hit the whole internet at once. So that's a possibility. And y 'all know better than I do how few systems internally

get patched, right? So like, the systems internally to a to a corporate, a larger corporation are a super melange of old outdated nonsense, right? Like, so you may you may see use out of these exploits for a decade to come because of that. I think the one of my main takeaways here was people hunters are patient, just in general, right? Like, and I think it's really funny.

JAGS (08:29.487)
Mm -hmm.

Dave Aitel (08:47.478)
that people are like, well, this exploit takes a week to run. Therefore, it's not that good. And I'm like, a lot of great exploits take a long time to run because you have to increment a counter and it has to overflow across 32 bits. So that's a realistically, once 64 bit became a thing and 32 bit counters could be overflowed and run to zero and then you could still have memory allocations, there's a huge space of...

really good exploits that took weeks to run, who cares? And that, this is one of them, right? So like, that's a funny thing that the offensive teams are well aware of that the defensive teams maybe are not, I don't know.

Ryan Naraine (09:31.182)
So let me ask.

JAGS (09:31.183)
I think that's what I'm trying to get my, that's where I'm sort of sitting here and going, look, I'm glad we're all comforted, but should we be, right? Let's be honest, nobody's running the patch this, if you don't tell them that the internet is on fire and the whole place is melting down, especially right before a holiday and whatnot. But more than anything, the fact that we're sitting here going like, eh, this is okay. It's really fine. It's built upon the premise of

one particular way to hit this vulnerability and its constraints. So that's where I look at Dave and other people who know this space a lot better and go, I feel like you guys know how to do this better. Someone out there knows how to do this better than what's already known to us. And there's nothing inherent into vulnerability that says that someone isn't going to figure out how to hit this better.

Dave Aitel (10:21.238)

And they talk about it a little bit, right? They're like, an LLM might help us, they say. They're sort of making it up. You know what I'm saying? But they also point out that this is something that other people saw as well. They point to the, you know, little bugzilla thing where they're like, hey, someone else noticed that there's a signal race here. We're not the only ones who can see these things. So you're not wrong. These risks are always downplayed because it does make us feel better, right? It's like, we think we can recycle plastic.

JAGS (10:25.679)
Come on.

Dave Aitel (10:50.934)
Right? Like there's a whole bunch of things that like make you feel better and you just do them. It's great for you. Otherwise.

JAGS (10:51.599)
You

Ryan Naraine (10:56.462)
Plant a few more trees. Dave, did it help that this is a bug that we knew about in 2006, previously reported by Dowd? Two things. How does a bug get accidentally reintroduced? One, did it help this comfort level to know that we had seen this before? It was.

Dave Aitel (11:14.998)
I almost thought it made it feel like we were even dumber. Yeah, I know. It made it worse for me. I'm like, so you knew about it. So you redid it. That's great. That's fantastic.

JAGS (11:17.103)
Does it make it worse? Yeah!

Ryan Naraine (11:23.726)
No, from a protecting ourselves from it point of view.

JAGS (11:23.887)
Wow.

Dave Aitel (11:27.638)
I think maybe, I mean, obviously like things have changed since 2006. I went back to the national vulnerability database to look at the, you know, all the links from from Dowd's original bug. There is one of the best things about it though, is if you go to this particular bug on 2006, you'll notice that almost all the links are broken. Right. So that's actually really fun. It's like,

Ryan Naraine (11:38.926)
There still is a national vulnerability database.

Dave Aitel (11:55.158)
is like to see the bit rot of the internet has forgotten this bug, but Qualys hasn't.

Ryan Naraine (12:00.942)
Interesting.

JAGS (12:02.291)
That's a nice bit of advertisement for them. They should take that as a as a byline

Dave Aitel (12:07.19)
We know where these people come from right like

Ryan Naraine (12:07.47)
But it also tells us about the quality of the NVD as well. I mean, as a reliable database of where you should be able to go back and find the history of these things.

JAGS (12:09.391)
Yeah.

Dave Aitel (12:19.638)
You should. This was something we should have thought about 20 years ago is that we're going to need a really solid history for all this recorded in like somewhere easily accessible because the data is so valuable, right? Like what's the actual patch that introduces and removes this vulnerability? Would have been a great thing to be able to get three clicks into. But no, you can't see that here. So all that information is real fun. I don't think it makes me feel better that it's an old bug. I think

Ryan Naraine (12:39.886)
Right.

Dave Aitel (12:48.662)
There's a set of vulnerability types, like bug classes that I think people both know about, but don't care about. And that's always been where hackers have lived, right? So you try to do the unexpected. And, and a lot of that is things that people thought weren't that important. And I'll, you know, I'll just tie this right, right to modern events, right? James Kettle is doing a talk and at DEFCON or Black Hat or something about timing attacks as well, right? He's doing race conditions in modern.

HTP apps and people had written off the idea of race conditions in modern apps and even though he talked about it last year, they're like, well, that was cool. Whatever, right? Like, and he's teaching his classes like, no, no, these are real. These are things that can actually happen in your web apps. And people like, yeah, yeah, yeah, it's good to know, you know, but like, that's great. There's like, you find five bugs, who cares, right?

JAGS (13:37.934)
That's great, Guy.

Dave Aitel (13:44.534)
The reality is these things, if you're a good hacker, you're looking for the cutting edge. You actually are saying, this guy's onto something and I need to go further than he did. And that's how the system works, right? If you listen to Mark Dowd's podcast, he said, the offensive teams are two years ahead of the defensive teams because they have to be.

JAGS (14:03.567)
So that's exactly why I wanted to ask you about this bug the way that we have. Because not only am I put off by the notion that we're seeking comfort so quickly at the discovery of this thing, but I am extremely aware that we don't know what the hell is going on in the real cutting edge vulnerability space at all.

Like whatever we talk about as zero days, whatever we talk about as sort of exploitation in the wild, you're talking about something that's just A, so far, we're so far behind on the discovery and B, it means that we got to see like a shooting star and got to, you know, just try to characterize it, but we do not understand what is happening in that space for the most part. So I don't want to, you know, set the coordinates of our comfort.

around Oday as being like, well, this is the one we know and this is the only way it can work. Like that clearly is not the case.

Dave Aitel (15:02.422)
I mean, I wouldn't say it's the case. I would say that you have to look a little bigger on this one and look at like, what class of vulnerabilities are we missing? You know, it's not just all about SSH in this particular case. There's going to be old SSH boxes laying around that are still vulnerable, but it's about the technique.

Ryan Naraine (15:18.35)
There's a long tail for this bug. You think this bug has a long tail where offensive security, big game offensive security teams are investing in.

Dave Aitel (15:26.55)
And I mean, I don't even know, to be honest, I think you're going to want to hit this bug because it's exposed in a lot of places. But I also think this is the kind of bug that gets people excited to hit just because they're counting coup. You saw exploits coming out, you know, immediately, but getting it to a level of polish. Honestly, you often don't see a level of polish from a bug unless people have had it for a while as Oday. Right? Like I think that's always been one of the big tells.

JAGS (15:55.023)

The POC right now, apparently it doesn't work. Like it's not like it's just sitting out there. My understanding is that the proof of concept code that everybody's been sort of freaking out about, it doesn't actually work yet. Right, it's not to say that it won't, but... Right.

Dave Aitel (16:07.894)
And it's not really the basis to build the real thing on yet either. But you know, it's almost like a document. They're like, this is a start, which is fine. I mean, that's what it comes down to.

Ryan Naraine (16:22.574)
you guys mentioned ODE and I want to just kind of throw in something here. There was a Cisco NXOS ODE used in the wild, discovered in the wild, linked to Chinese APT that happened this week and nobody talked about it. It was just kind of flew under the radar and there have been, according to the Zero Day database, there have been 43 documented in the wild ODE attacks, in the wild discoveries so far in 2024. Those numbers either appear staggering to someone

Or to someone it's a roll of the eye of like, okay, this is just our reality. Dave, why are we here?

Dave Aitel (17:02.262)
Why does Oday exist?

JAGS (17:04.335)
Why are we here?

Ryan Naraine (17:04.622)
No, not only does it exist, but why are we here as an industry where everything is on fire over here and nobody cares. And we all get excited about an Open SSH, unauthenticated RCE over here. And it just feels like we're disconnected in where we are.

Dave Aitel (17:19.382)
That's true.

JAGS (17:22.927)
You get excited about it the way you do when you see like a train crash, right? It's not... Let's be clear.

Dave Aitel (17:29.558)
I mean, I think there's two different things here, right? The open SSH bug is art and people get excited about art. And then on the other hand is an industrialization of a surveillance capability that the Chinese government has put together and has aimed directly at our hearts. So, I mean, those are two different feelings for us, two different, almost two different industries that we use to address them. I think the Cisco bug is a command injection bug. I think.

Cisco NX has not had the world's best. This isn't the first ODE that they've even had from, I mean, we saw this in the ISUN leaks. Like the ISUN team had a Cisco NX bug, if I remember correctly. And they weren't the top tier team in China from what we can tell from those leaks. So, you know, I don't do a ton of threat intelligence, but I would just say like, I think part of the issue is like, yeah, that should be really important if you're running Cisco NX. But if you're running Cisco NX still, why? Why are you doing that?

JAGS (18:05.839)
Right.

JAGS (18:27.791)
You

Dave Aitel (18:28.246)
Right? Like, you already knew that you had a problem and you should have thrown them into the sun. So you didn't throw it into the sun and now I blame you. You know what I'm saying?

JAGS (18:37.487)
Well, come on man, like what do you run that is not, what appliance do you run that is not currently being popped by the Chinese in mass? And I say this like, look, when you tell me there's a zero day in Cisco anything, in my mind, I'm almost relieved because at least Cisco is still patching their shit and like they'll acknowledge that something is happening. Where it's like, yeah.

Dave Aitel (19:02.422)
They have a good P -cert, to be fair, they do.

JAGS (19:04.399)
Yeah, they do. And for the past two years, what we've been dealing with is like Fortinet and Pulse Secure, Avanti, whatever the hell you want to call them, not acknowledging that it is happening, then sort of acknowledging that it is happening, then asking you to sign an NDA to even help you try to triage whether something is happening on your box. Then they go, yeah, here's a zero day. Don't worry. We'll throw it in the pile with all the other zero days that everybody's been exploiting. And you move on. Right. The edge device thing is just insane.

Dave Aitel (19:30.998)
actually, even that is not the worst part of the political process that they're going through, right? Like, I think the worst thing is when they encrypt their their appliance, and then tell you it's to protect you from the adversaries. When it clearly it's protect them from a bad PR moment, the adversaries decrypt it very quickly. Right? Like, but you have no access to do forensics. So you don't know if you've been hit or not. Like, I think that

JAGS (19:46.863)
Hahaha!

Yeah.

Dave Aitel (20:00.79)
That is the worst thing they do. And honestly, it's one of those things that I just don't think like CESA can't address because it has a good cover story, if that makes sense.

JAGS (20:10.127)
That's definitely one of those places where you expected like if there was a spot for regulation to come in and just in the sense of like defending customers and users, it's like, yeah, selling me an appliance that I cannot readily investigate that is vulnerable and then telling me the only way that I can check it is by signing an NDA so I can't tell other people that this appliance is vulnerable is a state of, you know, consumer

fucked upness that I would have expected the government to maybe attempt to intercede in.

Dave Aitel (20:44.182)
I mean, I'm sure they're trying. I know that they've been pushing regulations left, right and center. I think the latest one is the idea that any software company with more than $47 million in revenue needs to report compromises within 72 hours, if I read correctly. I think that's a proposed rule right now and not a rule.

JAGS (21:04.399)
Can they report that through the NDA that Fortinet made them sign? Or is that...

Dave Aitel (21:09.11)
I mean, that's a really good question. I don't know how the logistics really work in these cases. I think it's a Slack channel, right? Like, I'm not on the Slack channel. So.

JAGS (21:15.279)
Sorry.

Ryan Naraine (21:18.926)
Hey, but here, Juan raises a great point about like just the muckiness in that edge device world and all of this stuff, right? But these companies have all signed the CSRB pledge. This is a pledge, right? A pledge that commits, the purity pledge that commits them to these eight goals and these, they're genuine goals that push people in the right direction, but it's all voluntary, right?

JAGS (21:30.831)
The purity pledge.

JAGS (21:41.391)
You can make motivational posters out of them, right? Like they're lovely.

Ryan Naraine (21:45.294)

Right. But a company like Yvanti signs it, right. But we know in the background, they are a complete and utter mess. Does that give them cover Dave? Like, do you think CISA is providing these companies with a little bit of cover and a little bit of wiggle room to issue press releases for another year about how serious they are before we could even get to the point of like, some of them aren't even looking at MFA yet or like.

Dave Aitel (22:05.878)
Is it wiggle room or is it, I think it's different for every company, right? Like Microsoft signed it, like, but I also saw a lot of security companies signing it, right? Like, so, I mean, you call Avantius, right? Why wouldn't you sign it?

JAGS (22:14.223)
Well, why wouldn't you? There's no teeth to it. Like, look, if I go and sign this thing and my code base is 20 years old without, which is the case for like a company like Avanti where it's just like, you know, we bought six companies, renamed ourselves 10 times and then the code base is still more or less the same for 20 years. Like, yes, I'll sign a pledge that says that whatever code we decide to write from this point forward will be in rust and will be like, you know, blessed by a system minister or something, but

Ryan Naraine (22:16.046)
Yeah, there is no

JAGS (22:42.319)
I have no intention of rewriting my entire codebase, so...

Dave Aitel (22:46.806)
And even if you wanted to, you couldn't. Like the rust thing has to stop.

Ryan Naraine (22:49.966)
Petras nascut ruredo.

JAGS (22:52.047)
It doesn't really ask you to do anything.

Dave Aitel (22:53.974)
No, it doesn't. You make so many good points here, but I just think that the reality of like the pledge is that a lot of it's PR, but PR is not a bad thing. Right? Like, like having like a little like, yes, provides sort of a cover in a sense, like, but I don't think it's a malicious cover. I think it's sort of like, you can use these pledges internally. And I think that's a lot of what you see CISA do, is you can see them say like, okay,

Now that you've signed the pledge, you can beat up your VPs using the pledge, right? So like, I think some of this stuff is pretty genius in its in its way. It just appears nonsensical from from the outside, because the dynamics don't make any sense, right? Like you're like, you signed a toothless pledge, you're not going to change anything. And the answer is, yeah, of course, they're not. We have no we have no teeth anywhere in government that could properly address this problem. We need them to address it themselves.

JAGS (23:50.031)
True.

Dave Aitel (23:52.278)
So we're gonna give one guy or person who's inside one of these companies a little stick that you can use to poke something with. And that's it.

JAGS (24:01.999)
How about some, can we give her some whistleblower protections along the way as well for when they inevitably get fired for not shutting the fuck up about?

Ryan Naraine (24:02.254)
Fair enough.

JAGS (24:06.534)
I'm not sure.

Ryan Naraine (24:07.822)
Fair enough. Fair enough, Dave, but let me push back a little bit because we said the same thing about the creation of the CSRB. They make up the CSRB. It has no enforcement power. It's just a lot of talking. CSRB actually brought Microsoft to their knees and we actually saw Contrite Microsoft implementing changes or at least maybe we can call it PR again. But isn't it fair to say the CSRB actually had a significant effect on where things are going?

Dave Aitel (24:17.874)
But.

Dave Aitel (24:38.198)
I had an effect on the conversation for sure, right? Like, so a PR blow is still a PR blow. Microsoft spends a lot of time and all the big companies do trying to make sure their image is unsullied. So it's not nothing. I would say that the CSRB I think has underperformed from what most people were hoping for. I would say so. But I like all the people on it. I'm not saying that. I just feel like...

Ryan Naraine (24:55.79)
Really? Really? What were you expecting? No, no, no, this is not about...

JAGS (24:56.527)
Wow.

JAGS (25:02.831)
Well, you like that class of the CSRB, right? Like, let's also acknowledge the fact that we had some really amazing people, Dmitri Alperovitch, Katie Maciurus on the CSRB, among others, but they're also rotating, right? So we liked a certain class of the CSRB, and to Ryan's point, I was deeply impressed with them. Like, I did not think that the Microsoft...

report was going to actually come out and say things the way they were and they did and it's super impressive. Then we get to the fact that like

Dave Aitel (25:36.15)
Okay, the Microsoft report might have been a high watermark though.

JAGS (25:39.311)
Yeah, no, no, for sure. I mean, you can see even the politicization of it even as Brad Smith discussed the CSRB with Congress and others. It was like, well, maybe next time you can maybe not staff it with people that have an axe to grind with Microsoft. You're like, yeah, you're clearly not understand. No, he does not. Absolutely not.

Ryan Naraine (25:55.79)
He has a point though. At least he has a point. He absolutely has a point. A VP at Google doesn't belong there. It doesn't matter how great they are.

JAGS (26:05.263)
And, but I'm sorry, they, look, I'll say this. Heather recused herself before the cloud thing and where the hell, but where do you find people that know what's going on and understand what's happening who don't work at a compa - who doesn't work at a competitor of Microsoft? Microsoft is in everything. Google is in everything.

Ryan Naraine (26:12.846)
They have rules in place that demand those recusals. These are not voluntary recusals.

Dave Aitel (26:19.574)
We have a deep bench. No, no, no.

Ryan Naraine (26:19.758)
Come on, in the whole United States we can't find someone, in the whole United, I'm not buying that. I feel like, and it's not only about the private sector participants, it's about the government participants as well. Like there are, the makeup of the board isn't perfect. I give him that. I disagree with that.

Dave Aitel (26:24.086)
Yeah.

Dave Aitel (26:29.75)

Okay, but I think we have a deep bench.

Dave Aitel (26:38.806)
Great.

JAGS (26:39.375)
It can't be. Which one? Where are you gonna get a bunch of government participants who are not about to leave the government and go get a job at Microsoft?

Dave Aitel (26:47.254)
That's a tool Microsoft uses very well. I think that tool is used heavily against the academic world and the think tank world even more so. It's hard to get a think tanker to put out a report critical of Microsoft because where's the next job coming from?

JAGS (26:49.935)
Absolutely it is a tool that Microsoft uses.

JAGS (27:05.263)
Look, the reality of the Microsoft situation is worse than we know. And like I think in the pre recording chat, like we were talking about how like US centric we can be here. Well, like I, so I was in the Hague, beginning, wow, Jesus Christ, the beginning of last week. and, we were talking about, issues with, with Microsoft issues with GDPR, et cetera. But like what I was trying to drive point to them is, sorry, the point I was trying to drive home to them was there.

is an obsession with regulatory capture from the part of Microsoft in Europe. And it's actually really, it should be insulting to us in the US because it doesn't happen in the US because I don't think they think that any regulatory problems could possibly come out of our gridlocked shitty system in the US. So there's this obsession with the EU going after, you know, events at the ICC.

Having the cyber peace Institute lobbying everybody out there. There's just constant Microsoft outpouring Brad Smith out there talking to everybody in the US They don't even bother and they'll just come and like lie to Congress and walk away and everybody sort of like dust off their hands and move on and yeah, which is something that to us as Americans should maybe concern us that like the the big companies have gotten to the point where they do not feel threatened by the US government in any way whatsoever

Ryan Naraine (28:13.838)
They don't have to.

Dave Aitel (28:27.894)
Would you? I mean, I get it.

JAGS (28:30.254)

No, I don't, but I wish that I wish they were like I wish they did. Right. The whole point is they're supposed to be this countervailing forces that are trying to keep each other honest here. And that that tension does not exist on this side of the world.

Ryan Naraine (28:44.75)
Well, let me point out here with Dave, let me point out here that we are less than 24 hours after the election of a new prime minister in England, where there's a lot of cybersecurity regulation based conversations or security things happening from the previous government. Dave, do you think there's some disruption in place, that there's some disruption coming down the pike in this conversation that Juan just called?

Dave Aitel (28:44.95)
I mean, I

Dave Aitel (29:05.43)
I'll just say I'm looking carefully at the Pall Mall process, as they call it, which is a process. So it's a diplomatic process that the British and French are leading. And, you know, both of them have had pretty big hands in it, but it's about looking at intrusion software and who's buying it and what you can do to essentially normalize the practice such that it's not

Ryan Naraine (29:12.238)
What is the palm oil process?

Dave Aitel (29:34.87)
being, you know, causing systemic risk is the theory. So it's a pretty big process, right? So it's a diplomatic process with cabinet members from the UK are involved. And I'm not an expert at the UK's government, but I kind of assume those cabinet members got fired yesterday. Like maybe or maybe not, I don't actually know. Right? It's like, like, so it's sort of like, these processes can get disrupted. And the same thing happens here in the States, right? So, you know,

Ryan Naraine (29:53.198)
You

Dave Aitel (30:05.302)
Every national cyber strategy quotes its last national cyber strategy, but they come from really different, you know, theories of government. So if we get another Trump administration, we're going to have a very different theory of how regulation should happen in this space. And when you interrupt these processes, I think they're very delicate, right? Like if you stop having the conversation on software liabilities for four years,

Does that kill it or does it just reappear in four years as if nothing had changed? Do we have two governments or one?

Ryan Naraine (30:36.654)

Right, a lot of this stuff is driven by momentum, right? Like real momentum.

JAGS (30:37.391)
No.

Dave Aitel (30:40.502)
I would think so.

JAGS (30:41.775)
Yeah. It's funny. I mean, I don't understand enough about the policy at all. I don't understand policy at all. But like, if there's one aspect of the Trump administration that folks seemed almost excited about and saw progress in, it was the cyber side, the pointy end of the spear within the USG.

and getting a bit more of like allowances and less red tape, somehow bureaucracy getting removed from the process of actually using some of the cyber capabilities in the US government. And God knows what else sort of falling out from that. And I'm very curious. Like I will openly say I'm not enthused by the idea of another Trump administration. I don't know who may or may not be. I do think there's two issues where that may very well prove.

beneficial to some niche of folks and it's like folks concerned about like Israel's ability to do whatever it needs to do under the circumstances and people hoping for more offensive cyber operations. Like those two, in my book, those are two camps that like can actually be excited for a new Trump administration, whatever that.

Dave Aitel (31:54.646)
or a Kamala administration to be honest, like Kamala came out on Twitter and everyone's been being really annoyed at her for not wanting to use Bluetooth headphones. And she's like, it's a security risk. I think it's been a long time since we've had a president who understood that Bluetooth can be a security risk. That's, that's pretty cool. Maybe that's the real issue.

Ryan Naraine (32:11.598)
Well, you can barely get Bluetooth to work when you want it to work. I don't know how you get it to work for an exploit, but I can't have you guys using Bluetooth microphones for this podcast, for example. Let me pivot to something that kind of just happened and I have not seen much of a cybersecurity conversation around is the Supreme Court ruling on the Chevron deference has been overturned.

JAGS (32:15.407)
Come on.

Dave Aitel (32:23.134)
It's true as well.

JAGS (32:23.247)
boomer.

Ryan Naraine (32:38.222)
Do you expect security regulations implications from that Dave?

Dave Aitel (32:44.054)
I do. I mean, I saw Juan shake his head, but the reality is, is like,

JAGS (32:49.423)
Only in disapproval. I have no idea.

Dave Aitel (32:52.598)
Okay, I see a lot of, there's not going to be a lot of specificity in general to cyber regulations in the law. First of all, it's moving too fast. It's tough to write laws about today's technology and then you find out three weeks later, they're completely wrong and, you know, or just unworkable, right? Like, so right now, if you look at like the national cyber strategy, you could see them say, well, we want rust on everything.

And then you're like, yeah, but we don't have any Rust programmers. So that's not going to happen. But if you'd written that into law, like, you can't, you know, launch a new operating system in space without Rust, you would now have an unworkable law. Right. So the specifics are not going in there. And I think the same thing is true for regulation in general in this space. It's just really tough. The sectors are evolving. I think the cyberspace lariam has done a pretty good job of getting their idea of what, you know, should be going into

regulation and just into cyber in general, but a lot of that they've done the really easy stuff first. So they've done a lot of the sort of, I'm going to add more money to a pot and give a little task to CISA, right? Like that's kind of the bread and butter of some of the latest regulation sort of, or cyber legal shenanigans. But in general, like FCC is hit pretty hard, right? The federal communications law is one of the most vague you could have possibly come out and outdated, right? Like in

And they've been running on just the Chevron ruling for the last many years. And I think the same thing we're going to see in cyber is people are just sort of going to... Constant litigation.

Ryan Naraine (34:27.63)
Do you expect litigation? Do you expect litigation to like existing decisions? No, no, no. To old existing decisions?

Dave Aitel (34:33.654)
Of course, of course they're going to start regulating all the FCC things that they don't like. And then they're going to start, I mean, anyone who's for example, if you're, if you're larger than $47 million revenue software company and CESA says, here's a new regulation for you. You're

going to, you're going to, it's cheaper to litigate it than to follow it. That, that's an endless series of excitement for our cyber strategy.

JAGS (34:58.063)
strategy in quotes.

Ryan Naraine (34:58.382)
You mentioned the strategy calls for regulations for securing critical infrastructure. I mean, if you look at page eight of the strategy, that's there. Chevron being overturned affects that directly, right?

Dave Aitel (35:11.478)
Of course it does. But I mean, they say critical infrastructure, those are really broad swaths of, of, you know, industry, I think schooling is considered a critical infrastructure under that definition. And we all know Miami data is humongous. I think they have four people securing 300 ,000 computers probably, I don't know, if you had to guess. So everything is critical infrastructure, everything's going to be in theory regulated, and then everything's going to end up in the courts.

That would be my summary.

Ryan Naraine (35:42.318)
Right. But the reason we had Chevron...

JAGS (35:43.503)
Or you can skip the whole problem and not regulate any of it. Which is where we seem to be.

Dave Aitel (35:49.622)
And that's where we've been for the last 20 years and I think people find it also untenable, right? So we are between a rock and a very hard place.

JAGS (35:57.327)
Yeah, I'll say, I'll admit I'm kind of sad because we started to see the involvement of the FCC in some of these things and they actually, it was like an adult walked in the room for 30 seconds. We were like, okay, they're used to doing some no nonsense regulation. They're used to some of the criticism that comes along with that. Maybe they'll come up with some good ideas and try to, you know, they do scare a lot of these big companies because they play in so many different spaces like carrier regulation and so on.

where they are used to the sharp end of the FCC. So to see them start to come on the scene and immediately get shot in one of the legs is concerning. We're sort of right back to square one in some way.

Dave Aitel (36:39.126)

I think we're right back to square one in a lot of places, not just in cyber. But I mean, I was spending a lot of time talking to CISA at a conference I was at recently. And they were like, we're doing our best. But we have, you know, we've essentially been told that Trump's gonna fire all of us, even though we're non -politicals. And we don't even know if we're gonna exist in a year. And that's their, that's their morale, right? So at that point, they're like, we don't even know if we're gonna exist in a year.

JAGS (36:57.327)
Yeah, true.

JAGS (37:04.047)
Yeah.

No, I mean, CISA's had a really rough go of things. Like, you know, we laugh and we give them a hard time and we razz them because I think there's been a lot of like high expectations, but they've had a really tough go of like the political process in so many ways, right? And they've become synonymous with the notion like all this bullshit about government censorship of blah, blah, blah, and you know, things with the cyber league, like there's so many ways in which...

Cis has just gotten sort of the short end of the stick. And to be fair, what is the point of killing yourself right now? If you know, there's a not even 50 50 chance that in a few months you're all just, you know, backs against the wall, right? So.

Ryan Naraine (37:45.326)
What is CIS's biggest achievement? If I could ask you to identify the biggest thing CIS has achieved.

Dave Aitel (37:53.622)
I personally would say being the one open door that industry can reach into.

Ryan Naraine (38:00.014)
communication point.

Dave Aitel (38:01.942)
Yeah, and I think that's where their strength lies is being the open door, being out there, being communicating everything. Do you think of them as a highly technical agency? Not necessarily, right? Like, I don't think that's their current strength. That's the NSA strength. And that's fine. But the NSA strength is not communicating with you. It is neurodiverse, and it should be. Right? Like, that's where it is. So

CESA is the, you know, I need to have a discussion with someone and get a straight answer team and that's perfectly good.

Ryan Naraine (38:37.102)

Yeah, but Dave, for that budget, that's what you get? I mean, like, you get an open door for that budget? Like, I feel like we should have a flag to stake in the ground that says CISA has done this that justifies a little bit of that spend.

Dave Aitel (38:44.982)
I think

Dave Aitel (38:48.886)
think we're going to see a lot of the a lot of the things that they've done flesh out over the next five to 10 years, right? So that's the other thing is like, I don't expect instant results. And I don't think the American people should expect instant results. I think they had a humongous mandate constantly changing, probably bigger than they really should have had, and probably still bigger than they should have had, right? Because like, the focus was, it's rough. But on the other hand, I think, overall, they've done a pretty good job. I think the whole, the whole, you know, like,

thread from Obama, honestly, through to Trump, and then through to, you know, the Biden team, you see a huge improvement right now in the quality of what's happening in government overall. They know who to talk to now. They signal message you, right? Like, I'm pretty sure if you had something that you needed to tell the director of SISA, you could get their signal number and you could signal them, you know, if you're at a reasonable size. That's new. Like, that's super new. I don't know if like, that was that that's a revolution.

JAGS (39:42.575)
Yeah.

Yeah, that is credit they deserve. And look, I'll be the first person to say that I've been really harsh on Cisa in a lot of ways. And I continue to be very harsh on Cisa. And Jen has to, at some point, will hopefully forgive me for being so. But there are aspects of what Cisa has done materially that we ignore because we're a different class of people. Which is to say, threat intel.

producers, vendors, security space folks. Like we aren't actually the main stakeholder on which you should judge this as accomplishments. They're busy, you know, raising awareness for MFA and getting a bunch of these like tiny bullshit 50 people, important companies in the middle of like middle America that you had no way to reach before that you could never get them to answer anything on security.

they're aware that CISA exists. They know what it means for CISA to reach out to them. That is a paradigm that has evolved that did not exist before, right? Who was supposed to go there? Secret service, FBI? Like it was very, and that was hard in itself, right? Like, absolutely, right? Like that was a self -defeating thing in and of itself. So in many ways you've created that. I think also like, you know, CISA has been around for a bit now and you can talk about different CISA administrations, but like,

Dave Aitel (40:53.43)

It was always FBI. But not being FBI is a huge strength.

JAGS (41:10.607)
under Krebs all the like election security stuff that happened. Like there are things that have been great even from the perspective of like raising awareness in a larger US populace that had no appetite, no understanding for what was happening in cybersecurity. Cool. Is that enough? Does that match the remit? I do think that CISA has.

Ryan Naraine (41:30.062)
And the budget, like guys, how much money does CISA have to spend? And I mean, like you're telling me this is a user awareness, that's their biggest accomplishment is a user awareness thing and an open door. There isn't anything technically that we can plant a flag in the ground. Like I'm just being devil's advocate here. I'm trying to get a sense of like, what has CISA accomplished?

JAGS (41:37.167)
Hahaha

JAGS (41:51.823)
There are things that I'm sure... So let's break this apart. Again, this is where I get into trouble, right? Like I love Chris Krebs, I love Jenny Sterling, I keep getting into trouble, right? Like I made a comment on Politico and I'm sure Jen has not forgiven me, nor should she. Fair enough, nor should she. But look, the problem with SISA to me is you can say they have a lot of money and they have a...

Ryan Naraine (41:58.094)
That's what I'm trying to do.

Ryan Naraine (42:05.678)
She's not gonna listen to this, go ahead.

JAGS (42:18.415)
getting way too much money if you look at any one of these individual remits and go, what have you accomplished? I think there's a larger issue here, which is there is this undefined mission. And I think in the perspective of running a new org within the US government, the thing to do is to keep trying to expand your remit, expand your authorities, and expand your budget. And what that has done in

a space as complicated and difficult and unwieldy as cyber is to create this monstrosity that has to address everything, could barely address anything, and for whom what looks like a lot of money isn't possibly nearly enough money. Like CISA just has too many remits, too many things within it, taking authorities from other places that could have possibly done it better, could have possibly done it together, and then having to offload what are technical processes to places like the TSA that can't possibly do any of it. Right, like that's the really weird thing about CISA. It's meant to do everything and it kind of doesn't want to do any of it, and it's kind of been given enough money to do a lot, but it's kind of expected to do so much that it's not enough. Like it's a very weird creature sort of in the middle of it.

Dave Aitel (43:42.006)
Yeah, strong agree.

Ryan Naraine (43:42.414)
CISA has a big naming and shaming stick as well though, like in the midst of all these Ivanti things, it's because of CISA's in the background, like cracking a whip that you start to see companies even acknowledge little things. I mean, there's a lot of, I'm trying to give CISA a lot of credit for behind the scenes whip snapping. Is that fair?

Dave Aitel (43:57.846)
Although getting owned using that Avanti thing was a bad look. So, you know, like, that's pretty bad.

Ryan Naraine (44:02.99)
Yeah, I mean, that's the reason they had to crack the whip, right?

Dave Aitel (44:08.886)
Yeah, it's pretty embarrassing.

Ryan Naraine (44:12.366)
we, we, we running out of time and I want to wrap up again. It's kind of folding it all back in once. Yes.

Dave Aitel (44:17.334)
All right, before we do though, I want to answer. No, I want to answer your question from last week. Right. So, so, costin was like, my gosh, what, what is one? What's that? Where? All right. And I was thinking about it since then.

JAGS (44:19.087)
Do not wrap up on shitting on SZA. Like that is not the last topic.

Ryan Naraine (44:21.646)
No. Yes.

Ryan Naraine (44:29.966)
Where are the press releases? Where are the press releases of these big giant success stories? Right? And Dave, yeah, Dave, you actually co -wrote an article on Lawfare, a responsible cyber offense where you called for like an honor among spies or an honor among

offensive security teams. When you kind of like, when you're having this conversation and Costin says, show me your success stories, what is your retort?

Dave Aitel (44:54.998)
Alright, I have a really clear one and it's Kaspersky, right? Without someone popping Kaspersky, right? And I don't know who that is. Would we know how bad they've been penetrated by FSB? Right? It was pretty weird because it was just like a very unbelievable New York Times article comes out says, the Israelis hit Kaspersky and then they discovered a bunch of FSB people sitting at the desktops.

Ryan Naraine (44:58.702)
Hahaha

JAGS (45:00.271)
Sorry. No, go.

Dave Aitel (45:24.822)
basically doing some bad stuff. Right? Now, I don't know if you can believe that article. But if it hadn't have happened, would we get the sanctions? Would we have solved a systemic issue with Russian access to both American and European, like telecommunications and other hardware, right? Like, this is a huge success story. The sanctions took years to develop, and you don't develop them without great information from the inside. That information could have come from a lot of places.

But the only place we know it probably came from based on Kaspersky's own reporting is from their systems, right? We know they were an actual target. We know that they were doing bad things and they got sanctioned for it. And we therefore protected American people, American industry and our allies from a known threat. And I think that's a fantastic success story.

JAGS (46:14.991)
I feel like you've just been, you've been rubbing your hands with this, with this story and you know, waiting to come on. It's coming from inside the house. I don't think that's a good example. I don't think, I think it's a terrible example. Mostly because like, it's a variety of, it's a variety of conjectures that I don't necessarily fundamentally disagree with, but you're putting them together to tell a story that I'm not sure is the right story, right?

Ryan Naraine (46:17.838)
yeah.

Dave Aitel (46:18.934)
I have. I've been like, you want the answer? The answer's you, man. The answer's you! That's what it is.

Ryan Naraine (46:20.814)

of July 4th.

Ryan Naraine (46:28.718)
That's a terrible example.

Dave Aitel (46:28.982)
I know.

Fantastic example.

Ryan Naraine (46:40.846)
Yeah, you're just stitching everything together into one big story.

JAGS (46:44.719)
You know, you want to talk about how we got the sanctions? Like they had enough to go on for a variety. Like moreover, what's the discussion here is like, why did you sanction individuals? Why did, if you did, why didn't you sanction Eugene and certain individuals? Like there's so many ways in which this is like a weird one. Yeah. That please.

Dave Aitel (46:45.014)
I don't know.

Dave Aitel (47:01.622)
I can answer some of those questions. I mean, if you want. But I will say that like, it's really under reported how much offensive cyber operations are used as part of sanctions enforcement. And you see this very heavily when it comes to the IRGC and oil and various Chinese tankers trying to move that oil and then get sanctioned and people leaking how that happened. Right? Like, you see a lot of this information come out. And what they're saying is, if you do business with these IRGC front companies,

you are getting sanctioned. And that's just the way it is. We know everything and we know it through cyber and we're very clear about it. And I think you, I mean, this has just been one of those understated things in terms of how governments operate these days, how things have changed. Kaspersky is not, not a counter example, I don't think. Right. So like, is it cyber? Maybe, maybe not. But the cyber was probably a big part of that story. And that's a huge, if you think of it as removing a threat,

like a dagger pointed at our necks? That's a success story to me.

Ryan Naraine (48:04.046)
But that's, I mean, the argument was against like the intellectuals and the predators and the NSO groups and those guys. You're lumping them all into offensive cyber in your example.

Dave Aitel (48:15.862)

Well, you got to say this offensive cyber solve problems first like it doesn't solve strategic problems and it does. Yeah. And, you know, in Alexa, you know, that report came out recently that they're not doing so well after they got sanctioned. I think there were.

Ryan Naraine (48:21.71)
Of course it does solve problems.

Ryan Naraine (48:31.31)
So you're of the view that these go on.

JAGS (48:31.823)
Fancy that.

Dave Aitel (48:34.422)
Sorry, go ahead.

JAGS (48:35.503)
I'm saying fancy that, right? Like it's a business. You made them financially incapable of functioning. Yes, they're not going to do well, right?

Dave Aitel (48:43.414)
Yeah. Well, the question then is like, does all of the people move to another business that does the exact same thing in Cyprus? You know what I'm saying? You know, like these, these, these can be very hard businesses to target.

JAGS (48:49.999)
Absolutely. Absolutely. That's a discussion we had last time, right? It's like all the cyber -merk companies, if anything, you almost forced them to go underground. And by underground, what we mean is they went to three or four countries that they are allowed to do whatever they want to do. Now, partly in service of governments that are our frenemies who we supposedly have good relations with but can't possibly get to comply.

So like, I'm not sure the sanctions for cyber mercenary companies thing was necessarily the best way to address that.

Dave Aitel (49:27.606)
I think that's why you're also seeing things like Paul Maul, where people are trying to build a stronger regime around how these things should work. People are trying to build norms. People are trying to regularize the whole process. So I think they start with sanctions because that's faster than some of these other processes, but I don't think that's where we're going to end.

Ryan Naraine (49:46.734)
Dave, I saw in the tagline the footnote of the article criticizing Google for burning counterterrorism operations. Your name was there as kind of like an inspiration for this piece. Do

you believe that Google is out of pocket one? And how should they proceed when you find all these attached to these offensive campaigns? Like what's the ask?

Dave Aitel (50:08.502)
I don't think it's a reasonable ask to say, you found an O -Day. Now we want to tell you what to do with it. That's the reverse of the ask that Microsoft has always said. Like, you found an O -Day. We want to tell you what you can do with it. And I think that's.

Ryan Naraine (50:25.198)
So, going to a government and asking that?

Dave Aitel (50:30.454)
What I mean by that is I don't think it's the offensive community is telling the defensive community what to do any more than I think the defensive community should tell the offensive community what to do. But I think if you are a defensive company with broad access, you get to choose your project, your tag, right? You get to choose what and how you target. And I think that's probably where you want to make your choices, you know, good.

Ryan Naraine (50:47.214)
You're project zero. You're Googling your project zero. Right.

Dave Aitel (50:59.958)
or bad, right? And I think the same thing is true for offensive companies, right? They get to choose what and who they target. And what people have asked them to do is try to target stuff that affects our adversaries more than it affects us. And I think it's the exact same story on the defensive companies, please try to target stuff that makes it so you're not protecting the Taliban.

JAGS (51:14.575)
That's safe.

Ryan Naraine (51:21.422)
This is such a ridiculous take.

JAGS (51:23.027)
I don't I don't think that it works quite that way. Yeah, it does not work quite that way frankly Let's start with that notion of targeting right like the on the defensive side like it's not like Google Google it has an embarrassment of riches when it comes to resources in general But I don't think they're sitting on look here's 20 Zero -day delivery ops boxes, which one do we want to fuck with?

today. Like I think you have you run into a box with seven no days. It's a box with seven no days. It's a crown jewel that you've reached. And frankly, let's discuss the counterfactual if they ran into a box with seven zero days active zero days into platforms they control and they looked away. Like you're talking about a violation of whatever. Yeah.

Ryan Naraine (52:11.758)
This is what Dave is asking. Dave is asking defensive companies to look the other way based on a notion of good and bad. Who determines this?

Dave Aitel (52:18.454)
No, that's not what I said. What I said was, you know, I don't think they ran run into boxes. I don't know the particulars of this particular incident.

Ryan Naraine (52:26.318)
They do inject themselves into these campaigns.

JAGS (52:29.231)
That's the job. That's the job. That is the job.

Dave Aitel (52:32.438)
Alright, but you can pick where you decide to inject yourselves into, right? Like, do you inject? Are you out there protecting like, bad people or good people? That's really the question and or, you know, by whatever definition you want to draw that.

JAGS (52:44.271)
Did you, you're patching O days. Like you're patching O days. You're not protecting good or bad people. You're just protecting Chrome, right? Like at the, again, if you knew that Google project zero knew about a Chrome zero day that's being exploited in the wild and they said, it has a scent of America on it and decided to leave it alone. Like, a, it entails no parallel discovery. Nobody else has it be like they had a

sense of attribution, you know, and they knew for sure it was the US and we're so comfortable walking away from it. See, like, you're talking about them abandoning a core remit of what they're supposed to be doing. I think that the discussion can be how you go about it, who you tell, in what order, you know, what time you give people, all those discussions we can have. The notion that they should look at a zero -date, they are within their own house personally responsible for taking care of.

and walking away from it seems like a ridiculous thing to ask.

Dave Aitel (53:44.726)
So are you trying to say they should run every ODA they find through the US government?

JAGS (53:49.615)
Not necessarily, though frankly, what is the problem? When you say run it by them, I think you and I have different definitions of that. It's one thing to walk up to whomever and say, hey folks, I would like to make you aware that we are in the process of patching these seven vulnerabilities

and what is a very unusual set, you know, circumstances for discovery happens all the time. and we will be patching these in the next two weeks. So if anybody

Ryan Naraine (54:12.846)
happens all the time.

JAGS (54:19.375)
would like to figure out where their equities lie, now is the time, as opposed to just think of the alternative. Are they supposed to look at a Chrome Zero Day and go, not today, and they just leave it there and walk away?

Dave Aitel (54:33.046)
Well, I don't know that they didn't do that in this case, right? Like they may very well have followed that exact process.

Ryan Naraine (54:38.798)
But Dave, you can't be proposing that though, like that's as a norm to look the other way. Dad, what's the ask then? Tell me what's precisely the ask of Tag?

Dave Aitel (54:44.854)
That's not what I proposed at all. I think that may be the current norm.

Dave Aitel (54:51.766)
My ask is that where analytics can be targeted, you target them at protecting us. That's it. And where they can't be targeted, if you're just doing a broad sweep, you're doing a broad sweep. The offensive teams will manage themselves. If we get caught by a broad sweep.

JAGS (55:06.831)
Well that's what they're doing. That's what they're doing! They got caught by a broad sweep. You - you -

Dave Aitel (55:13.014)
Do we know exactly how they caught this particular example? Because I mean, I don't.

JAGS (55:16.847)
Yes and no. Yes and no. So let's not talk about specifics. Let's say theoretically. If you fix certain heuristics around how you as a company scan all these C2s around the world or these boxes around the world and figure out sort of how some of that stuff plays out, what they deliver, what they put where.

If I find a box that at any point has delivered a zero day or a strange payload or something that doesn't quite play out well in a, let's say a sandbox of some sort that I've designed for these weird boxes that I'm probing and that thing pops an O day. And when I go poke at it, it, it not only pops a no day, but pops many a no day. That is the kind of thing that you would spend quite a bit of time building other heuristics around, right? Like

You're talking about a staging box that has produced a great deal of value. Why wouldn't you spend a great deal of time building other heuristics to see what else you might find that acts similarly? Not necessarily that is the same people, but like from a hunter's perspective, if you tell me that I had no detection logic that would have surfaced a box that delivers, that figures out what browser you're using, what...

type of device you're coming from and then serves you with the correct O -Day, then I'm messing up as a hunter and I better spend some time figuring out how to do that. And it seems like they did, they have, they have some very competent people. Google has plenty of logic around how it scans the internet. That is kind of like the bread and butter of what they do. And they turned that box up and a lot of other boxes.

So like there is an op -set question here, which is just, if Google has figured out a way where in those boxes we'll just come to the top of an analyst pile, then the ops people need to figure some shit out. They have a larger systemic problem. And what we're doing is having a conversation about a one -off that makes us uncomfortable, but there's a broader issue here from a detection perspective.

Dave Aitel (57:24.534)
Well, let me, I don't know. It sounds like what you're saying is that there's detectable heuristics that you can use to find targeting boxes. Right? So it makes complete sense, right? Because if you're serving two different pages, depending on what browser version they're using, that's detectable, right? Like,

JAGS (57:37.807)
Absolutely.

JAGS (57:46.223)
Yeah. And I have every browser, like, and I have a share of most of the browsers on earth that I can check for how they've responded to this site, for example. Not to mention my own heuristics, if I wanted to run that in a sort of browser sandbox of some sort. Like there's like, there's people whose whole job this is and like they do great stuff.

Dave Aitel (58:10.518)
Okay, so let's talk, let's go back to Kaspersky actually.

JAGS (58:13.935)
Alright, fine. Go for it.

Dave Aitel (58:15.798)

No, because I think it's a better it's a more it's a well documented example because they gave a huge talk at CCC about what they did with triangulation. Right. So and they did quite a lot of work. I don't know if you watched the talk, but they they quite literally they were like we're going to reverse engineer put all the public keys that were used into in the protocol and proxy the whole thing to try to pull the whole chain back. Right. If

JAGS (58:30.127)
I did.

JAGS (58:41.615)
Right. What you have to do because it's iOS and there's no way to actually inspect iOS properly. So they would have had to come up with all kinds of shit just to try to get in the middle.

Dave Aitel (58:53.302)
Okay. If you were an American based company or a European company, would you have also expected them to go through that much effort to peel back something that they suspected was counterterrorism?

JAGS (59:09.231)
well, this is what you're lumping a lot of things in there. A, yes, I would. If that was happening to my team in the US, I mean, I'd be infinitely proud of us. And I would love to see that level of effort. A, B, how do you say that you suspect this counterterrorism when we're finding it in our own phones? Like, unless you're saying like I'm staring in the mirror going like you're the terrorist, right? But that is a that is not a claim that I can go with.

Dave Aitel (59:30.294)
Okay, I'm not saying it's in your phones.

Dave Aitel (59:38.23)
Okay, it's not your phone. Let's say it's a mail server somewhere in the Middle East.

Right? Like there are all I'm trying to point out is there are scenarios here where you know enough information that you don't necessarily need to put in that kind of effort. If that makes any sense. Like there's a space here.

JAGS (59:52.527)
But you're limited. You want to throw away the fact that these people found it on their own phones. And that alone is a circumstance that like, it's hard to not be, you know, to discount, but also like, yes, that's exactly the work we would do. And I say this, like if Coasting was here, like we've done this work before for operations that could have been friendly, could have not been friendly, but the only way that you know is by doing all that work and going, look,

This is the grand scope of what this thing is. And if you really sat down at the end of it and went, holy shit, everything about this looks like counterterrorism, I do think you have a much more complex discussion to have. But that's the big difference between op triangulation and whatever the hell you want to call the like Google Oday box, right? The claim is that the Google Oday box, whatever that operation was, was awesome.

Thousand percent counterterrorism and some people someone just injected themselves in the middle of the thing whereas without try Maybe there was some CT, but their sure shit was just plain old espionage and your victim caught wind and That's that's a situation where you don't get to be like yo Can you guys chill out and not let people know we're spying on you right like that's I'm not saying yeah It's just not a good comparison

Ryan Naraine (01:01:14.446)
Yeah, that's ridiculous. Yeah, that's not a f -

Dave Aitel (01:01:17.206)
So.

Dave Aitel (01:01:20.63)
Okay, I'm not trying to posit like that op triangulation was not espionage because it looked like espionage it acted like espionage right so And you know, obviously, I think the name is a little silly as well. You know there's and we could probably talk about that for a bit too. I think that that in this particular case, you know, when you're when you're looking at counterterrorism ops. I think there's also a requirement on governments that they separate out counterterrorism ops.

JAGS (01:01:23.407)
You

Straight up.

Dave Aitel (01:01:49.43)
from espionage ops when it comes to their whole tool chain. Which is something that people don't talk about, but I think we did list.

Ryan Naraine (01:01:55.022)
This is the responsible part of the responsible offense that you're arguing for.

Dave Aitel (01:01:58.71)
I think that was in the paper that we published on lawfare, which I think is an important part of it, but it's difficult to ask some of your smaller governments, right? So like if you talk to the United States, that's certainly a possibility. If you talk to, you know, a tiny little government somewhere, it's harder for them to say, yeah, we have two completely different tool chains, one which you use for counterterrorism and one which we use for, you know, espionage and other things, or law enforcement. Like law enforcement should be separate as well.

Right, so I think these are complicated questions. That's why it's an evolving surface.

Ryan Naraine (01:02:35.406)
just to close a loop on the Google thing is the notion that if Google actually builds capabilities for government spying, we would all frown on it. But we're asking them to turn a blind eye to their obligation to fix it. And that doesn't compute in my brain. And they ask of Google from

Dave Aitel (01:02:54.294)
No, because I think it's at the wrong spot in the chain, right? Like once you found something, then, you know, at that point, you have to follow your processes. I think the places where you make decisions are higher up, they come into bar, budgeting and targeting. And that's the same stuff you would ask of an offensive company.

JAGS (01:03:03.503)
Yeah, I -

JAGS (01:03:11.855)
I think this is where the Vaughan folks, and I'm sort of putting you as a representative on that side, are not as familiar with the hunting process, where you would abstract some form of a heuristic from this, and I will bet you you're going to find multiple boxes from different types of actors altogether. So that's what motivates the process to iterate on this. You go, hey, there was a blind spot that didn't catch this immediately.

If we fix that, what else do we find? And it won't just be boxes from some Western gov. You're also gonna run into some random other thread actor that uses a similar JavaScript logic to find this, that, and the other. So like that is precisely what hunters are supposed to do.

Dave Aitel (01:03:58.582)
Yeah, I don't disagree. I think it's very interesting that there's an equal blindness from the offensive teams when it comes to how defensive heuristics work as there is from the defensive teams when it comes to how offensive teams work.

JAGS (01:04:11.279)
Absolutely.

Ryan Naraine (01:04:13.358)
Can we leave it there and pick it up another time? We were an hour and five minutes in. Dave, I tell you, you were amazing. Thank you very much. Appreciate it.

Dave Aitel (01:04:16.054)
For sure. Winning.

JAGS (01:04:17.391)
Man.

Dave Aitel (01:04:21.206)
Thanks for having me.

Ryan Naraine (01:04:22.478)
Juan, fantastic. Thanks. Congratulations on your Black Hat talk being accepted. We'll get into it next week. And Dave, just quickly, what are you up to with Cordyceps Systems? I know you left in immunity and you launched this new company. What specific areas are you guys looking at?

JAGS (01:04:27.695)
yeah, Lord.

Dave Aitel (01:04:38.838)
Honestly, we do national security work and a lot of graph databases. And these days we're competing with the DARPA AI cyber challenge. So we're trying to find bugs with, with LLMs and it's going, I'll say middling. It's sometimes you're good. Sometimes you're bad. but there's no other way to do it than to do it.

Ryan Naraine (01:04:46.99)
What are you building?

Ryan Naraine (01:04:50.862)
often.

Ryan Naraine (01:05:00.078)
Sounds great. Come back when you guys win the challenge and we'll have a long conversation about it. Thank you guys.

Dave Aitel (01:05:04.086)
For sure.

JAGS (01:05:06.351)
Thanks guys.