Episode 14: Three Buddy Problem

Exploding beepers, critical CUPS flaws, Windows Recall rebuilt for security

LISTEN:
https://securityconversations.com/episode/exploding-beepers-critical-cups-flaws-windows-recall-rebuilt-for-security/

Cast:

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

Ryan Naraine (00:02.466)
Welcome back. The three buddies are all back together. Welcome back to the three buddy problem. Costin Raiu and Juanito is here with me. Costin, you've been missing for a few weeks. By the way, thanks to Gabe for filling in last two weeks ago. You've been missing for a few weeks. Welcome back. How are you doing, my friend?

COSTIN (00:18.029)
Doing great, thank you.

Ryan Naraine (00:20.365)
And Juanito, you're recovering from LabsCon 24. By the way, let me start by saying congratulations on the delivery of another successful LabsCon. Just let me share some numbers very quickly. We had 164 attendees from 16 countries. People came in from Australia, Germany, Switzerland, Slovakia. There's a big giant list. We had journalists from every major publication there. It's been fascinating to me to remember the first sit down dinner we had with Migo.

JAGS (00:23.855)
recovering.

Ryan Naraine (00:47.905)

Hey, let's get a come up with this idea for LabsCon to where it is today in three years. So congrats on that. Can you give the people a big quick recap of your own feelings and how it went?

JAGS (00:58.166)
Yeah, so I mean, obviously I feel just massively better as a person just knowing that it that it's done right like and that we we nailed it and the people are quite so happy but trying to get a little perspective it's it's been really hard for me like I I slept for three days straight once the conference is over I think it's been like tipping over like a burnout point of being like okay we made it everything like everyone's fine everything's safe like and also like

It coincides with S1 taking on a really big initiative around my team and labs and sort of a lot of hiring and all that. So it just felt like we needed to get to this point before I could like just like relax. And so it's taken me a bit, but looking back on the conference, I have to know like we've gotten a lot better at putting it on. It's a lot smoother. People know what to expect and it's starting to create that like competitive.

camaraderie where people want to surprise each other with the content. They want to bring something that like no one else was expecting and have their own version of shock and awe. And it felt like it really paid off. Like the talks were phenomenal. The amount of effort that some people put into their costumes for the gala party was insane, right? Like Mark and Silas coming as the Palo Alto booth babes incident.

Ryan Naraine (02:22.951)
the lanterns on your head.

JAGS (02:24.205)
my God, mean full drag. Well done guys.

Ryan Naraine (02:27.889)
Imagine Mark Rogers in drag costume. Quite a sight.

JAGS (02:30.871)
Phenomenal. Yeah, yeah, it was was actually really special.

COSTIN (02:31.206)
I've seen the photos.

Ryan Naraine (02:35.462)
And you added a lot of stress to yourself by taking on this keynote, keynote day presentation that you did. I'm going to punt it now to Costin, because you got a chance to listen to it, Costin. sent you the transcript as well. Your initial take on seeing this type of keynote at the Cyber Security Conference.

COSTIN (02:55.847)
I think it was very brave and I did appreciate the fact that he started by saying that everyone is great, my company is amazing, I love you all. But there goes. So I thought it was pretty nice. It was a very thought challenging, thought provoking talk. I think it's...

JAGS (03:09.226)
Yeah.

COSTIN (03:19.225)
It will really benefit having a longer paper or an essay based on the ideas from your talk. And the first thing Ryan knows, I asked for the AI summary of the talk and you kindly provided so you can just sometimes it's easier to look at the text and try to understand the ideas and listen to it. And of course, there'll be I'm confident there'll be a lot of naysayers and haters.

They're like one of my smart, smart ass Romanian friends. I'm not going to name him. He said like, why can't one just like everyone just buy a Porsche instead of being depressed? And I said, dude, he already has a Porsche. This is a stage two.

Ryan Naraine (03:59.168)
He already has two Porsche.

JAGS (04:02.992)
There are next level of depression and the midlife crisis now. I don't know.

Ryan Naraine (04:08.036)
Juan, you deliberately try to not make this a I'm depressed, like I'm in bad shape talk, but that's how it was received by a lot of folks. What was your intent? Like give me the essence of what the intent of the

JAGS (04:21.609)
well, so let's be, let me treat that on two different levels. First of all, I am normally depressed, right? Like that is just like a lifelong thing that I've, you know, I'm very open about my mental health and I think it's important for people to talk about that stuff more often. I'm well -medicated. I have therapy every week and I have been working on all my childhood shit for many, many years. and we'll continue to do so cause that stuff is just, I mean, it's, it's amazing. It'll be there for fucking ever.

Ryan Naraine (04:46.626)
It'll be there forever, so just embrace it.

JAGS (04:49.828)
So, know, wonderful. think, you know, my therapist is having a great time, but there's the depression side of things. There's just the normal mental health stuff. Then there's what I see with this industry. And the reason that I'm pointing to it is that the threat Intel industry has been a

salve for my mental health for many years. It's brought me immense satisfaction. It's given me unbelievable room for growth. mean,

Kostin, when you and I met, I couldn't reverse anything. I didn't know how to write Yara rules. didn't know, I was very much on a different side of the house. And this has been a challenging and extremely rewarding thing for me to take on over the past decade or so. So to look at that and say, look, I know I and a lot of other people have gotten so much from being a part of this and found so much satisfaction and felt like we were doing something meaningful.

and to look around and get the sense that that is not the case. Not just for me, but for a lot of people. It just made me feel like something is really wrong. And if I'm having this hard of time with it, and I'm in a relatively privileged position, I'm in a company that supports me, I have a team of amazing researchers, we have great resources from our company, we have had no layoffs, like everything has been pretty charmed for us.

and I feel this way, then how must these people be feeling in these other companies? How is everyone? Like it was almost a temperature check. And I'll say on some level, I might've been a little bit relieved had other people looked at me and been like, hey buddy, like, I think you're having a rough time, but the industry's fine. We're all having a great time. You need to go like, go adjust your meds. Like on some level it would have been disconcerting, but on another would have been comforting to say, no, no, threat intel's fine. I'm just having a bad time.

Instead, what I got was everybody, VCs, researchers, whether you're a high level exec or a low level, like brand new individual contributor, and even government people, everyone came up afterwards and was like, were telling me their versions of what they heard and what they were reflecting on, which at least lets me know I'm not completely nuts, but

JAGS (07:12.991)
also lets us know that we are in the midst of a crisis. We are in the midst of a difficult time in this industry and that's worth airing and discussing and trying to address and trying to fix instead of just letting ourselves drift into the ocean.

Ryan Naraine (07:27.358)
Now, let me flip the conversation because this whole mental health issue, isn't it our own fault that we get ourselves so engrossed in this work and give ourselves so much of this kind of glorification and self -importance? I'm simplifying things here that it affects our mental health. And of course, in Utah, you've talked about mental health in the past and the importance of going on vacations, the importance of working from home and working from amazing places.

doing taekwondo, finding other things. Is there a connection between, you know, in cyber security, we kind of build up ourselves into being so important that we get into this, I don't know what you call it, this hell hole that one feels.

COSTIN (08:10.253)

I don't think that's maybe the main issue here. I think we talked about it in the exit interview with it when I was mentioning the story of Paul Morphy and the fact that everyone, whenever he traveled to a new city, they expected him to play some kind of a masterpiece and the stress, just the stress of being able, you know, every every Lapscom to do a big announcement like the biggest, it must be bigger than the previous one. Yeah.

Ryan Naraine (08:20.102)
Mm -hmm.

Ryan Naraine (08:27.087)
Be great.

Ryan Naraine (08:37.199)
gotta top the previous year,

COSTIN (08:39.785)
like whenever you know to any kind of conference we need a bigger announcement we need like more money more flesh more fireworks and i think that that's one maybe part of the problem and think uval noah harari was also talking about this and said you know everyone is so excited everyone is like super super super excited when instead maybe we should try to be less super excited like let's be more normal if you want

thinking about the long -term survival of our species and how we accelerate learning and how we grow as individuals.

Ryan Naraine (09:16.27)
What is one thing you hope to not have to go to LabsCon next year and do the exact talk one? Is there one fixable thing within a year that you can see? Is there a way we can get journalists, for instance? There was a call to action for journalists to be more discerning on these bullshit marketing things, these reports without IOX. I'm seeing you salt typhoon. You know what I mean? Is there a way we can, is there.

JAGS (09:39.325)
It's salt time for that.

Ryan Naraine (09:43.145)
One takeaway that you see, you feel like people should work towards. Instead of us, I'm just trying, like we throw our hands up in the air and say, we're in this void guys, like we gotta figure it out. But like where should people start?

JAGS (09:47.813)
JAGS (09:54.686)
I don't think that there is any one thing that can be fully addressed. What I hope to see is all of these things having some level of progress because they're all moving. They're just all moving in

a bad direction. The VCs, the journalists, and the research cycles and the mega companies, they're all moving in a bad direction. I'm looking at you, Cisco, I'm looking at you, Microsoft, I'm looking at like all of you, everyone.

They're all sort of trending in a bad direction. And what I would like, it's just a year. Like personally, I have some goals and some milestones as an individual and with this team that I'm entrusted and that we have just so many amazing people in. I have some personal milestones around what I want to see by the next LabsCon, what I want to have fostered.

within Sentinel -1 and that doesn't have to come from me. I expect to see it from the people that work there and giving them literally everything we can to succeed and say, look, your jobs are not in danger, your resources are not cut off, you have everything you could possibly want. What can you make happen? And I wanna be surprised in that sense. But that's us, right? Again, in a very privileged position.

What I want to see from the broader end of the industry is I want to see a healthy sense of empowerment across these different sectors. I think at the core of that whole keynote is this notion of disenfranchisement. And what I want to see is disenfranchisement being pushed back. I want these people to feel like they have a voice. I want them to feel like they are having the seat at the table that they should have, whether they know they need it or not.

And I want to see what that will result in bringing the smart people back to the decision -making table should mean that we start to see cascading effects that otherwise tend to fall into the cynical realm of Ryan you do this all the time. We all do it of like well, but that's never gonna get fixed well, but that's never gonna get better well, but that's you know

Ryan Naraine (12:05.107)
But 20 years, 20 years, it's the same thing over and over, right? Like I write the same stories and I can change the headlines and the dates and it's year after year. It's much of the same thing. We'll get to this cups vulnerability down in a minute and some on some of the other issues, right? It's just this recurring feeling. You call it a void. I call it a feeling of helplessness where you're just we're spinning our wheels and nothing is really going in the right direction. But, you know, a lot of people are making money. We're all employed. We kind of get to go to conferences. Like you say, we're in a privileged position. It doesn't affect us.

JAGS (12:17.763)
Yeah.

Ryan Naraine (12:33.228)
nearly as directly as maybe it should. I don't know.

JAGS (12:36.256)
I think we need to check our cynicism in the sense of... I know, look, I was having this conversation last night, but everybody seems to think that we're living in the worst of times. And

then statistically, in reality, we're in the best possible time of all human civilization. Everything is trending better. The disparity, the ratios of people that are...

Ryan Naraine (12:42.674)
It's hard,

Ryan Naraine (13:01.585)
You sound like Bill Gates now, bro.

JAGS (13:03.691)
But that's dude, seriously, like you, if you look at the numbers, not the experience, the amount of people that can read, that can eat, that have running water, that are in, that have an access to some level of education, like humanity is trending upward and has been steadily trending upward by ratios and numbers and just, just pure statistics, no matter what. And I'm sure that the situation is somewhere similar in technology.

At the same time, your experience is also true. Yes, we keep telling the same stories. We keep having the same problems. And we have a lot of like, what are like organizational, behavioral and psychological issues that we cannot seem to get ahead of. But it's not all the same, right? Like let's remember that it's not all the same. And I think both points of view are valid. It's just hard to have perspective.

Ryan Naraine (13:47.023)
That's fair. It's fair.

Ryan Naraine (13:56.472)
You know what's funny? In my private life with non -security people asking about what I do when I have to describe my industry, I find myself being the cheerleader. I'm less cynical in that world. I'm cynical in our world. But in that world, I'm telling people, listen, imagine you go to Walgreens, right? And you buy something off of there. And you literally walk by a piece of machine and you take your phone and you scan it like this. And wirelessly in the background, there's all kinds of magical authentication that goes here.

JAGS (14:08.894)
Right, right, right.

Ryan Naraine (14:24.981)
and make sure that the money is there and all that happens in a split second. Like, wow, you walk out the store, you've made that payment. All the security and technology built into these platforms and the systems and so on. I'm cheerleading for what the industry has done and built and like what some of these technologies we've invested in have pushed, you know, these leapfrog things in the future. So it's interesting that in that world, I'm like super excited about what we do and very excited to talk about it. But when I talk with my peers, it's this.

Disenfranchisement, devoid, don't know, Karsten, do you find this happens to you?

COSTIN (14:59.082)
Not really, No, no. The only thing that I was thinking about. I need to smoke more, right? I don't smoke anything, guys.

JAGS (15:00.489)
Yeah.

Ryan Naraine (15:03.244)
Dustin doesn't smoke enough. This is the problem. This is the problem.

JAGS (15:05.948)
Ehh

JAGS (15:10.325)
Clean living, it's a straight edge buddy of the group.

COSTIN (15:12.557)
Like my drugs are maybe what chess and even online. No, what the...

JAGS (15:17.765)
Eve online! my god. I felt bad about my Starcraft thing. Never mind.

Ryan Naraine (15:17.798)
I've is

COSTIN (15:24.653)
yeah so the t -shirt i wanted to ask you though if you were to choose what were like the the best of times you know like there was the best of time the worst of time what were the best of times in your opinion the golden years what were those like 2015 2020 2011 before for for for for threat intelligence yes

JAGS (15:42.637)
of times. Like in the industry you mean?

Ryan Naraine (15:43.349)
For security, for security or for my life?

my life you could send me back to high school I'd be pretty happy.

JAGS (15:53.557)
I, I think that, nostalgia is a, nostalgia is, is actually a bit of a human disease in some ways. Like we yearn for times that were never even what we think they were. so if I, if I had to indulge in

nostalgia, I would look back to a time that I wasn't even a part of, right? Like what you guys were doing in 2011, 20.

COSTIN (15:54.253)
threat intelligence wise.

JAGS (16:23.219)
12, the Stuxnet Dooku Gauss era, when all there was was discovery and there was no real sense of like the weight and reality of what's going on. what, you know, are are are they going to blow up our cars or are they going to give us awards? Does anybody care like that? We're doing this or does everybody care that we're like there was still a time when like things were unwritten and and there was like a magical period of discovery that

Ryan Naraine (16:51.632)
In a sense.

JAGS (16:53.138)
Well, that I think is very exciting. However, I don't think of that as a better time necessarily. I just think of it as a sort of like a nascent period that sounds very exciting. Similarly, like the great years of like 2014, 2015, which I was to some extent a part of, I think were an amazing time.

things that kind of been established, you could see the marketing value, there was a lot of support and there was still a lot of room for discovery, right? Every couple of months, you'd be like, my God, we just found the cool and then, my God, look at this thing and then, my God, like it was a very exciting period where the drawbacks and the pressure, the friction, the politics were just not a part of the picture yet. So I look back at those times and go, those were very special moments that I hope are codified, but I don't think they're necessarily better.

Ryan Naraine (17:43.367)
Then you went and wrote a paper about the ethics and perils and opened all our eyes to the reality of where our world was. I fucking blame you for this shit.

JAGS (17:48.695)
Man, fuck you guys. was trying to help. No, I think it was an appropriate diagnosis of a situation that we needed to be cognizant of. I do. Man, all right. I don't want people to hear what I'm saying. know I will. I just I don't think that the best of times are ever truly behind us. I think that that is a kind of nostalgic.

Ryan Naraine (18:03.494)
Pull that mic a little closer, pull that mic a little closer. You keep pushing it away.

JAGS (18:17.827)
boomerism that I don't want to be a part of, which is why, again, I did that keynote not in order to commiserate that it's the end of times and TI is dying, but because I want to say, look, things are

not good. How do we make them good? I'm not going to figure that shit out on my own. We all need to come together with a shared consciousness of the situation that we're in and be honest and point to executives who are trying to stuff us into shitty boxes we don't belong in.

point to a lack of investment in things we claim we want to happen. Point to cloud companies that claim cloud is the most important source of revenue and that's all they care about, but they just fired their entire security research team last week. Like there's a lot of hyper cloud companies, very, know. There's a lot of bullshit that I think we need to call out. I don't think that means we're in the darkest timeline. I think it means we're in a place where something's wrong and we need to make it better.

Ryan Naraine (19:01.455)
hypercloud companies.

JAGS (19:16.777)
And that could lead to, I hope, a golden renaissance of TI, right? Like, I like to think that we're always trending upward.

Ryan Naraine (19:25.765)
Costin, what's your answer to your own question?

COSTIN (19:28.543)
I need to make TI great again.

Ryan Naraine (19:31.375)
What's the best of times for you?

COSTIN (19:33.549)
For me, the best of times. I fully agree with Juan. Those years were the most interesting, the most exciting when there was potential and discoveries all the time. It was a bit chaotic and was a bit crazy and felt like a rollercoaster in a way. But that was for sure some kind of high point of TI.

absolutely like just like with the stock market and economy things usually also like they just go up and then they go down before they go up again and It may very well be that we have hit just some kind of a bottom point and from here. It's all upwards I Listen like I have I have hope so typically, you know when people have some kind of identity challenge or identity crisis they just going on a pilgrimage to maybe the middle is they go to

Ryan Naraine (20:17.367)
All right, we're twin.

COSTIN (20:30.657)

Jerusalem or they go to Mecca, they go to Beirut, they go to all sorts of hot places to solve, like to seek interesting stories, to, I don't know, see what the world is, what the world looks like from a different point of view. And there's been a lot of things happening there, like recently, which I think some of them were reminiscent of.

Ryan Naraine (20:31.647)
Juan, listen for some wisdom here.

JAGS (20:34.088)
I went to Brooklyn, bro. I... Hang out with Nasrallah.

COSTIN (21:00.173)
2015 -2016 discoveries or at least so they look.

JAGS (21:03.796)
care.

Ryan Naraine (21:05.086)
I actually saw a stat that every time a tech CEO goes to Bali or wherever to find enlightenment with the monks, he ends up losing his job and his own company, right? So Jack Dorsey is a perfect example. So be careful what you're suggesting.

COSTIN (21:09.739)
Mm -hmm. Mm -hmm. Mm -hmm. Good night.

or to the Amazon to try ayahuasca.

JAGS (21:20.071)
Well, mean, look, Jack Dorsey might have gotten whatever from Twitter and he I think he ended up in the better situation. He's the only winner. The only winner in that situation is Jack like Square Jack, right?

Ryan Naraine (21:27.401)
He's the winner, right?

COSTIN (21:28.557)
She's back, right?

Ryan Naraine (21:35.263)
All right, gents, we're 20 minutes in and we haven't touched the news yet. So this might end up being a long episode. I want to pivot quickly to the news and I was touching a couple of small items that, that I put together here. One is this Cops vulnerability, CVSS 9 .9. It's the biggest rage in Von Land. Cops is this common Unix printing system affecting Linux. Costin, you've kind

of dug into this for a little bit. What are we, what will like set the stage for us and what it is, what's the risk and what's the, you know,

the mitigations available.

COSTIN (22:05.143)
Yeah. So I mean, if you guys have friends running Linux systems, you know that they all struggle with two things. They struggle with their GPU or graphics and they struggle with printer. And sometimes they struggle with the audio. Like these are like the big three struggles. Audio, absolutely. Audio, video and printer. Audio, video and printer are the three big problems of all my friends, essentially. I did like once...

Ryan Naraine (22:18.536)
printer drivers.

JAGS (22:22.446)
microphones, webcams, speakers.

JAGS (22:30.866)
gooey's batteries.

COSTIN (22:35.693)
I challenged one of my friends I said I'll give you 50 lei which is like $10 if you can print this word document and I give you 15 minutes to print it and he managed to print it but in 16 minutes so I won but that's the truth I mean yeah and I think this is part of the solution or the problem if you want the common Unix printing system this super

Ryan Naraine (22:49.82)
I

COSTIN (23:01.901)
complicated subsystem that you install in Linux together with the GUI. So if you have a laptop or a desktop or Linux installation, it'll probably come with the CUPS. And typically this listens on port 631, but at least in my experience, it doesn't open if you want to like widely. It opens port 631 on the local host. So...

I think there are probably some conditions in which it does listen on the internet. was thinking maybe the most likely option here is some kind of a router or like the typical, you know, the typical cheap IoT device that you have in your home and it's a Wi -Fi router. It can be anything, including a printer server and by some accident or miracle or whatever, it also listen to the internet. my friends who can print on their own machines, they can print on anyone's router if they want.

but I think yeah, cops is this thing that's been around for a very very long time I was kind of expected to have vulnerabilities but on the other hand it's a bit I think weird that there's 75 000 vulnerable potentially vulnerable devices according to showdown on the internet with Romania being one of the top countries if I remember correctly was it like number four something like that

Ryan Naraine (24:27.788)
That's your buddy's trying to print.

COSTIN (24:30.125)
possible possible it looks like it's wormable yeah I think it might there's apparently there's some kind of user interaction required for the exploit to work however that user interaction might potentially be triggered remotely as well so to be honest there's there's a lot of things which are maybe not clear just yet we're still kind of waiting for more more details on this and of course everyone's waiting for

Ryan Naraine (24:32.96)
Is it warmable?

COSTIN (24:57.795)
the patches to be fully distributed and be available everywhere.

Ryan Naraine (25:02.328)
When you see CVSS 9 .9 out of 10, it kind of will set all the scanners alight. Should people be nervous, worried about this? And is there room here for this to say, why the hell do I even have this in my systems? Let me just remove it. Like, what's the mitigation?

COSTIN (25:04.557)
Hmm.

COSTIN (25:16.457)
Absolutely, absolutely. And I think we're going to see cases when company X and company Y, they got popped by whatever ransomware gang which exploited this vulnerability. You know it will come. And I think the best thing to do right now is to just block these ports from the internet. There's no reason why anyone from the internet should be able to connect on these ports on your infrastructure. I would just actually I did that already. We put

4 .6 .3 .1 in all our firewalls, we blocked everything. next, if you don't print on your servers, just do like everyone. Have a Windows laptop nearby and print from there. And just remove this from all the Linux machines.

Ryan Naraine (26:03.858)
One, you expect a lot of malware related noise with this and what happens inside a lab when something like this comes out? Are you guys scrambling to ship signatures?

JAGS (26:09.899)
There's no malware on Linux and I don't know what you're worrying about. Look, I find this shit hilarious on some level. I love, love that you have this massive attack surface area for something that most people seem to think has never worked well, but is on by default. I just love that. I love, I think it's hilarious. But the...

That's me. That's me maybe being a little more dismissive of like the Linux ecosystem just because they tend to be so unpleasant in in how they handle bones in how they handle realistic assessments of like threat modeling. Like I don't know what makes people Linux people. So I think it's this notion that you somehow control everything and therefore are more secure when in reality all you're doing is like the only line of defense is a password, just a simple password.

One simple password and that's it. But sorry, it's just to say that when something like this happens, there's a lot of concern primarily asked to how this is going to affect or how could it affect really VPSs like cloud, Linux instances and servers because that's where the intersection of Linux and importance lives. It's seldom about the

Linux users on laptops and whatnot. It's more about, you know, what websites and, and, you know, big database servers, whatever are exposed and have this thing available and are now sort of so, so infinitely poppable. And I don't know what that intersection really is, but contingent on that. Yeah, this is going to be the usual disaster and we're going to be dealing with, you know, corporate ransomware and all that kind of stuff. But it's like,

one of many at this point so

Ryan Naraine (28:04.686)
In addition to removing cups, patches are available. If you're in an organization, your last word costing put a bow on this. Make sure you patch this thing, right? As much as this being dismissed as did some hype and it might not be exploitable. People should take this seriously and just at least mitigate it.

COSTIN (28:19.917)
I think you should take it seriously. Block port 631 everywhere on the firewalls from the internet. Uninstall CUPS on all the systems where it shouldn't be actually installed. There are some super nice scripts actually available at the moment like Python scripts and other scripts that can just help you uninstall all the CUPS related software. And of course, just make sure that everything is patched when the patches are available.

which I think it might still take a few days.

Ryan Naraine (28:51.358)
switching gears to the very, very first episode of the three body problem. actually kicked off our esteemed podcast discussing the windows recall AI thingy that was coming in these windows

new AI PCs. Microsoft, had just, I think, pulled, they made the decision to kind of pull the preview and re -architect the security model.

Yesterday they announced that it's ready. It's ready for prime time with a bunch of security related goodies in there. I had a chance to sit down with David Weston at LabsCon and on a call yesterday kind of going over this overhaul of the security architecture, proof of presence encryption, anti -hammering, anti -tampering, some embedded DLP checking, screenshot data managing enclaves, like a security architecture that he's very, very proud of. We had a long discussion about how we got here.

as well. I don't want to dig into too much, but Costin, your initial response to Windows Recall is, who wants this shit? Like, why is Microsoft billing this shit? They're insisting that it creates an exciting new search ecosystem that you're going to be fascinated and amazed by. Just give it a shot. What's your reaction to the news of the new security model first? And are you going to give it a shot?

COSTIN (30:12.681)
This is my first reaction is I was to ask what is the secret registry setting for France that permanently disables it like that's the first reaction Yeah, I mean you were saying that there's actually some kind of Windows installation option to to never install it right like not to have it installed

Ryan Naraine (30:30.485)
Correct. I think he mentioned that he's like once you can have the bits removed at setup that it will never ever be available again. You can't turn it on. You can get rid of it forever from the system.

COSTIN (30:40.557)
I tried asking ChatGPT by the way, how do you do that? And ChatGPT didn't know, like didn't understand the question. Well, it was more like asking like, what do you mean? Which recall security and so there's so many analogies here. I probably do not deny that there might be some use cases here, any kind of maybe parallel and we were discussing this Ryan.

In the sense that Apple is doing the same. Why isn't anyone, you know, picking on Apple and only on Microsoft? The reality in my opinion is that Apple is not doing the same. Like they're not just taking screenshots of your desktop every five seconds. If you take a screenshot, then it can be indexed, right? That's what Apple does. And you take a photo, you need to do the action. Take a photo and then they will identify objects, blocks, people, paths and so on in the photo.

they won't automatically monitor, you know, be the big brother and look at everything that you are doing on your machine. And you can say, yeah, sure. But that stays in an enclave. It's on your machine alone. But like the issue.

Ryan Naraine (31:48.668)

And it's only activated for presence. It removes from memory as soon as it's done. It's built like a password manager to time out. There's like a bunch of security mechanisms embedded in there that says, listen, everything happens on device as well. I'm just kind of giving you the Microsoft Spiel. Everything happens on device. It's turned off by default. Like all the things that you would want in a feature is there from a security perspective.

COSTIN (31:57.717)
it is but...

COSTIN (32:11.315)
Let me ask a simple question. Have you ever seen any kind of security feature that was not broken like in the end? Like it was not cracked somehow? There will be bypasses for it and when the bypass happens, what happens? Like people will still have access to the data which, like from my point of view, that's a vulnerability. Having all that stuff on my computer, that's a vulnerability. Like it's a risk for me, considering my work, what I'm doing.

Ryan Naraine (32:17.905)
correct bypasses, there will be bypasses.

COSTIN (32:39.617)
having my activities recorded, it's a risk. So for me, it's kind of unacceptable. It might be useful, like I was saying, for some specific cases, right? And I understand the need.

Ryan Naraine (32:49.562)
Your beef is that Microsoft is creating this data. This is just creating this data, this big giant data store of stuff. Even though you can gran...

COSTIN (32:54.625)
Yeah, why?

COSTIN (32:59.789)
of me, of what I do and how I do and like, I don't know how I do things. And the question is why? Like, I don't need that. let's make an analogy here. So let's say the NSA comes to you and they say, listen, Ryan and Juan, we gonna install a new feature, which is we'll save all your home traffic from now on. It's free, like free of charge. It doesn't cost you any money. So whenever you forget something,

JAGS (33:10.761)
Heh.

COSTIN (33:29.357)
You can go there and look back at your home traffic from one year ago, two years ago, three years, 15 years ago, like whatever you were doing there, like what kind of websites you were browsing. Would you feel comfortable? Comfortable with that?

JAGS (33:40.18)
It's not a good corollary. It's not a good one. Yeah. Yeah.

Ryan Naraine (33:41.571)
It's not a good analogy because if it's happening in my house and it's happening on device, I think the on device thing is a big mitigation here.

COSTIN (33:47.981)
But they'll say like, listen, we will develop this software that we will install on your computer so the data will be available on your computer alone, but we'll develop the software and we'll put it on your machine. Would you be comfortable with that?

Ryan Naraine (34:00.937)
One, you said this is not a good analogy.

JAGS (34:03.591)
It sounds kind of cool. I don't think it's a good analogy, but precisely because I understand the point of what Cosin is saying, We're once again going back to the original recall discussion. You're talking about a flight recorder. That's just like, it's just like if you told me the equivalent of like, hey, we're going to install a keylogger and therefore everything you ever type will be searchable. All right. It makes me uncomfortable, right? Like I have to, okay. But well, yeah, I suppose.

Ryan Naraine (34:29.069)
not much different.

JAGS (34:33.424)
Look, I have changed my tune and it might be entirely based on my exposure to Dave Weston's strong jawline and deep conviction that he's doing very well with this. But no, seriously, I I like what he was describing. And to be fair, I don't want to just be cynical and say there's no way they could ever do this right.

Because Apple has shown us that there's a lot of things that you can do right, right? we, there were like what you just described, Ryan, like with the idea that you can just show up to a CVS today and pay with your phone. none of us as security experts look at Apple Pay as a weakening of your general security posture, even though it holds complete like control over your finances, it can work when it's not connected on the internet, et cetera, et cetera, et cetera. Like they figured out a way to make that work to a reasonable standard.

And what Weston, I think, was describing is not just a security first re -engineering of an interesting new capability, but also a security minded harness for what can then subsequently be applied as well. The idea for other things. Yeah. Yeah.

Ryan Naraine (35:53.98)
everywhere else. I'm excited about transferability to all kinds of other features within Windows, but go on.

JAGS (36:02.052)
No, I mean, you're telling me that you can have VM segmented features that rely on the TPM and proof of presence. Like they're, built into some kind of enclave. They require proof, like actual biometric proof of presence to be turned on and then subsequently be used. The APIs that are in it are designed to avoid

any kind of hammering. So it's not like I can just go brute force this thing for as much data as I ever want. And it gives me a specific kind of capability, which I think what Weston noted that I think Microsoft has done a poor job of communicating when it comes to recall as a feature is this is their version of spotlight. And I love spotlight on my machine. I think the only part where Apple fucked up on spotlight is the part where it tries to run

web searches for me based on what I'm trying to search locally on my machine. That's the first thing I turn off or block. But if you remove that spotlight is an amazing way to find literally anything in your Mac OS or in your iOS and people love it.

Ryan Naraine (37:11.161)
And you know the NSA has done it already, Do you know what's lost in the shuffle of this whole triangulation story? Is that the NSA had a plugin.

JAGS (37:14.825)
I don't know.

JAGS (37:23.775)
I'm going to just stop you from saying the NSA and triangulation at the same time. Yeah. Talk about triangulation. Don't talk about the NSA just because I don't think it's the NSA, but like just, just, I don't know, but let's not do that.

COSTIN (37:26.349)
triangulation attribution triangulation attribution

Ryan Naraine (37:33.531)
Why did I say? Okay. But that's the perception audio. Alright, I'll probably delete this whole section then.

COSTIN (37:36.301)
Who is it?

JAGS (37:42.335)
No, just say it, just fucking own it, because everybody else says that shit too. Just say OPTRI.

COSTIN (37:42.679)
Don't they know why why why?

Now this is a good example of why we need this recall, so you can delete things.

JAGS (37:51.085)
At Microsoft recall would let us know. Yeah, how to edit this shit

COSTIN (37:54.657)
Like a witness.

Ryan Naraine (37:56.045)
Wait a second, wait a second. The point I was trying to make is triangulation had a plugin that was mining spotlights by default, documenting of all images and screenshots on your devices. And they were able to use their C2 to call that to see things. that was the first documented example of a high -end Apex predator using AI on spotlight type devices. And there's no mitigation for that.

COSTIN (38:05.005)
Mm -hmm. Mm -hmm.

JAGS (38:06.455)
Yep. Yep.

COSTIN (38:08.973)
Mm -hmm. Mm -hmm.

JAGS (38:19.253)
Yeah.

Ryan Naraine (38:22.838)
What Weston describes here is is at least a mitigation for that.

JAGS (38:26.678)
What you're talking about is an on device ability to categorize. So let's take this on two different levels as a as a TTP as a thing that a threat actor does. I think it's a absolutely fascinating and I missed it when they when they just yeah, I know I. I listen to the talk every night. I missed it, but but also it's something that falls.

Ryan Naraine (38:43.809)
Done already. They described it in the CCC talk and it was, it went completely unreported.

JAGS (38:55.35)

It fits very well within the Western style of APT -ing because other APTs would just come in and smash and grab their way through. Well, just give me everything and I'll figure out on the back end what's valuable. And Western APTs were always known for coming in and being like, well, I'm not about to exfil a hundred gigs worth of stuff and get caught. So how do I bake some logic into the implant such that I can preselect

down select what is actually valuable and take it. And what they figured out is, mean, spotlight is an amazing feature for users to know how to categorize their own data. Why wouldn't they do that too? When you keep that in mind and look at all of the engineering that's going into recall in a universe where it is implemented well, and it's not subject to some categorical failure as so often happens with these things.

there is more security baked into recall than there is into spotlight. Like spotlight, once my laptop is unlocked or my iPhone is unlocked, there's nothing that keeps anybody from using spotlight search to find every picture of my cats. Nothing. So in some ways, I mean, in this escalation of slightly invasive ML...

forward feature creation. Apple got their first, did well and made people happy without them thinking about the ML side of it. Microsoft is coming second. Everyone is hyper focused on the AI -ness of it and the way that data is being stored, generated and used. But they are in this second iteration putting a lot more security into it than Apple has. At least for its access and use.

Ryan Naraine (40:50.142)
Here's my beef with it though. It's turned off by default, which they're making a big deal out of announcing. Who knows if it's not gonna be turned on later on. We've had these examples with Microsoft in the past once, and even if it's not turned on, how much their salespeople are gonna be badgering you.

JAGS (41:00.219)
Yeah.

COSTIN (41:01.142)
Mm.

JAGS (41:04.027)
some idiot PM is gonna like push for this needs to be on all the time or

COSTIN (41:05.463)
Mm.

Ryan Naraine (41:08.036)
Not only that, but you're going to get these constant alerts to please turn it on, please turn it on, please turn it on. Even if people, you know, doesn't activate it. And that drives me crazy with Microsoft as much as you want to applaud David Weston's and the technical folks efforts into

kind of baking this security mechanisms into it. Like you just can't trust the vendor to not mess with it later on. And I feel like how do we get, how do we get to that point where I don't know, this is, is when the depressing. Yeah.

COSTIN (41:08.151)
Mm.

COSTIN (41:13.356)
Mm.

JAGS (41:35.077)
That's a bigger problem. That's a bigger problem with Microsoft. It sorry with Windows ever since we got into like the Windows 10 and 11 era of things where they they've taken a really paternalistic approach, which in some things I can appreciate why. Like I think, you know, insisting that you have to install patches. Everyone hates the way they do it, and I think there's probably a better way to do it, but.

I appreciate that you're saying, look, motherfuckers, like you need to install patches. Like you cannot have a computer and just keep pushing the postpone button for like six months and then cry because you didn't update your shit. I appreciate that. I do not appreciate the way that they've gone about enabling Cortana, enabling some of like the search stuff, even in your like.

in your start bar and like the inability to like, how hard it is to turn off Defender even for like legitimate uses like our own. Stuff like that really bums me out. And I think that's where you see this like weird commodification of Windows as an advertising platform rather than, and like as a telemetry generation platform rather than an operating system. In that it has made the idea of using a Windows laptop as like a daily,

actual thing like nah, no, no, I'll VM it. I'll use it for dynamic analysis. If I ever have the misfortune of using Linux, I'll keep it around so that I can print stuff, but I don't know that my daily driver can be that.

Ryan Naraine (43:17.326)
Speaking of daily and drivers and Windows, Microsoft, since we last spoke, Microsoft had an EDR summit. again, Weston is in the news here coming out and saying, listen, we're going to provide a user mode API for you guys to stop hooking into our kernel directly. I imagine this is going to be entirely voluntary, right Juan? Like it's up to the vendors to decide if they want to use this or not. What is your reaction to the little driplets of news we got out of him about this?

And this SDP, this software development practice that will require this phased rollout and so on, like all the things that, you know, should have been there in the first place, you're going to be asking for quick reaction.

JAGS (43:51.97)

I have no idea. That's my quick reaction is I have no idea. I think in some ways it's kind of what I'd been asking for in the podcast. So yeah, great. You're standardizing the way in which you're gonna kind of fit into the kernel. This one is gonna come down completely to implementation and enforcement.

Ryan Naraine (44:03.468)
Mm

JAGS (44:16.832)
and in a variety of ways, right? Is this gonna become a way to crimp the AVs or make them stronger? Is this gonna become a way to muscle people out of your market or to enable them to do better and like focus more of their resource? Like look, how many developers at every EDR and AV company are dedicated to stability? Is that something that we can finally start to like, okay, I don't have to have.

10 dudes who spend all day trying to make sure we don't like have some kind of like interrupt problem or like deadlock something like now it's all great. Okay, cool. That sounds really nice. At the same time, how is that going to be implemented? How's it going to be pushed out to all of the legitimate folks that want to use this? And then more importantly, I saw some offensive folks like folks in the room who have done offensive work before who were salivating at the notion of a user land.

way to like hit the kernel that Microsoft manages. So there is a lot of potential to like kind of concentrate all this and all this capability in a single place and then go, okay, well, how are you actually going to manage and make sure that it isn't being misused by somebody else? All of that is unwritten as far as I'm concerned. I'm not saying that it's not doable well. I'm saying that my judgment is completely tempered.

until we see how they roll it out and what they do.

Ryan Naraine (45:46.932)
Kostin, you've said, I'm interested in giving up some speed in the interest of reliability. Does this move in that direction for you based on what you've heard so far?

COSTIN (45:50.566)
Mm -hmm.

COSTIN (45:56.597)
I think so. And to be honest, this is in my opinion, it's a very good initiative. It's the kind of things that we were recommending and the kind of things that we were expecting. And maybe just a bit dive into Adam Myers testimony in the Congress where he essentially said that they are now doing the things that we discussed in the podcast initially, which was like slow rollouts, testing on

know, probabilistic distribution of the updates, testing on more platforms and so on. So all of this, think they're pretty good progress. And for me, they look very positive.

Ryan Naraine (46:38.982)
Does this make this never happen again? Let's assume it's implemented and it's managed and, you know, it's optimized one. It's let's say in the best of the worlds. that, does this CrowdStrike incident happen again?

COSTIN (46:42.413)
Mmm.

JAGS (46:48.375)
It, it, I, I think that this is, there's no reason to think that we have changed a paradigm. What this is going to make sure is that this doesn't happen again with CrowdStrike. We have done nothing that suggests that other companies will suddenly become extremely responsible about their update mechanisms.

And like, that's the thing, like, I think everyone is so focused on the fact that like, you can cause kernel instability and therefore a blue screen of death. And we're not discussing the part where you go, okay, that's like a, that's something you cannot engineer out of an operating system. Like all we're doing is trying to find ways to like mitigate that possi, like the risk and the possibility. Okay, cool. What about,

Update mechanisms like frankly, this also came up with like the discussion about KL and like Kaspersky suddenly like force updating everybody onto like this is your new stepdad kind of situation and sort of shoving their whole US customer base to some random fucking company. But like the fact that we allow each company to implement their own update mechanisms and have their own standard practices around updating.

I'm surprised that that is not something that gets more attention. That is frankly one of the weakest points for all of our security postures. is

Ryan Naraine (48:26.637)
What's the answer though? Do everyone use Microsoft?

JAGS (48:30.401)
I'm not saying use Microsoft's, but like some semblance of like a managed update pipeline or whether it's managed by the mega vendor or you create some solution that means that it's managed by the people that that run MDM and enterprise like management or whatnot. this is something that would do well to find. I'm not saying centralization, but standardization update mechanisms need.

some level of standardization, granularity and visibility. Right now it's the wild fucking West and it's much more terrifying for package managers and things like Brew, NPM, Apt that everybody

in the Unix world uses and have zero visibility into what updates are going in there, the health of those updates. Like that's why we have so many like supply chain vulnerabilities these days. It's, you know, from not Petya on down.

The fear is, yeah, today's software was great, tomorrow's software update is a fucking question mark. And like, we'll see if it was sent by the person that was supposed to, if it was well QA'd, if they went through canary testing, you have no idea. That's an area that I think we're doing really poorly on. And it shows.

Ryan Naraine (49:53.897)
Kostya and he buried the lady there for a second, but I also have this ultra AV people on my list here. And I'll punt the question to you. People woke up to find that they were a previous Kaspersky customer and they had this ultra AV thing and ultra, I think ultra VPN as well. If you had bought Kaspersky VPN, you got this ultra VPN installed quickly. Is that a normal thing when, when, when divestitures happen? Let's just say it's not Kaspersky. It's not these people. A normal divestiture happens.

and we got to switch products and we got to switch branding and so on. Is it normal to just remove one and re -upload a new one and move on in our world or is this a big problem?

COSTIN (50:30.477)
In my experience, I never heard about anything similar before. Typically when something like this happens, what you see is some kind of pop -up which says, hey, we're going to be gone by the end of September, but worry not. Here's an alternative that is free, it's compatible with your license and you just click here to install it. I've never heard in my life like something getting upgraded to a totally different software, totally different company.

that you didn't buy from, that you don't know, that you don't trust. Maybe they were good, but again, you don't know them. You don't know who they are. And like overnight, I don't know, like this seems to me very risky.

JAGS (51:06.359)
How can you trust them? You don't know who the fuck they are. None of us know. No one knows who they are.

Ryan Naraine (51:14.622)
Do we know how many US customers they had? Like how many people would be impacted by this? Are we talking a million, 10 million?

COSTIN (51:20.333)
should be a couple of million I guess. Again, I have no way of knowing, but just looking at previous reports and the bans in the United States, I would say probably a couple million.

Ryan Naraine (51:32.86)

And the Kaspersky apps have been removed from the Play Store as well, right? I believe that's completely gone. You can't even find it in there.

COSTIN (51:39.319)
but not replaced with the ultra EVA thing.

Ryan Naraine (51:42.568)
Who is this ultra AV people, do we know?

JAGS (51:46.419)
heard it some Indian company, apparently their who is registration is like super fresh. it's a, this is, I mean, this is beyond fucked up in a lot of ways. Like I think we would have a far easier time if it were not that it makes it any less sus, but like if they had just been like, okay, you're all Norton customers now, like by it'd be like, okay, well it's an established AB competitor that people have known forever.

COSTIN (51:46.551)
We don't know.

JAGS (52:12.73)
I'm not saying that I'd be thrilled to see that crap pop up on my computer, nor do I like the idea that a vendor just are again arbitrarily updates me to whatever the they want. But it shows you that they've always had that ability, right? That was Rob Joyce's point on Twitter. Yeah.

COSTIN (52:15.18)
Mm.

Ryan Naraine (52:27.353)
This is Rob Joyce's tweet. Rob Joyce tweeted that, Hey, this has always been a risk of giving Kaspersky root access to our machines. they like, here does this, does this minimize Kaspersky's previous, Hey, you don't have proof that I've done any of this. Now there is proof that you could have and you have.

JAGS (52:34.233)
Well, I don't

JAGS (52:42.556)
To me, it shows a weakness in a variety of statements and arguments, not just Kaspersky's. I always thought the US government came in extremely weak and flat -footed and not very smart when it came to the way that it tried to problematize things with KL, because it was sort of mincing words in a way that didn't really...

make the argument they wanted to make or that they should have been making, which is AVs and EDRs imply a deep trust relationship. You are generating telemetry and you are allowing

somebody to look out for your best interests. And like the move from AV to EDR, what made that slightly different was instead of completely trusting the company to do that for you, you suddenly had a kind of

co -managed relationship on the EDR side, right? You have a management console, you can see the telemetry that's generated, you can also kind of be involved in the management of what's happening with your systems, but there's still a deep trust relationship. I, again, if your problem with KL was the ability to do silent six, which everybody can do, everybody does, or if it was like the idea of like having

specific targeted detections and whatever that only showed up to one computer and not the others, why didn't you focus on the update mechanism? Why didn't you focus on scrutinizing the signatures that were coming down that pipe? That's what needed to happen if you ask me. Now, on the KL side, like let's focus back on KL, because they are clearly the ones acting in some level of bad faith at this point. It's like your whole statement, your whole stance was,

Yes, but you can trust us. Yes, but you have never caught us actually, you know, show me the receipts. You've never actually caught us doing something wrong. You're bitching about silent signatures. Everybody else does it. Show me a silent signature that that did something that we weren't supposed to be doing. That was a lot of you know us, you trust us and to then go, ha ha, never mind. This is your new Indian dad. You go, what the fuck just happened? Right? Like the it was all.

JAGS (55:07.683)
I think it comes back to our discussion even on the first episode of this podcast, which is to say, I was very happy to put my face forward to defend what great was doing when it was under the control of folks that I trusted and saw acting in good faith, which means that I have an equivalent responsibility now to look at what they're doing now that they're not acting in good faith and go, yeah, that's fucked up. That's not the right thing to do.

That's not what a software company should do. They put their profits at the 11th hour ahead of any trust relationship with their customers. okay, I understand maybe you think of sanctions or whatever, justify that. But what you've shown is that when push comes to shove, you're not a trustworthy steward.

Ryan Naraine (55:57.493)
Dustin, is this a change in the culture of the company, you think? Because this is not something we've experienced before. How did you react to seeing this whole ultra -AV reinstall thingy?

COSTIN (56:09.289)
Well, I was well, first thing that I was thinking about was I would like to get my hands on this Ultra EV to look into it first of all, just to understand is it maybe the same product with the same engine with a different name, like, you know, white labeling. I think that would be interesting to

verify. Probably it's not, but nevertheless, I was thinking how do I get my hands on it? And now the second thing was imagine that, you know, this comes to Europe.

JAGS (56:19.692)
shh shh shh shh

COSTIN (56:37.995)
Like maybe the same kind of situation happens in Europe. And does it mean that all the users in Europe will suddenly see their installations replaced with the ultra AV as well? It's a legitimate question. Like, is this a scenario that expects all the users? Like, I don't know, outside Russia. It's a legitimate question.

Ryan Naraine (56:58.084)
legitimate question for all AV2. mean, if I'm using ESET and they get acquired next week by some company in some different country, is that a legitimate worry that I now have to take on a little bit of a risk factor I have to take on when I think about purchasing and installing these products?

COSTIN (57:03.789)
Mm -hmm. Mm -hmm.

COSTIN (57:14.581)
That's true, but when they get acquired, things won't change automatically. Instead, you'll probably have to pay or to agree to having your software replaced by something else. Actually, I was just wondering if this is maybe potentially an option for a class lawsuit, I don't know, for the US users. Because in the past, companies that were caught selling telemetry, for instance, they were fined like in a very, very bad manner.

And I think potentially, potentially this could be the case as well.

JAGS (57:49.604)
I'm curious, like, you know where I would go look for a precedent is what happened when like Norton got bought by Symantec, for example, because you have an equivalent product that they could have pushed. I'm pretty sure they didn't. I think they eventually end of life did and said, hey, you know, this is gonna this is gonna stop like you can upgrade if you want. But again, you don't see the push. think that's that's where you can say this is a relatively unique circumstance with the sanctioning and whatever.

but it almost, to me, looks like somebody at KL went, okay, well, fuck you. And like, in that case, let me just pawn you off and make some last bits of money out of this thing. And I guess that seems in like a teenage rebellion mentality, that seems like a reasonable thing to do, but reputationally, like you're once again in indefensible territory.

Ryan Naraine (58:24.46)

Fuck you.

Ryan Naraine (58:44.662)
An interesting question is in the US there was a fraction of folks, I know, technical folks who were rebellious enough to say, I'm going to use Kaspersky, I've never seen proof, I'm going to continue to use the product, it's a superior product, I trust the great guys, the great guys do great research, the product, these guys consistently find the big things, I'll continue to use this. What do you say to those folks now? Get rid of this thing, is that like your advice now is how do you, what happens next for folks? What should folks do? Let's put a bow on the story.

JAGS (59:15.433)
asking me.

Ryan Naraine (59:16.872)
Anyone like if, if, if there's a buddy of yours that come and say, I've always used Kaspersky because the product was just very good.

JAGS (59:24.005)
What is the so I will say that before when it was discussions about telemetry and discussions about like the nuances of signatures and sensitive data, it was relatively easy to be like, yeah, mom, but like, this is a good AV, just install it. like for the purposes of what you're doing, you know, you're like, no, no, the coverage is fine. You're not handling classified data. I just want you to like not get popped. This is a good product.

Ryan Naraine (59:53.3)
I was giving away free cereal keys to family and friends for exactly this reason.

JAGS (59:56.378)
Well, just because and frankly, mean, what what do you recommend to people? Because like, look, I'll tell you. right. No, but I was going to say, like from the perspective of like CrowdStrike Sentinel one, like any of us, like we don't do consumer. So there's no competition there at all at all. That is just not our area, not our bailiwick. That said, this change now makes it so that from a consumer perspective.

Ryan Naraine (01:00:02.89)
Now they have this ultra -AV shit on their machine.

JAGS (01:00:25.497)
there's a legitimate concern and the legitimate lack of integrity that I could no longer recommend. Now I'll go, well, and I've already been doing this. It's like, yeah, just go buy an ESET license, right? But it's based entirely on they have great researchers, they do great work, it's a good product, it's consumer licensable, and we've never seen them suddenly decide to fuck over an entire customer population. Big difference, right?

Ryan Naraine (01:00:56.059)
Next story in the list should have been higher, but I think we should discuss it because the implications for device security is the exploding pagers in Lebanon. Since our last podcast, this story has been the biggest story. The New York Times did some fine reporting with the long -term play at creating this company, creating this special company, and kind of targeting that whole marketplace long before.

JAGS (01:01:07.853)
You

Ryan Naraine (01:01:21.531)
really fascinating thing on the intelligent side. My question to you is, do we have to worry just generally about the ability of little, little devices like that to explode and cause problems with all these chink -ski devices we're buying from China and bringing all over the

JAGS (01:01:39.693)
Are you planning to be like a Hezbollah courier at some point?

Ryan Naraine (01:01:43.525)
No, but someone, let's say someone wants to cause as much commotion here in the U S and, and figured out you could figure out a way to get into this cheap knockoff IOT Chinese ecosystem and have some sort. I'm just curious if there's a supply chain implications for the rest of us. The question is, have we crossed a Rubicon here? Is there like a, is there a wow, they went there.

JAGS (01:02:02.626)
No, I don't think we've crossed a Rubicon because what we apparently understand in this situation is that there was tampering to include an explosive, like an actual explosive component into a otherwise safe device. It's not they figured out a way to blow up a standard device from the factory.

the way like if they had figured out a way to just like bleep bloop their way into like having normal standard beepers blow up, then you go, that is a terrifying be perfectly replicable see completely unavoidable. So what the fuck did we just unleash on this world?

Ryan Naraine (01:02:32.173)
Yeah, those are two different things in tired.

Ryan Naraine (01:02:50.189)
Replicable through interdiction though.

JAGS (01:02:52.662)

Well, that's no different than me, like just having your food delivery stopped and putting a bomb inside of it, right? Like you're talking about like, can I violate the integrity of any device or any container you use and put a bomb in it? Sure, that's never been different.

And they weren't irresponsible about it. They didn't go into the middle of the standard manufacturing process and put a bomb in every beeper that's ever been made and then blew up a subset of them, right? they, this was by all intents and purposes an unbelievable intelligence coup. It was, I understand that people are upset at the notion that you would blow up these things without knowing who might be near these people. Okay.

They're in a fucking war, right? Like they didn't do this in the middle of like Hungary at random. They did this with somebody that's like shooting ballistic missiles to the north side of the country nonstop all the fucking time and has an army sitting there waiting to like come down and fuck with you. There is nothing like to me this was A, unbelievable intelligence coup, B, like

the true payoff of an amazing intelligence operation. You build a manufacturing capability, you figured out a way to get them to source that shit, you made it past any controls, it was distributed to everybody, and then it goes boom, and like, sure, there's some collateral damage, as in all things, like grow the fuck up people, like yes, there are other people who stand next to people.

Ryan Naraine (01:04:33.343)
That's very callous, it's a little strong to say just grow the fuck up because collateral damage and a child might hold a beeper.

JAGS (01:04:38.371)
I think people need to grow the fuck up. People need to grow the fuck up about collateral damage. There is no world in which we play gods and to take perfectly morally rounded out decisions. That doesn't exist. That Mickey Mouse bullshit version of the universe, why don't you just let not bad things ever happen? We all wish that were the case. It's not the case. You don't want them to go and carpet bomb half of Lebanon.

So how about you just let them strategically disable an entire core communication network with like minor casualties along the side. That's a nice, it's a pretty well done thing.

COSTIN (01:05:24.737)
Yeah, I think it was something that someone wrote on X today, which was just imagine the fact that now the people who run the Hasbolag are those who are not deemed important enough to have a pager. Yes.

Ryan Naraine (01:05:38.076)
I beeper.

JAGS (01:05:39.933)

I love the the I don't know if this was true or not, but like the reports that what was it like the Iranian ambassador had like had a beeper on it, which is just fucking hilarious, right?

COSTIN (01:05:52.715)
I think the follow -up was that the next day as things progressed and people were mourning essentially the first round of terrorists who exploded, then the second round started with radios exploding as well.

Ryan Naraine (01:06:06.723)
at the funerals. Yeah, there's footage from an actual funeral where a beeper goes off, where they're actually mourning the guy who died from a beeper.

COSTIN (01:06:13.741)
Correct.

JAGS (01:06:14.242)
Well, the part that where you're not like that, we that I haven't seen drawn as like, I haven't seen a causal link discussed publicly is okay. And then a few days later you get to take out Nasrallah. Like how much of that? I don't know how much of that is a direct corollary to we need to meet in person because there doesn't seem to be any secure comms.

COSTIN (01:06:41.805)
Yeah, beepers.

JAGS (01:06:43.926)
And then like you get to take out this dude you've never been able to take out before in a massive strategic coup, right? Like you can't say it's short -sighted. Like it is just masterful. And I think, look, and not to just like fawn over the Israelis all day long, I will say this is what it looks like when they know to respect an enemy.

and properly prepare and fight them well, which was not the case with Hamas before October 7th and it shows, right? Like they thought Hamas was like a backwater, backwoods, like small issue that could be contained and could be handled in small skirmishes. And when shit really popped off, you saw how flat -footed they were. you know, it's been a difficult entrenched fight. They've always known to respect Hezbollah as an organization that...

Ryan Naraine (01:07:16.409)
Yeah.

JAGS (01:07:38.358)
not only as a terrorist organization with a proper army, but one that could project power around the world, right? Like the Amiya bombing, they were able to carry out terrorist attacks globally and they knew to respect Hasbala and now you see the caliber of capability and thought out, you know, kind of power projection that they can do in those circumstances.

Ryan Naraine (01:08:00.599)
pretty incredible that not only what you're talking about all this thing, but going all the way back and betting that they will move towards beepers because there were warnings from above around cell phones and other types of devices and having the foresight to say, you know what, in two or three years, they're all going to be sourcing beepers. Let me go create a beeper company that makes its own beepers, plant it in Hungary, have a system in place to make sure they order it from here and get it into the right set of hands. mean, if you...

JAGS (01:08:26.977)
telling you,

COSTIN (01:08:27.382)
See where this is going, Ryan. Like they're probably building companies now doing pigeons, right?

Ryan Naraine (01:08:32.682)
This is my thing. It's like how many more of those companies are all around us, like coming to our conferences and high -fiving with us. Like, it's fascinating to me.

JAGS (01:08:33.185)
B

JAGS (01:08:41.985)
Dude, how many there were two people dressed as like Hezbollah comms people at labs con and I won't name them but they did for not I'm glad this didn't happen early enough where I was tempted to show up dressed as a giant beeper or some dumb shit like that but as that's that's right.

Ryan Naraine (01:08:45.8)
You

Ryan Naraine (01:08:58.54)
Instead you were dressed as an astronaut in a big giant white helmet.

COSTIN (01:09:02.369)
What was Baldi dressed as? Like him.

Ryan Naraine (01:09:04.566)
Boldy went as a LIDL delivery guy first, and then he changed into being a prisoner with a 29155 badge on his chest.

Aye, aye, aye. Quickly, just as a quick related story and it's something that we've been following here on this podcast is Apple suddenly dropping its lawsuit against the NSO group, citing fears

that all their data and some kind of sensitive security vulnerability information will leak to the very people that you're accusing of exploiting them. One and two.

citing reports that officials in Israel may have removed relevant interesting documents from the NSO headquarters in Israel. this lawsuit will go nowhere. The landscape have kind of changed. There's some others popped up that has kind of supplanted NSO groups. So we're going to bail on this. Disappointing to me because it was kind of like we had a big strong ally that would plant a flag in the ground and say, okay, let's at least have a balance, a push and pull on this side. Now that they have bailed, what it will...

Cost in your reaction?

COSTIN (01:10:07.159)
Well, I think everything kind of revolves around US politics. So here I probably think there's a lot of lobbying involved, a lot of money involved. Don't forget the fact that, because, I love those, the aliens, the Dutch, of course, must be involved. But I was thinking that there's probably not...

JAGS (01:10:18.846)
conspiracy custom.

COSTIN (01:10:34.721)
any good technical reason to drop the lawsuit. The only good reason to drop the lawsuit would be financial. That simply they don't want to pay the lawyers anymore. By the way, we were in that situation in the past when, let's say in a similar case with cyber criminals, essentially the lawyers were quite expensive and the question was what do get out of it? Like the best case scenario is they get convicted and they go to jail, right? And they did.

Ryan Naraine (01:10:41.923)
Not a problem Apple has.

COSTIN (01:11:04.447)
Is it still like any point further to continue in this direction or not? And in case of NSO, they're sanctioned, What can happen? Like what's the worst thing that can happen to them on top of sanctions? Maybe, you know, they got the outcome they wanted and from here on it's up to the US government if they want to make it worse for NSO or to make it better for NSO. So we'll have to see.

JAGS (01:11:33.317)
what to think about this one. It sounds fucking stupid for what are probably some of the most expensive lawyers on earth to suddenly realize they're open to discovery. Like, what the fuck are you talking? That's nonsense, right? Like you guys knew that was an issue. It's like part of the admirable aspect of this is well, you're clearly willing to open yourself up to discovery because you think there's something greater to be gained. And it

Ryan Naraine (01:11:45.467)
Yeah, that's nonsense.

COSTIN (01:11:49.003)
Yeah.

JAGS (01:12:02.564)
I'm wondering like what changed, it's hard to say that because I don't understand Apple's strategic priorities in that lawsuit in the first place. And if anything, kind of look at like face like Metta's attempt at going at NSO was sort of more significant, more interesting. But yeah, it seems kind of like a weird flash in the pan kind of thing. And we've known that there's other companies, we've known that NSO is going to be sanctioned. We've known like all these things like

None of that changed. So what exactly made this less savory for you? And if the big discussion is simply like, well, other people have replaced you. It's like, OK, well, when are you going to sue Paragon or whomever else? Like, what's the deal? What's the problem? Right. Like, are you establishing a paradigm here where you say, well, one of the reasons you should not want to be one of these companies is the richest like one of the richest companies on earth is just going to legally hound you until the day you die.

Ryan Naraine (01:13:01.005)
That was the hope, right? That was the hope from some of us who were anti -NSO type technologies is, hey, here's a rich vendor with mountains of lawyers that can throw at people to say, hey, you're not gonna fuck around on my platform and use my cloud services and you're not gonna put my, like this is the stance Apple was making and now they've disappeared. You think it's tied to the conflict? Because NSO is still a very important group and company in Israel providing very important technology as part of their war effort. It's publicly documented, it's publicly, I mean.

COSTIN (01:13:02.444)
Mm

JAGS (01:13:26.65)
Supposedly, supposedly. mean, yeah, but they jumped into trying to become more valuable the day October 7th happened. that's not necessarily the case.

Ryan Naraine (01:13:35.649)
Fair enough but still an important piece of technology for...

JAGS (01:13:39.917)
Sure, sure. mean, like, it's not the only one. I don't know. I don't understand what's going on here. And that sometimes is just the fact that, of course, we're ignorant to many things, myself especially. Sometimes it's due to the way that decisions are made in the Valley. And like, maybe

this project didn't survive someone's perf cycle. And that may very well be what determined this change.

Ryan Naraine (01:14:09.514)
Alright gentlemen, I think we'll it there. We're an hour and 15 minutes in. I want to end with some shout outs. Anybody who want to give some final shout outs to Juan? What is coming up next for you?

JAGS (01:14:21.036)
have no idea. I'm so I'm, I'm starting to kind of pull my foot off the gas pedal and like change, you know, how I'm, how I'm using my time and my efforts and so on. as a bit of the last hurrah on that front, I will be at virus bulletin, next week, just presenting some of our, rust research, trying to, Nicole and I are trying to rework.

Nicole fishmine from an teaser and I are trying to rework how the, the plugins and stuff work because in true hex race fashion, bless their souls. they have changed Ida Python all over again for Ida nine. it's not a bad thing. Like they, they, they finally standardized, Ida Python into an external library and like a bunch of things that we've been asking them to do. They're changing their pricing model for Ida pro completely.

And Ida 9 is coming out very soon and we've been using the beta and it's really cool, but it also means that all the stuff that we built to try to fix the rust reversing problem needs to be re -engineered a bit. I kind of saw this coming. So like we use the middleware library called feature proof and I now need to fix that library so that it actually works for other people. So there's like a bit of work that we're trying to kind of sort out in that so that we can release some of these tools. And then if I'm honest, I am

trying to back away from the day -to -day stuff for a few months and try to start writing again. I need to get back into the book. I need to start publishing things. Like even Kostin mentioned like that, that keynote, was a wonderful moment of like emotional openness about a problem, but it wasn't a comprehensive treatise on shit. And it didn't, I didn't get to cover like maybe 40%. yeah.

Ryan Naraine (01:16:06.441)
still also lube or paper.

JAGS (01:16:10.022)
Well, anyways, with that sense of overwhelm, that's the kind of things that I hope to be paying more attention to in the near future.

Ryan Naraine (01:16:17.519)
Shout out to Helen and best of luck to all the folks at VB speaking and going there. It's still a very important conference, a big deal for folks in Europe, especially for folks in Europe to have access to this quality of presentation. So good luck to those folks. Gustin, some final shout out words from you.

COSTIN (01:16:33.271)
Well, shout out to our good friend, Victor Manuel Alvarez, who keeps working, getting Yara X, speaking of Rust, to a stable version and closer and closer to the release date. I think that's a very interesting new project, very powerful, very important for the future of Yara. At the same time, I wanted to say, you know, shout out to Juan, of course, because of his work with Rust.

Nowadays the amount of things that I see compiled with Rust, written in Rust or Golang, it's just crazy, it's insane. Like most of the malicious tools malware that I see are actually a nightmare to reverse and a nightmare to write the other rules for. And yeah, you guys are doing God's work. So thanks for that.

Ryan Naraine (01:17:26.329)
And from my side, just to put a final bow, we started talking about LabsCon to close on LabsCon. big shout out to Courtney Duff from Sentinel One, who is like the mother of LabsCon, kept everything together, did amazing work. mean, we've told her in person, I just wanted to document it here in the podcast. And congratulations to Chris St. Meyers, your new deputy, Juan, who will help you kind of straighten out your work thing. So congrats to Chris St. Meyers.

JAGS (01:17:49.052)
Yes.

Ryan Naraine (01:17:53.123)
Shout out to all the LabsCon organizers, sponsors, people who attended. We just had some sad news as well last night. It's like it's been an overwhelming emotional experience, totally so. With that, and on that very, very high note.

JAGS (01:18:05.072)
Well, wait, wait, wait, you gotta say it though. So for folks who might not know, like Jeff Wade from Solace, who have been really good friends of ours, have been there from the first LabsCon and have always sent like a nice contingent of folks. Jeff was with us at LabsCon, actually dressed as a banana, dancing banana for the gala dinner. And then we heard he sadly passed away a few days ago.

You know, a lot of sort of bittersweet, like mixed emotions. Glad we got to spend that time with him. I didn't know him very well before that, but he was a very kind guy. And yeah, just, you know, one of those moments of reminder to appreciate the opportunities to be with our friends and these people that support us and that we care about and take a minute to stop hunting and give your buddies a hug at least. And just appreciate that we have these moments together. So...

Yeah, just a huge shout out to the Solus team and his family. I hope they're all well and all this.

Ryan Naraine (01:19:09.213)

Absolutely, sending along the best of vibes to our other friends at Solace who hung out there with us. I mean, these guys have been a key part of our conference and you know, the guys' family as well. It's just kind of one of those emotionally overwhelming things that I'm processing and trying to deal with. So thank you guys. We'll talk again next week.

JAGS (01:19:22.17)
Mm

COSTIN (01:19:26.529)
Thank you, ciao.

JAGS (01:19:26.736)
Thanks everyone. Bye.