Episode 37: Three Buddy Problem

Revisiting the Lamberts, i-Soon indictments, VMware zero-days

LISTEN:
https://securityconversations.com/episode/revisiting-the-lamberts-i-soon-indictments-vmware-zero-days/

Cast:

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

JAGS (00:00.202)
I appreciate that there's that kind of ambiguity. We were discussing what would you do as a naming convention? I hate the standardized naming conventions, but I remember back in the awful recorded future days, I just kept asking them, why don't we just do food? It's the same ambiguity, right? You kind of know where it's from, you kind of know who eats it, but you don't know. There's nothing keeping Ryan from cooking Thai food.

So like as far as an APT naming convention, like I think Hegel was talking about the disappointing curry, APT. I'm saying like it's the same ambiguity of like there's a vague regionalness to it, but you know, it could be New York.

Ryan Naraine (00:32.517)
lord, just make it stop.

Ryan Naraine (00:42.831)
nightly.

COSTIN (00:44.115)

I'm down. It beats a weather phenomenon.

Ryan Naraine (00:49.071)
Alright, let me start the show. Good morning everyone. This is Ryan from the Three Body Problem. I'm here with Juanito and Costin checking in for episode, what are we up to? Episode 37 on what is an International Women's Day, very much celebrated in Europe, Eastern Europe. Costin, what is your plan for International Women's Day?

JAGS (00:54.222)
Please cut that.

COSTIN (01:11.575)
stay alive no no no like in here there's a lot of holidays it starts with the four teens which is St. Valentine's Day then there comes a Romanian version of St. Valentine's Day the Drago Bete then comes the first of March the Merti Shor in which men give women some kind of small tokens for the spring and like little flowers

Ryan Naraine (01:13.473)
Stay alive. Are you that morbid? Like what's going on?

COSTIN (01:41.107)
except for some villages in the north of the country where actually women give men small flowers. It's interesting. And today is March 8th. So like it's a number of different holidays. Yeah, it's a number of different holidays one after another. And by the end of by the end of this cycle, you need to survive. That's a feeling.

JAGS (01:53.112)
Who gets flowers?

Ryan Naraine (02:04.994)
But this is a big day, right? Like this Women's Day is a big thing in Europe. I remember when we were back at the old mothership, mean, Kaspersky used to shut down for this day.

COSTIN (02:08.214)
It's huge.

yeah.

Ryan Naraine (02:16.386)
It's kind of like a big holiday.

COSTIN (02:17.862)
It's a holiday course, like a national holiday actually, except today it's a Saturday.

Ryan Naraine (02:21.134)
No. Well, shout out to all the women listening to the show. Happy Women's Day. Let's start with Kim Zetter. We'll start with Kim Zetter's reporting on the US-Russia stand-down order, something we touched on briefly in the last episode, but was kind of up in the air. We weren't clear on the reporting. What Kim did was go read all the stories and kind of put together a piece that not necessarily clarified, but explained all the different reporting. And a big takeaway.

COSTIN (02:26.922)
Happy Women's Day!

Ryan Naraine (02:50.338)
was to me, she read a story from the record, a story from the telegraph and the Washington Post and did a lot of our own reporting, checking in, checking out about what this stand-down order meant. It feels like Juanito, do you have any insight at all into what really happened?

JAGS (03:09.982)
not nearly as much as, as Kim or, I mean, the way that this is sounding to me, like talking to some folks who'd been there, back in the day who kind of understand how things work, there's some element of this that standard procedure in the sense of if you're having some kind of like diplomatic overtures with a country or like in the middle of negotiations.

I'm told that a certain amount of like stand down is normal because you obviously don't want to, you know, accidentally mess up. Yeah. Undermine what's going on. So I think there's a certain amount of this that's at least on the military side is standard procedure and it's being kind of like overblown. I think the difficulty here is that

Ryan Naraine (03:50.058)
undermine conversations, right?

JAGS (04:08.129)
the messaging we get from the administration is almost like purposefully vague. it's, and some of it, whether it's either things leaking from the bottom end, which received the message, which tells you something because it's like the message they're getting is sounds like it's, you know, it's a lot more, over the top and, and, definitive, dramatic,

Ryan Naraine (04:32.526)
Dramatic.

JAGS (04:35.542)
And then you get sort of this ambiguous clarifications and then, this isn't happening. No, this is normal, but no, actually it is happening, but it isn't at this place, but only if it's malicious, but not if it's the planning, but it's like, so look, I keep saying this. I, I do not mean to excuse being uninformed or, or unengaged in the civic process, but the amount of like purposeful roller coaster riding that seems to come with.

you know, political messaging these days is making me disengage. And I understand that that's part of the point, but I just like, need a TLDR, bro. Like I cannot live and die with like, today we're going to like put people in camps. No, tomorrow. No, we're not putting them in camps. No, the next day it's like, yeah, but they're nice camps. No, the next day it's like, no, actually they're, terrible. It's like the fifth day it's like, no, we'd never do that. You know, it's like, okay, I'm to wait a week and like,

Ryan Naraine (05:28.716)
Bye.

JAGS (05:32.59)
And I think this actually got brought up in the the All In podcast, which I finally I finally listened to a couple of episodes of the All In pod. And I want to kind of talk about this a little bit because you're the one Ryan, you're the one who got me to listen to this. But like they I think it's one of the one of the host is like instituting like a 48 or 72 hour rule. It's like I'll wait 72 hours before, you know, actually believing that any of this shit is happening, like because there's so many announcements of like potential whatevers.

Ryan Naraine (05:59.497)
Right, and announcements and statements that are part of negotiations. It's like the statement is the negotiation. So it feels like there's whiplash everywhere, and the 72 hours gives you a chance to kind of filter what actually happened and form a thought.

JAGS (06:14.478)
There's the naivete of it, right? while we're on the topic of sort of the whole Ukraine thing, right? Like, look at the political arc of what ends up happening with that, that shit show with, with Zelensky in the Oval Office. Everyone sort of freaks out about the, discussion itself and the change in tone and whatever. But when you look at it now, what is it, like two weeks later, right?

It's a series of ridiculous, like overblown overtures that might have been a negotiation before, right? You might have done it behind closed doors and saying, look, this is what we want. This is what you need. This is how we need to get there. You guys up for it or not. And like the public stuff can be just choreographed. Now instead it's like, no, let's have those blowouts in public signal to the Russians, force the hands of

the Ukrainians freak out the Europeans and hope that people make the moves that that you've been asking for for what would it be now like 10 years or eight years? You know, this since the Obama era, right? Like Europeans paying more for NATO. What are you going to do for your defense? Blah, blah, blah. And instead of trying to have a soft negotiation on it, I'm not saying that I appreciate what

what's going on here. I'm just saying like you turn it into this like public pantomime that forces everyone to come along and look at look at what happened at least where things seem to be

now with Ukraine is I mean they got what they seem to be getting what they asked for even the most ridiculous parts of what they asked for. So you see that and like I want to express some level of admiration for the political maneuvers that are happening.

but I don't want it to sound like approval or excitement. And that's kind of like a difficult thing right now for me where I'm like, look man, JD Vans pulled that bullshit. was, everybody was horrified. But then you look at how things play out and you're like, well, it works for what they seem to want, whether you agree with that or not, but it works for what they want.

Ryan Naraine (08:26.017)
It worked.

Ryan Naraine (08:34.88)
Yeah, just to loop back onto this story, Kostin, we got a tweet from DoD Rapid Response that says, be clear, Secretary of Defense has neither canceled nor delayed any cyber operations directed against any malicious Russian targets, and there has been no stand-down order whatsoever from that priority. Do you see relevance to the word malicious there?

COSTIN (08:53.598)
the emphasis? yeah I thought it was the typical kind of PR speak that we've learned all these years so we know it very well how to use it my sound sounds low

JAGS (08:55.5)
Malicious.

Ryan Naraine (09:03.256)
Your microphone sounds very low to me. Is it? it? Yeah, yeah.

JAGS (09:07.694)
Yeah, I think it's just a little far away, Kostin.

COSTIN (09:09.936)
I am like in the microphone when I am in the microphone

JAGS (09:11.982)
When you're in the microphone like that, it's good. Right in it. In NPR this shit. Just NPR it. Just ASMR this stuff.

Ryan Naraine (09:16.312)
Go ahead, go ahead. Go ahead, go ahead.

COSTIN (09:17.354)
That's weird.

So I think it's just maybe PR talk in a manner with the emphasis on malicious in the sense that I would read it as yes, some operations are on pause, but not the ones like against the malicious targets or the serious ones. And again, as Juan was saying, it kind of makes sense to put some things on hold. Just imagine that you blow up some gas pipes in Russia or

Ryan Naraine (09:38.038)
and some weird people, right?

COSTIN (09:49.003)
shut down some oil fields during these negotiations even by accident like maybe an implant goes offline or mistakenly triggers I know the chances like one in a million but nevertheless I think would be good to have some kind of understanding that we are temporarily not doing anything very bad and very offensive against the targets if we are negotiating with that with that country and the fact that

Here in Kim's article, there's also an interesting statement from Nakashima in the sense that, yeah, they were not kind of standing down the bigger Russia, well, operations against the Russian ops. And then something along the lines that they weren't engaging in these types of operations against Russia anyway. So I was thinking like, why

JAGS (10:47.326)
Uh-huh. Uh-huh. Uh-huh.

COSTIN (10:47.73)
why weren't they engaging against these types of operations right

Ryan Naraine (10:50.488)
Well, wait, me set it up. Costin is referencing Ellen Nakashima, who Kim Zetter spoke to. Kim spoke to Ellen directly. And Kim caught Ellen saying, was an order and it was issued to prevent an irritant to the talks. So they're standing by this story. But then she made, this is the Nakashima quote that stood out to me. It's like the real story is that they weren't doing much to begin with against Russia. So there was not that much to stand down on.

COSTIN (10:58.016)
correct correct and Kim quotes Ellen in the story

COSTIN (11:06.92)
Mm-hmm.

COSTIN (11:12.552)
Hmm, that would do it. Huh.

JAGS (11:17.87)

I'm sorry. I'm sorry. I will. So that's, I started laughing there because I was, I was waiting for it. Like my notes, my, I literally like my piece of paper just say, are there any operations in the first place? Like I've said this in the podcast before and I've gotten a lot of pushback, not just from you guys, but like listeners where I'll say something like, well, are they fucking doing anything? And people will go, of course they're doing something.

COSTIN (11:20.874)
That's a true question.

COSTIN (11:44.256)
Mm.

JAGS (11:47.308)
We have all this power and all this whatever and all these teams and all this capability and I go, yes, but are we doing anything? Because part of the problem in the U.S. has actually never been a lack of capacity, a lack of capability, but there's a wave. Well, no, no, no, no, no, no, no, no, no, no, it's not the laws. It's a sense of sort of wavering intent that

Ryan Naraine (12:01.878)
It's all these lads, right?

JAGS (12:14.878)
is bureaucratically dismantled layer by layer. you can, know, Ryan, you're the, you know, you're part of the administration and administration, you decide that like, we need to conduct some cyber operation, even if it's positioning or whatever against like Russia. And you guys assess that it's a good thing to do and you have the capability to do it. Cool. All right. How do you actually get approval for that authority to conduct a cyber operation?

Ryan Naraine (12:43.042)
That's what I talked about your laws. This is you going into there is no free for all.

JAGS (12:45.102)
But it's not laws, it's process. There's a difference between law. Legally, the authorities exist and Cyber Command exists and has the authority to do these things. Legally, it can do them. Procedurally, in the US though, you still have this bullshit where it's like, you know, we think we should do this and it fits our strategic objectives and we can do it. We have the capability.

Ryan Naraine (12:53.688)
the lawyers.

JAGS (13:12.982)
And in order to do it, we need seven signatures that go up through all of like DOD, then it goes to like, you know, Secretariat of Defense, that State Department gets to have an opinion, see, no. But dude, you're not, you're thinking about this like it's like seven functional organizations

who sit down together and have a conversation for the good of the country. Instead, it's a bureaucracy, a paper pushing that goes all the way up to the fucking president.

COSTIN (13:19.04)
Mm-hmm.

Ryan Naraine (13:23.734)
as it should.

JAGS (13:41.304)
So like actually pulling the trigger is like this near impossibility. And that's actually one of the few changes during the first Trump administration that people seem to be actually happy about. That then you spent years in the Biden administration with people like Anne trying to revert, which is the Trump administration kind of like undid a lot of that layering. They were just kind of like, fuck it, just go do what you got to do.

And then the Biden administration was trying to be like, no, we need to put that genie back in the bottle. But that's a really long way of saying to what extent has like covertness kept us from seeing what we do versus it's hidden the amount of dilly dallying that's kept us from doing anything all that significant, at least with effects.

Because I'm sure we're spying like fucking crazy. know NSA is out there. You know CIA is out there. Like we're spying. That's just the way it goes. But like there's a whole range of other shit that you do with cyber and that our adversaries and other folks are perfectly comfortable doing with cyber. And I'm wondering to what extent we've done fucking any of it, know, Stuxnet aside, not because we can't, not because we shouldn't, but because bureaucratically

It just never got to the trigger pulling point of things.

Ryan Naraine (15:11.68)
One of the weird things in this story as well is that our favorite government agency, CISA, got dragged into it. There was a report that CISA was part of the stand-down order and CISA actually had to issue.

COSTIN (15:19.446)
Stand on.

JAGS (15:20.564)
Now we stan Sisa. Now we stan them. we, you know, now we stan Sisa.

Ryan Naraine (15:23.596)
Now we stand CISA, because CISA had to put out a statement basically saying there's no change to its stance on detecting and disrupting Russian APTs. There's been no change in our

posture. Any reporting to the contrary is fake and undermines our national security. So it seems like CISA is doing a lot. They are continuing to do a lot. Why do you laugh, Costi?

COSTIN (15:40.681)
Hahaha

JAGS (15:43.446)
We stan CISA now. We're cool with CISA. We admire their work.

Ryan Naraine (15:48.16)
So I mean, there's a general feeling that none of this got caught. Sisa didn't get caught up in any of this and any sort of like.

COSTIN (15:55.009)
Do you remember last week we talked about who's gonna be the first company, private company to publish a report on Russia? Have we seen any reports on Russia this past week? Not yet, not yet. Okay, we're still looking. Let's see. Fair enough, fair enough. Yeah, 11.52.

Ryan Naraine (16:07.31)
Not yet, not yet.

JAGS (16:10.862)
We did Belarus. Is it close enough? it? Give me a Russian APT. I'll publish it right now. Let's see.

COSTIN (16:19.702)
Are you an American company? Okay.

JAGS (16:22.166)
Yes, we're a publicly traded American company. We're fucking apple pie and shit. all right. And we'll publish on whatever right now. Funnel cake, funnel cake, carnival funnel cake. Sorry, that was Lambert's blue Lambert inside joke. Good man, good man.

COSTIN (16:25.406)
Okay.

COSTIN (16:32.022)
Funnel cake.

Ryan Naraine (16:41.664)
It sounds like you and your food naming APT again. I smell, I heard fun.

JAGS (16:45.856)

I'm sorry. That was what they called their so like, okay, just to set it up because like it's kind of shitty that we have these inside jokes for the blue Lambert. One of the interesting things that led to some of the attribution stuff is that the encrypted configurations included crypto names for operations. So they had these like names in them that were supposed to exemplify like this implant is related to this up. And what was really funny about these is like some of them

COSTIN (16:49.032)
You

JAGS (17:14.956)
were so American, like so American in their context that like no European, maybe not even a Canadian would like know, like it was like references to NFL lip syncing videos, like a double-sided Scooby snack was one of the operation names, Carnival Funnel Cake was another one. like, it's funny what takes you, yeah, it's funny what takes you to like.

COSTIN (17:38.57)
Flash garden.

JAGS (17:43.768)
to attribution, at least vibes-based attribution. It's like, I mean, who else is gonna do this?

COSTIN (17:48.823)
it's a pity we aren't seeing much stuff like that anymore like the kind of stuff that you see nowadays it's much more boring there's no easter eggs no dead food like for another cryptical reference there's... wow

JAGS (18:00.0)
Deadfoot. Yeah, I have that one here actually It's on my wrist

Ryan Naraine (18:05.282)
So wait a second, wait a second. Can you guys kind of just help me understand on this reporting, the Lamberts, have we lost complete visibility? Like the last report I saw on Lambert must have been what, five years ago?

COSTIN (18:26.238)
Maybe more.

Ryan Naraine (18:27.66)
Maybe even more, a combination, any, any.

JAGS (18:28.158)
Well public or private public or private so let's start there I Think privately there's been what was the last things were? Maybe like three years ago. There've been there were some suspicions maybe for

Ryan Naraine (18:41.357)
Yeah.

COSTIN (18:42.742)
Three years.

from home.

Ryan Naraine (18:45.55)
Did they go dark? Is there no longer any visibility as people stop looking? Like, what's the status of...

JAGS (18:50.168)
So let's do a bit of background here and I think this is where people get kind of annoyed with us about like really pigeonholing right away. So like the Lambert's constellation is essentially the...

Ryan Naraine (19:02.59)
I've wanted to tee up this conversation for a long time. Go ahead.

JAGS (19:05.364)
I know. Well, and this is one of those where we should just do originally discovered by FireEye. So they, they, yeah, that's true. So, so black Lambert is the first sighting of any of the Lamberts discovered by FireEye. FireEye reports to Zero-Day, but doesn't report the malware. Oddly enough. the malware was super fascinating, like interesting in memory implant, found at a nuclear agency, I believe, at an interesting time.

COSTIN (19:06.006)
Originally discovered by FireEye, like originally discovered by FireEye, Black Lambert.

JAGS (19:35.192)
doing interesting things. It was around the P5 plus one negotiations. And because of that positioning and because of the kind of malware that it was, remember originally people thought it was a Dooku variant. Correct me if I'm wrong, Kostin. So eventually, this becomes this big Lambert's constellation, as we called it, because

COSTIN (19:49.104)
mhm mhm yeah yeah because of the exploit

JAGS (20:01.58)
It was very hard to parse the malware, like the different variants and strains and to jump from one thing to another. So it became this big project over like maybe 18 months between like things being found and things actually being like properly pieced apart and reported where we

just ended up color coding them. So you'd get, you know, black Lambert, blue Lambert, red Lambert, violet, purple, green, et cetera, because that was easier in that way. And it was a really

Fascinating and difficult like it might be one of the most difficult APTs to like go from one family to another to connect one type of op to another precisely because I think it's an APT that reflects its organizational culture where tradecraft is of paramount importance because when you fuck up your tradecraft people die and like that you see it in how the the

not just how the operations are carried out, where there's no extraneous infections, there's no like, we landed on some random person's computer and we leave the malware there just because, just maybe whatever. Like, no, they would clean everything up. They were super careful, but also in the structure of how the malware is built, which I now, like with the years, we kind of started to understand a lot more about like why it was so hard to go from one to the other. So that's where like the marble framework discussions come in. Like the Chinese have been trying to kind of make that

a weird misattribution thing, but in reality, what it is is they systematized ways to mess with attributory components inside of the malware. They systematized ways to scramble some of the structure of the malware. They systematized ways of scrambling, of changing the crypto in the malware at each time it was used. And all those things made it extremely hard to go from one to the other.

And just to like for the punchline in case it's not obviously clear, this eventually when Vault 7 comes out, we get very clear confirmation that this, that the Lamberts are like clearly related to the CIA. Like clearly, just because Vault 7 like ultimately ends up kind of clearing a lot of that up.

Ryan Naraine (22:15.478)
And what was that connection with? Is a specific Vault 7 piece of thing that made that clear?

JAGS (22:19.49)
There's a variety of them. There's a variety of them from like command and control server, mercuryvapor.net, actually redirects to my blog now. There's a couple of connections in different like flux wire and like some of these different components that actually were detailed in there. And then there's some really hilarious ones like there are forum

like internal chat posts where there's discussions of attribution fuck, like moment, the operational fuckups, one of them called Blackstone, which is in the PDBs for one of the Lambert samples. Like there's a lot of one-to-one connections there. And I think my favorite thing in Vault 7, like favorite, is there's a forum discussion, an internal forum discussion where they are basically,

doing a post-mortem on the equation group discovery. And the discussion is fucking phenomenal. It's fascinating. It is actually the most telling thing about like the equation group attribution because everybody mistakenly attributes equation group with NSA like one to one.

And in reality, it's like a series of tools that were used in certain like interagency contexts and contractors and stuff. like saying one to one NSA to equation group is not quite right, like not fully right. But that's something they discuss.

Ryan Naraine (23:55.191)
And it's also why triangulation attribution is a little...

COSTIN (23:55.628)
now you're going like a soul typhoon ghost emperor on us

JAGS (24:03.918)
I mean, but organizationally, it's that, right? Like when you build a series of tools and some of it might be used by like the DEA, some of it might be used by some kind of like JSOC or Special Forces operation. And then some of it is used by by CIA, some of it, and a lot of it is used by NSA or a lot of it is developed by NSA. To us, it's one big threat cluster, especially because the infrastructure is systematized, not segmented, all that stuff.

But that's why we hedge our language. People fucking hate it that we're like, well, it looks like, and it kind of seems to be this, and we sort of think that it's aligned in this whatever. And they're like, why do you guys parse your terms so much? It's like, because honestly, the granularity of what we can tell compared to the possible and actual arrangements of how this shit works, they just don't match.

Ryan Naraine (24:57.326)
Cost 10 without Vault 7, did we already have the attribution piece locked in or did you need that to finalize?

COSTIN (25:01.91)
No, I think actually it was Symantec who made the connection and they were the first to publish on this attribution if I remember correctly with they call it Longhorn if I remember correctly and with the connection being the one called Hive was apparently the same as what we were calling the Pink Lambert

Ryan Naraine (25:15.181)
Longhorn?

COSTIN (25:27.156)
Yeah, well, that was like an interesting piece of research from Symantec and going back to your original question, like did we lose eyes? I think nobody knows, probably nobody knows at the moment if these things are still in use, where they're in use or how they look nowadays. Most certainly, I don't have the means to look for anything of sorts. I'm just curious if Symantec still sees them while...

Nowadays Blackberry, Blackberry I think they were Broadcom, Broadcom. It's a bee. And would be interesting, mean even if Sentinel-1 sees any of these things, although it might be very difficult because I would assume despite all this...

JAGS (25:59.072)
No, Broadcom. Broadcom.

JAGS (26:11.422)
We've seen so like I we haven't seen I can say it right here. We've never seen them in the wild I I've ran into variants of Lambert's that have just kind of popped up here and there in like VT context But nothing crazy and like some of it It's just like an old sample will pop up some like white Lambert thing from like, you know Korea, you know, like okay. This is from like six years ago, right? Yeah

COSTIN (26:23.945)
Mm-hmm.

COSTIN (26:34.31)
Mm hmm. Yeah, that's what I mean, because I you need visibility into maybe China, Russia. mean, despite all these reports and denials of reports and reports of denials of the denials, I think there are still operations going on malicious against malicious targets. Also, it's difficult to say what is malicious nowadays.

Ryan Naraine (26:45.804)
Middle East.

JAGS (26:48.909)
Middle East.

Ryan Naraine (26:52.014)
You

COSTIN (27:02.806)
I still think there's operations going on but you would need visibility into Russia and China in order to spot them.

Ryan Naraine (27:10.058)
When you say you would need visibility, you would need to have an agent installed on a target machine in one of those very, very specific places, right? Yeah.

COSTIN (27:15.838)
yeah russian government russian military chinese military mss and so on

Ryan Naraine (27:21.976)

So which means we're always...

JAGS (27:22.07)
Also, like a good, a good, and you're talking about it, not just an agent, like you need something that's doing like behavioral and memory, because you're not just gonna see it, like it's not gonna show up in a fishing lure or some bullshit.

COSTIN (27:29.802)
Mm-hmm.

COSTIN (27:34.934)
This will never be spearfishing. Yeah.

Ryan Naraine (27:36.13)
which means we'll stay dark. mean, we...

JAGS (27:39.606)
Well, there's another element to this that I've like, I've sounded cagey about this before when we kind of get into some of these discussions, but it's not out of any kind of like inside knowledge as much as like, I think the Lambert's is a really interesting, insane like amount of activity. And it's obviously an eye like a tip of a bigger iceberg that we will never because of their successes, we will never be able to recreate the larger set of activity to their credit.

But I also don't see that being the only toolkit or like the only type of operation or the only outfit that's working out of that side of even just that side of the house. So like we got visibility and it and it's we learned a lot and it's fascinating. But I also wouldn't rush to pat ourselves on the back that we somehow saw everything they had or even like.

I'm sure that there are multiple streams of what we would name APTs that fit each one of these houses, not just one of them. So even if we went dark on this one because they shut that shit down, it's because they had other stuff. And even by nature of how the Lambert's worked, like what one of the things that makes the Lambert's fascinating is that it was obvious that there were multiple like parallel lines of development for platforms at the same time, which is extremely rare.

in those types of like mechanized, like mega APTs, when you look at the development of the equation group platforms, you can put them in a timeline. And it's like, this one was there for three years, and then you can see that the other one kind of overlaps and then is there for two years. And then the other one kind of overlaps and is there for three years. And it's like, it shows like cycles of investment over time, but they're essentially like, there's one thing that replaces the other, that replaces the other.

With the Lamberts, would have two, it seemed to be at least two development groups and like you would see three or four platforms operating at the same, like in sort of parallel tracks. And I think that speaks to, they're definitely not putting all their eggs in any one basket.

Ryan Naraine (29:47.168)
If I were to read a one Lambert report, which color should be the one that's the most explosive, interesting, fascinating?

COSTIN (29:57.467)
Hey, so it will be difficult for you to read any of these reports, right? Because only very few are available publicly, but I would start at the very beginning, the Black Lambert. Yeah. Because it's a mix like from delivery, from the spearfishing PDF, all the way to the implant installing in memory and leveraging hard-coded proxy server from the targets organization, right?

JAGS (30:09.302)
You have to start with black. have to.

JAGS (30:24.886)
Internally. Yeah.

COSTIN (30:27.302)
So I would start with that and I think that based on the different modules and libraries from that people created a lot of interesting signatures which led to the white Lambert and many others.

JAGS (30:41.486)
I think you have to start with black culturally, organizationally, attributionally. Blue is the most interesting. That's I think maybe the weaker, like most telling one. From a pure like early development standpoint, gold was fascinating. That's one that we find after the territorial dispute leak. So gold was a very, very early one. If I remember correctly, it was like 2006 or something.

COSTIN (31:03.711)
Mm-hmm.

COSTIN (31:09.76)
Six, mm-hmm.

JAGS (31:11.424)
And it's like POSIX compliant in a way where like it's Windows malware, but it's clear that it was built to be cross compiled for like Unix, Linux stuff. like it starts to show you like organizationally how brilliant some of this development is. And then white, like from a technical standpoint, like I thought white Lambert was fascinating. Like it was like, how do you coordinate multiple infections inside of a single enterprise?

And like you have like this like unicast, multicast like protocols and like all this. It's fascinating. I mean...

Ryan Naraine (31:43.906)
and all of this is still hidden privately.

COSTIN (31:47.572)
I think so.

Ryan Naraine (31:48.621)
Is there any public reporting, if I want to talk to someone in the audience, reaches out and say, what, how can I go, based on what's publicly out there, what do I read?

JAGS (31:48.792)
I am.

COSTIN (31:51.775)
Mm.

JAGS (31:55.598)
Well, we published, we did publish a blog about the Lambert's constellation. It just wasn't all the full detail, but it's kind of a condensed like overview of the stuff that we had gotten up to like back at the mothership. like in Securalist at Kaspersky, like there's, is a blog on the Lambert's, like I think it's called like Unraveling the Lambert's constellation or something like that. And then Symantec did their

Ryan Naraine (32:06.67)
Who's we?

Okay.

COSTIN (32:15.35)
Mm.

Ryan Naraine (32:19.362)
You should read the Longhorn report, right?

JAGS (32:21.324)
Yeah, TamanTech did their Longhorn one, which actually covers some other interesting stuff like the Mercury Vapor thing and some of the overt connections are there. Then that one of the few but really good Chinese ABT blogs was that I think it was the Reddrip like Reddrip team on one of the Lamberts. I can't quite remember. It was a long time ago.

I think that might be all of the reporting. There might be some tidbits here and there, like small blog posts, but I don't think that the wealth of what's in the Kaspersky private reports for that stuff is fairly unique.

Ryan Naraine (33:01.324)
And that's only available to paid customers of their private reporting service, correct?

JAGS (33:04.534)
Assuming you can even pay them for it at this point, right? Like I don't know how you even go about that, so.

COSTIN (33:06.922)
Hehehe.

Ryan Naraine (33:12.398)
I remember when we were talking about triangulation on an earlier episode, I flagged attribution and you both corrected me. What's the consensus on attribution for that one? What's the public consensus on what the attribution is for triangulation?

COSTIN (33:28.539)
No attribution, think. The consensus is no.

JAGS (33:30.764)
Well, no, think the consensus is like people, the rumant, vibrant consensus is that it's the US and what you get with people.

COSTIN (33:39.402)
Mm.

Ryan Naraine (33:42.346)
And I bring that up because of what you just described about this kind of sharing of resources and so on.

JAGS (33:46.274)
Well, it's why I don't like any of this shit. Like, I think people rush to cite organizations and it bothers me because it puts you very close to like the tinfoil hat, like schizophrenics who stop taking their medication side of the house. And that's why like people like Jonathan Data were doing so well, like, you know, scamming everybody.

Ryan Naraine (34:09.142)
Right, but we got people listening to the podcast as the first thing that pops into your head is who is this? And that's the last thing that you guys get to deliver.

JAGS (34:14.626)

But, but that's my-

Well, but it's the last thing we get to deliver and the last thing we want to deliver precisely because I think if you're intellectually honest as a researcher, you know how little you know. So with something like Optry, yeah, yeah, yeah, yeah, it's because of how little we know. Well, with Optry, I think that what everybody assumes is like, well, this is going to be CIA. But like,

Ryan Naraine (34:29.462)
Is that why we're hedging so much on this specific one? Because we don't know.

Gustin is smiling there.

COSTIN (34:36.884)
I'm a...

JAGS (34:43.508)
I really hate this kind of shit because I don't disagree that it looks Western. I don't disagree that it might be the US, but I don't like us simplifying things because I think we've made huge mistakes in the past on the basis of those oversimplifications like Reagan, right? In the very beginning, there was this assumption that it was like one particular org or two particular Five Eyes orgs and whatever. It turns out the answer, which is far more complicated than anything we could have come up with, which is

It's four eyes in a development, shared developmental framework that is compatible with the equation group way of building things for cross compatibility, but not equivalent one to the other, which is.

Ryan Naraine (35:24.438)
Where can I read that? Is that available publicly? Like that one you just described?

JAGS (35:27.406)
It's in a footnote on a 20 page paper that I released in Virus Bulletin. I also put like hundred dollar Amazon gift card, still waiting to see if anybody read that far into the... Nobody reads, nobody reads the paper. But yeah, that's the whole Wasowski API and like compatibility library. Like it's why I talk about them so highly. It's like people don't understand how...

Ryan Naraine (35:39.732)
Really?

JAGS (35:53.676)
earth shattering and like how complex a problem it must have been 20 years ago in this like early days of cyber operations to say, how do we build platforms for like global scale espionage that are reliable, maintainable, cross compatible, cross compilable, that can be developed by teams that will never meet each other.

that builds specialized tool, one team builds a specialized tool in Australia and we want to be able to use it in the UK and for the output to be compatible with these backend databases and systems that we have in Fort Meade. Like it's a, it's a no joke DevOps problem and they tackled it way before anyone else and the outcome shows in the operations in good and bad ways. That's why it's so reliable and systematic. It's also why it's so like,

easy to spider through the minute you actually latch on to something. Like the hardest equation group finding was the first one. And then everything else was super fucking easy. And that's not the case with the Lamberts.

Ryan Naraine (37:06.776)
Kostin, do you agree with him that the triangulation attribution is still kind of murky and we don't know enough to be confident?

COSTIN (37:16.054)
I fully agree that yeah, there's no solid attribution at the moment. What I was thinking here is that one of the principles of modern cyber warfare is to try to stay under the radar as much as possible, not only technically, but commercially in the sense that maybe you deploy some kind of operation and if that gets burned,

Ideally nothing else gets burned as Juan was saying like in the past once the first Lambert fell all the Lamberts fell as well. So I wouldn't be surprised if this was some kind of a toolkit developed by a private contractor or by like private company that was being used for a very specific purpose and in addition with many other things like with similar capabilities.

If I had like a big budget, I would try to acquire as many of these toolkits as possible from different companies, make sure that they are technically unlinkable to each other so you cannot from one derive the other or find it. And then if one gets burned, it's not really my problem. It's like just another burnable toolkit. I just use the others. And I think that this is what we are seeing here with triangulation and

probably there are others, you know, used for other purposes that are completely different from triangulation, which explains why I think that, you know, people, especially like Russian companies have been trying very hard to link it to some Windows malware or some Android malware and so far failed, simply because it's probably an isolated cluster part of a modern cyber warfare philosophy that is being employed at the moment.

JAGS (39:06.296)
think it's sort of interesting that you put it that way because that would speak to like, look, if we were to assume that this is one of the other organizations we were just talking about, it speaks to the point I was trying to make earlier that we're like, it could be them, it could not be them, but we have seen them in the past and we can't connect the two, right? It tells you how some of this

investment and how some of these things kind of play out. And I mean, to your point about like somebody else built it and whatever, guys, like we know enough about at least a...

COSTIN (39:24.405)
Mm.

JAGS (39:35.534)
contracting in the US to understand that that is precisely how this shit is gonna like there I'm sure that there's teams within these different orgs that have built some of their own shit and like TAO must be developing super cool stuff but most of the platforms that we've been tussling with at that scale for sure were built by like a Raytheon or a Booz Allen or Mantek or whatever in some contract even if it was

COSTIN (39:58.625)
Mm-hmm. Mm-hmm.

JAGS (40:02.934)
that the people who work there in order to be paid properly or to be able to walk in out of one building and into the other had to leave and then go work for a defense contractor. So like there's all kinds and that's that's why like what's really funny about some of the things like Kosen says like, you can't link them necessarily. Sometimes the the the whole operation is completely different. The implementation is completely different. But when you look at the

structure of how the different components work, they're built to the exact same spec. Or when you look at like the config or like the exfiltration schema, it's the exact same one because those are the things that got put in the document of like you need to make it in this way. It has to have these 12 features. It has to connect to a command and control server and give it this information in this array like this, this schema.

And like, there are ways in which that will be your downfall regardless. It just depends on how much visibility we get into it.

Ryan Naraine (41:04.054)
Yeah. All let me pivot quickly to some of the other news items. I don't know how we got off on a tangent on Lambert's and triangulation. You know, just riff on other stuff.

JAGS (41:12.034)
That's because I haven't read most of the other stories, so I'm more than happy to break this shit over here. I'm like, I'm running out the clock. So like, you know, that's how I'm like, survived.

Ryan Naraine (41:21.102)
This week we had a zero day drop from VMware by Broadcom. By the way, they're very, very specific about their branding. Symantec by Broadcom. VMware by Broadcom has information to suggest that three unique CVE's or these have been exploited in the wild. They're VMware

ESXI, Workstation Fusion. What do we know, Costin? Do we get any IOCs? Do we get to do any hunting? What do we know about what?

JAGS (41:31.042)
Bye, broad.

Ryan Naraine (41:50.863)
these zero days are. I can mention that they were discovered by Mystic, which is Microsoft's threat intel team, but we did not get a Mystic blog, which is interesting in itself. What do you know about these zero days?

COSTIN (41:53.525)
Hmm.

COSTIN (42:02.198)
Yeah, mean, all three zero days are the kinds of zero days that you can use to escape from the sandbox or like if you want to escape from a virtual machine into the host. So they would make them interesting to all sorts of threat actors. So in particular, guess ransomware people like this very much because sometimes they infect some kind of a virtual machine.

And the ability to jump out of that virtual machine is Equals essentially to infecting the whole network and from the top server getting to everywhere else But I think they would be also very valuable to APT's and to be honest I was kind of surprised that we haven't seen more of these being used in the wild considering there's We have we have yeah, but what I mean, we haven't seen more more and I tell you why just

Ryan Naraine (42:45.878)
We have though, we have though, like this ESXi and Fusion bugs are constantly being exploited. I see.

JAGS (42:49.582)
guys, like, it- well... No, no, sorry, sorry, let's not stop. Go, go, go, go, GoSan, go.

COSTIN (42:55.208)
If I may finish, explain why. Because I was thinking there were a lot of workshops and trainings for writing this kind of exploits in the past. I think Alisa, Alisa Esa, she was doing a number of webinars as well as workshops to teach people how to develop this kind of zero days. And I was wondering, like, there must be a pretty big interest in to getting

Ryan Naraine (42:55.426)
Wait a second.

COSTIN (43:24.122)

more of this kind of zero days and using them in the wild. yeah, why aren't we finding more? I think the reason we are we aren't finding more is because maybe they are not only that, but they aren't maybe being used for like long periods of times. All you need them like you fire them, you jump into the host. They're not visible into the host. They're more visible into the if you want into the guest and.

Ryan Naraine (43:33.592)
We are looking.

JAGS (43:35.423)
Hmm.

COSTIN (43:49.115)
after that I just delete them and move on and that makes them difficult to catch I suspect.

JAGS (43:52.408)
Mm-hmm.

have a different theory. I have a different way of looking at this. I think sandbox escapes are actually the hottest, most desirable, probably closer to more expensive O days you can get these days, up there with iOS type shit. because people think about them the wrong way, I don't think about...

COSTIN (43:56.939)
to us.

JAGS (44:23.392)
Sandbox escapes in the context of like you're gonna escape some random service into the hypervisor I think of them in the context of we're living in a cloud world clouds are hypervisors for Thin client servers being laid out on top of whatever so like maybe the first question I had When this we posted this story because it was it wasn't a story. It was a fucking Ode Bulletin It was like, okay. So is this like is this cloud like?

Reli like is this a this a cloud issue? Because the reason the reason I'm putting it that way, right? If you're talking about something that escapes jumps out of a sandbox into hypervisor, but it only works. In my VM where fusion where I run my like Windows VM to try to do some debugging, then it's a it's a really interesting exploit. The impact is fairly limited. If you're telling me that it's a sandbox escape, let's let's move.

You know, let's zoom out a little bit from this VMware one in particular, but a sandbox escape into a hypervisor for whatever AWS is running is a categorical catastrophic incident because if someone can jump out of an AWS VM into the AWS hypervisor and run around, they own the fucking cloud full fucking.

You know, like that's a different level of access and I'm sure it there's a lot of effort being put into that. I want to say, I'm sure it's happening. I don't know who we think would have an interest in reporting that shit to us at all. Which one of the cloud providers, like you think Google is going to come out and be like some genius shit happened and they popped out of GCP into like our hypervisor and they've been living with us.

for like 11 months and they could see everybody's cloud instances. And the only reason we're telling you is because we're Boy Scouts, because none of you have the visibility to know that this has happened. None of you can check that, only we can. So, you know, we're willing to take the stock price dip just to like tell you the truth, be honest Abe Google. Like, no.

COSTIN (46:22.994)
Everything.

Ryan Naraine (46:43.896)
Gustin, your guess is that this is ransomware.

COSTIN (46:46.454)
No, what I was thinking that who would probably leverage these kind of things for the most profit would be ransomware groups, which can afford zero days and we know they've been deploying zero days in the past. But again, this is kind of exploit exploits if you want, because it's like three of them probably working together that are valuable to both APTs and ransomware. Unfortunately, again, no IOX, no information.

Ryan Naraine (47:14.178)
Yeah. I mean, doesn't Mystic know better? I mean, I know there are guys from Mystic listening here and I've been told in the past, I actually had someone approach me to talk about, you guys on the podcast are talking a lot about Mystic not releasing IOCs. By the way, Ryan, this is all legal stuff. Like the lawyers block. They're, they're quite frankly says, listen, we're going through months and months of meetings, trying to get these things released, trying to ship IOCs. We just get blocked from doing them. So in fairness to those guys, it's not their call. And.

COSTIN (47:17.049)
Wow.

Mmm.

JAGS (47:30.156)
Yeah, yeah.

Ryan Naraine (47:43.65)
We can't talk to the lawyers, the lawyers do their lawyering. But like, what's going on? How does the rest of us protect ourselves from an ordey exploited in the wild and we have no way to go hunting to know what's going

JAGS (47:48.716)
I mean, you can...

JAGS (47:57.126)
I think on the we can't talk to the lawyers thing, I look, I used to in this podcast be absolutely rabid in talking about like Brad Smith and Tom Burt. Tom Burt, look, the Reese, yeah, you don't know who that is. That is the person doing all that like legal decisioning up.

Ryan Naraine (48:12.812)
I don't know who that is, who is that? That's the guy.

JAGS (48:21.73)
the chain of command that Microsoft and Brad Smith at the end of the day is supposed to be sort of where the buck between him and. God damn, I just blanked on the CEO of Microsoft. Well, anyways, between him and him, between him and Satya, I have not slept. I'm sorry. Between him and Satya, that's where the buck stops. So I never am going to come down on a mystic researcher and be mad at them because they haven't.

COSTIN (48:34.358)
Satya or who?

Ryan Naraine (48:34.67)
Satya?

JAGS (48:49.834)
somehow change the whole organizational culture from the bottom up. So my reaction is just to go, okay, who the fuck is the top of that org? You. Hey, why the fuck can't we get IOCs? And like.

Ryan Naraine (49:03.032)
Yeah, and this is a John Lambert question. Like John Lambert is all the way up there. He's a threat intel guy. He's aware. He obviously is aware. The mystic guys that approach me and talk to me about this, they're obviously aware. It's like, how is John Lambert and these guys allowing a legal guy to affect what is right?

JAGS (49:16.01)
The complication.

JAGS (49:24.044)
because what is right is not obvious in a lot of these circumstances. look, look, the legal muscling itself is a problem that I think needs to be addressed period, full stop, in the sense that I don't, I think that any of these companies where legal is that involved in decision making process on a case by case basis has a huge fucking problem. That company has a.

Ryan Naraine (49:50.636)
Is it because it's victim data? I mean, like, what?

JAGS (49:52.672)
No, no, no, no, no, no, no, no, no. Look, it's just it's just to say what we're seeing here is a failure of leadership at any big company where legal is that involved, where they're in the room for every single one of these releases. You have a problem because you haven't established a process with guardrails that just says this is what's OK from here to here. As you know, from here to here, you can operate.

And if you are escaping these, if you're coming up against these guardrails, then please call somebody from legal and we will review whether that needs to be the case, like whether we need to determine something. And it's obvious that companies like Google and Microsoft and Apple and Amazon, so on, do not have that. And that's why we're seeing these conversations where like, where we having these conversations where it's.

It's obviously not up to the researchers at all. It's not up to their discretion at all. And it goes through a ginormous process, which is why it takes them weeks and months to publish anything, because you're sending it through. It's the same discussion we were having with Cyber Command. Like, it's just like bureaucracy, bureaucracy, bureaucracy. And at each point, I think the problem, what people don't understand about that is it means that you have to fight to publish.

It's not that someone has to fight against you not to publish. And that means that in most cases, most things will not make it out to sea. Because you have to put up a good argument for why are we doing this? Why is it worth it? Is this blog about some Indian APT really worth it? And if you do that for five rounds, most blogs turn into like, no, it's not fucking worth it. I want to go back to doing my real job.

Ryan Naraine (51:15.075)
Bye.

Ryan Naraine (51:37.303)
Yay.

JAGS (51:37.674)
And so it's a failure of like incentives from the bottom, like just in the way that the process is stacked. Then you get the next layer of that conversation, which is, well, what good is it going to do to report this? And that's where you get into problems with some of these O-Day ones, where if this is a consumer grade problem, then there is an easier argument to be made for why you want to publish. But if this is like,

This is affecting clouds It's hard to argue that the right thing to do is to publish a blog as opposed to Sending this out to other blog or other cloud Providers and saying hey This is something that you need to worry about and thereby skipping the whole public face of this that actually puts some pressure on them to fix it and discuss it So that's where you know these perverse incentives

You need to address them purposefully because it's not something you can fix in a case by case issue. You're creating problems and skipping right things to do routinely by not addressing them proactively.

Ryan Naraine (52:53.006)
Kostin, if you're a corporate customer using VMware ESXi Workstation or Fusion, you can't hunt because you have no IOCs. What's the advice you give these people? Just scramble, go patch, DCVEs. By the way, we're referencing VMware's bulletin, VMSA 2025-0004. So number four for 2025, these three O days. What's your advice to them, Kostin? Just go figure out patching and move on with your life?

COSTIN (53:17.992)
I mean, sure, listen, patching is always good, although I can tell you that it can be a pain in the ass with these virtual environments. I know, like myself, running several virtual environments for multiple servers. Whenever I need to install like a patch on the host, on the server, like for the virtualization software itself, it's terrible. Like typically if it's something serious, you need to reboot it, which means to reboot all the...

all the guest machines so because of that I think a lot of people just try to avoid this as much as possible I know people who are running Cytricks and other things that haven't been updated in years basically because they just couldn't afford to reboot so even patching might be difficult here of course if they were to find whatever activity is related to this I would say that like the

regular guards or logs monitoring or EDR or whatever has a higher chance of catching the resulting activity than rather than the exploitation itself. So they might catch, you know, if it's ransomware, whenever the ransomware gets deployed, or if it's something APT related, whenever the APT is trying to run Mimikatz, the like similar tools or move, move lateral. Yeah. So

Ryan Naraine (54:41.258)
set your traps right.

COSTIN (54:45.59)
I mean, I can't provide a lot of good advice besides probably what they are doing already. What would be amazing is VMware by Broadcom would be sharing a bit more information and IOCs by Broadcom for the rest of us that are not by Broadcom.

JAGS (55:03.928)

Hey, I'm gonna show you, I'm gonna put a little wrench in that. And I don't know if I think this is a good thing or a bad thing. But Broadcom bought VMware, which I think is a bad thing. Like that was a bad thing for the industry in general. It kind of killed VMware. It took away an important like pillar of an industry as a whole for no reason. But.

Ryan Naraine (55:29.56)
lot of money. This is a big reason.

JAGS (55:30.69)
For a lot of money, yeah, yeah, sure. But look, for Broadcom, all of these are just like, they're PE moves, like they're private equity moves. They buy these things, they got them within an inch of their lives, they try to make them profitable, they spend them out, and in the process, you kill the whole stack, right? Like Carbon Blacks and Mantech, fucking VMware, there's a lot of shit that's going into the Broadcom graveyard right now. But with VMware in particular, something interesting they did, something that I admire Broadcom for and I'm...

Ryan Naraine (55:38.926)
They'll spin it out eventually.

JAGS (55:59.222)
also kind of confused by is they took VMware and they said these consumer grade things, they're free. Just you have to like, you have to go through the true depth of pain that is navigating that fucking Broadcom website. Like the portal, like you need to, it's easier to get like a driver's license in the States than it is to like get to the VMware Fusion downloader in the Broadcom website, but it's free. And my point here is, okay.

Ryan Naraine (56:12.056)
to get them, but they're free.

JAGS (56:28.952)
Thank you Broadcom. Whose responsibility is it now to really put all that much effort into the fixing, the patching, the maintaining, the supporting of this now free thing? It's great, it's free. Okay, you don't have to pay for it. Awesome. Now who is the ecosystem maintainer? Who is the person that, like if this, let's put it this way. If this ESXi exploit shows that there's like a really vulnerable part of ESXi.

like in its architecture. And this is only the first of like 12 zero days in that same region of ESXi, who now has an incentive to restructure, re-architect, rebuild for a larger, like safer ecosystem that is unpaid for, unmanaged, and now there's no stewardship for.

Ryan Naraine (57:25.486)
We started to see these things pop up in this Sysachev list constantly. If you go to this non-exploited vulnerabilities list and enters VMware there, the list just keeps growing and growing and growing. So I think there's a lot of ransomware things happening there, but we've

also seen Chinese APTs connected to VMware stuff. So it's basically cross fingers, try to patch, add some layers of detection and godspeed basically.

COSTIN (57:52.183)
From the point of view of hunting I'm just gonna drop this hint here in case there's threat hunters listening to us So what we used to do in the past for for this kind of cases where there's no IOCs especially for for zero days What happens like typically the information information about this vulnerabilities is shared through map

and then different antivirus producers, will add detection for it sometimes with those names like CVE 2025 22224 or 22225 in this case. So what we were doing were just watch on virus total for when detections for CVE 2025 22224 shows up and that's when you get a sample and this works so wonderfully and at least in the past it allowed us to find some samples.

Ryan Naraine (58:48.782)
So this is a map workaround. This is a map. This is a map work. A map backdoor to find samples. Interesting.

COSTIN (58:49.214)
Yep. It's like a, yeah, it's a back door.

JAGS (58:58.478)
until they change it after this particular part.

COSTIN (59:00.854)
yeah now they're gonna rename it but like again the the good news is that the vendors and especially the the analysts the people writing those detections like yeah the people doing all the work if you want they don't listen to the podcast so hopefully they'll still push the detections for cv 2025 22224 thank you thank you please please do

Ryan Naraine (59:02.978)
Nobody listens to the podcast.

JAGS (59:04.876)
Nobody listens to this shit.

Ryan Naraine (59:20.962)
And if you are listening to the podcast, shout out to you for adding those CVS because.

JAGS (59:24.782)
Yeah, be cool. Keep the names. Add some notes. Let us know if you change the schemas.

COSTIN (59:32.128)
can actually search right now life I'll let you know if there's what's next what do we have next

Ryan Naraine (59:32.366)
Alright, let's... Let's...

JAGS (59:35.63)
do it. man, these systems, magic systems. Stop moving us along, man. Let them get some information. We're doing live farm to table research, live, real live hunting in on Women's Day on International Women's Day. Kostin is like Kostin is dangerously close to getting in trouble with his boss. We need to be quick here. Let him do some research.

Ryan Naraine (59:38.028)
Let's move on to the other... Live hunting. We're one hour in. We're one hour in. It's International Women's Day.

COSTIN (59:43.154)
Now what's next?

Ryan Naraine (01:00:02.094)
One year ago, we had this dramatic iSoon leak. iSoon is this Chinese private sector company. And we had a leak of their data that revealed in tremendous detail the methods used by Chinese authorities to do surveillance of dissidents overseas, hack other nations, promote pro-Beijing narratives, and so on on social media. What we had this week is a US unsealing an indictment against, I think it's Suatu.

Two Isoon people or eight Isoon? There's a total indictment of 12 people, including a bunch of these Isoon people described as hacker for hire operatives linked to doing hacking work for the Chinese government. Was this expected, Gustin? I mean, we kind of knew the leaks and your guys at Sentinel-1, Juanito, actually did a really, really good wrap-up of what the leaks, what was inside the leaks and what it meant.

But we talked in the past about what these indictments really mean and what these sanctions really mean. Does it really have any meaning or what? But on this particular front, what do you make of what we saw this week from the Justice Department surrounding ISUN?

COSTIN (01:01:11.51)
Well, I'll start by saying that the Justice Department indictment has more IOX than the VMware by Broadcom indictment. There's like tons, tons of new IOCs. Like they were, at least for me, they were new. There's like four or five new domains in there that I haven't seen before. And I think they are like...

Ryan Naraine (01:01:17.966)
Or from Mystic.

JAGS (01:01:21.858)

Ha ha!

Go Justice Department.

JAGS (01:01:33.592)
Well, guys, like to be clear on that one, like thank you, Justice Department, but they think like Villexity, PWC, like there's a few different companies in there where it clearly. Right.

Ryan Naraine (01:01:44.396)
Yeah, the heavy lifting was done by our US private sector companies.

COSTIN (01:01:50.282)
Yes. So what was the point? Like they forgot.

JAGS (01:01:50.296)
Sorry, Kosen, I didn't mean to stop you.

JAGS (01:01:56.236)
No, sorry, just to say, like, if we're giving them credit, like, the credit really belongs with, like, Villexity, you know?

COSTIN (01:02:00.087)
well, sure, I see what you mean. However, yeah, they could have just removed the exactly like, but not only that, but like the other thing which it's so painful to see is when they do the indictments and they release a PDF or scanned pages like that's so painful. So whenever they do the indictment, like

Ryan Naraine (01:02:07.49)
The lawyers could have removed it.

JAGS (01:02:10.633)
Hahaha

you

COSTIN (01:02:25.866)
where you can copy paste the text that's like wonderful that's it's a big deal for us please keep doing that yeah but so there's iOX in there that were new for me where the domains there's like a bunch of IPs most of them at Chupa which is probably very well known to a lot of people in the thread intel like there's a lot of Chinese stuff at Chupa they even

Ryan Naraine (01:02:28.43)
That's a big deal,

COSTIN (01:02:54.026)
kind of show some information on how these VPSs were being rented with the credit cards issued by Bank of China, also on different names. All of that is documented in the indictment. What I thought was interesting here is that there were two separate indictments, right? There was one directly related to the ISUN people released by the Southern District of New York, and there was another indictment.

Ryan Naraine (01:03:04.75)
and all this is documented in the indictment.

COSTIN (01:03:21.718)
against two hackers associated with APT-27 through the District of Columbia. And you can say that sure, what's the connection between ISUN and APT-27. In the past, there were, let's say, like this kind of fuzzy connections, which I personally I don't like when people say,

Yeah, that's kind of a cluster of activity which overlaps with activity from a different thread actor that we track under this name, but others may track it under a different name, which actually is not the same as our name, but somehow overlaps with that activity in some points, but not all. So this is case with ISUN and APT-27 here, and may very well be the case where like some of the guys working for...

or within part of APT 27 were either employees of ISUN or just moonlighting, having side jobs to their official jobs. APT 27 was huge back in the days when we were tracking them. They were huge in Europe, also known as lucky mouse. They were like pretty much all over Europe, all over...

Ryan Naraine (01:04:22.154)
APT 27 is one of the big ones that you guys track closely.

COSTIN (01:04:38.994)
European ministries of foreign affairs and they started targeting Middle East. I think they were extremely interested in whatever was happening in the geopolitical world. So they were moving from one place to another. So you could see them almost everywhere. Yeah, it was not necessarily super sophisticated. They were definitely not in the range of the top APT groups out there, but they were like

almost everywhere taking advantage of especially one days or like even older exploits again not necessarily the best but super super active going against us going against governments think tanks and so on and so on

Ryan Naraine (01:05:25.934)
What if for a long time too, like from 2016 through 2023, it's just routine work. iSoon is obviously not the only private sector Chinese company is doing this hacker for hire stuff. Do we have

visibility on others? Is there like kind of reporting on what this Chinese private hacking ecosystem looks like? there some work from the code?

COSTIN (01:05:27.768)
yeah.

COSTIN (01:05:45.334)
I apologize. Just wanted to say that was an interesting report that we may have missed about or did we discuss already about the connections between Pangu and iSoon?

Ryan Naraine (01:05:56.675)
Yes, yeah, we did it last week, yeah.

JAGS (01:05:57.23)
I mentioned it briefly, that's Eugenio Benincasa. We briefly talked about it, but honestly it's worth going into. was a really good.

COSTIN (01:06:09.96)
Yeah. So no, no, no. I was just thinking that this situation where the nation state sponsored operations combined some kind of military, maybe a unit or military organization or civilian spy agency, and then a bunch of contractors, this kind of model is pretty much, I would say, the prevalent formula everywhere nowadays, not just in China, but also in Russia.

Ryan Naraine (01:06:10.2)
Go ahead, Gustin.

COSTIN (01:06:39.612)
in the West, this is kind of becoming the norm. So whenever one of these contractors gets owned, we get to peek into the world and how they operate and how they go back and forth with these contracts with the government and who is doing the espionage infrastructure targeting and so on. And it's interesting to see that working for a contractor doesn't shield you from

from any of that so you can still get indicted right there can still be a bounty on your head for your capture so yeah targeted drone strike drone strike and who knows who knows in the future maybe APT groups will be designated as terrorist groups and they'll be like well

Ryan Naraine (01:07:16.93)
And according to Mauro's warnings, it's like you can be tagged as an enemy combatant as well. Yeah.

JAGS (01:07:30.286)
COSTIN (01:07:32.424)
Venezuelan gangs, drug lords and so on. What's next? Maybe APT groups and contractors working for this APT group. just maybe a word of caution to people. If you work for one of these

APT groups as a contractor through another company, this it can probably turn into some kind of a risky activity.

Ryan Naraine (01:07:55.407)
I'm glad you flagged the Pangu-ISUN connection and this Eugene's paper. Juanito, you brought it up here. It's the further examination of the leaks, just reading a line from the report, reveals a much more intricate relationship between Pangu and ISUN, extending beyond informal discussions and hacking contests. Now, Pangu is very, very well known as like an amazing iPhone hacking team that has gone to hacking competitions. I believe they used to come to the own PontoOwn before.

before the Chinese got locked out of it. You think this report can lead to a future where Pangu gets dragged into some of this from DOJ and from your law enforcement folks?

COSTIN (01:08:39.53)
That's why I mentioned it. I mentioned it for this particular reason. We don't know, of course, how they were selling the exploits. But again, in the past, we've seen like in Russia, we've seen cases of private companies who are selling zero days to the military. They got sanctioned. So very same can happen in China, I guess.

JAGS (01:08:59.96)
think it's hard to know for me how we actually want this to play out. And I say that because we have a very kind of moralistic sense in how we approach some of these things and not in how we approach others. And the inconsistency of it is kind of problematic when you try to apply that as a categorical imperative, as like a thing that matters across the board. And what I'm trying to say with that is,

We are.

The sense I get is we find it objectionable for companies that sell exploits to certain kinds of countries. well, anyways, we also find it objectionable for mercenaries who develop platforms for doing operations that are sold to different countries across the board in different regions.

Then we also find it objectionable that there are companies where people do ops on behalf of these other countries. We, you know, and I'm trying to kind of stratify like the different support organizations that go into these things being built. But my question is, what exactly do we find objectionable about a corporate structure of contractors in China that work

for the Chinese apparatus to do what the Chinese government does like who are we laying? Yeah, like like I'm not saying that that means you need to think they're like your best friends or any of that but like what exactly are we objecting to and like and I'll answer my own question sort of in the sense that I think we are objecting to the appearance of benevolence and like defense.

Ryan Naraine (01:10:35.534)
How is it different from what happens here in the US with all this?

JAGS (01:10:59.0)
from companies like Pangu, that have been coming to conferences and selling their wares as if they are defensive companies, whom when you pull the curtain back are like, no, actually these are like, these same dudes that are coming to defend the world from Vones are selling them directly to somebody or like giving them directly to somebody that's running ops and are engaged in the like nitty gritty of those ops.

I think that's the only part of this where I'm like, guys, let's stop. What the fuck? Like, let's, let's talk about it as a community. But the, they do, what they do is just like, they're doing business in their country. And if you have a problem with Chinese operations, you need to lay that at the feet of the Chinese government, not the companies doing that shit. Cause if we, if they did that to us, like the day they, you know, try to indict some random, you know, vuln research shop in the U S

We're gonna lose our fucking minds. And you're like, okay, well then what exactly is the problem here?

Ryan Naraine (01:12:00.623)
I think you nailed the problem there, which is they come to our conference, rub shoulders with us as reputable members of the community, they're private companies holding O days for use.

in nefarious things that pop up in malicious campaigns against the West. And then you're just like, okay, this is not appropriate. And we had this conversation last week about Celebrite and some of these vendors that come and sponsor these conferences and roll around. They're hoarding all these for use by law enforcement. And some of it is objectionable, some of it is not. We don't get many success stories. So we're kind of like in this pattern of just...

accommodating all of it. you find anything objectionable at all to Pangu and Isun doing work in their ecosystem for their governmental cost?

COSTIN (01:12:47.67)
Well, buddy Ryan, it's difficult to say because I've had a lot of friends in the past who are extremely, extremely worried when they were seeing this US indictments. They were saying like, what if one day, know, Russia, China, whoever does the same to us and we get to get our names on this list and seen as, you know, listed for facilitating whatever kind of activities. And if you

Ryan Naraine (01:13:16.386)
And this is a kind of reciprocity we should expect,

COSTIN (01:13:16.63)

If you ask me, well, what I think is that somehow the US law enforcement agencies have been more successful at identifying Chinese hackers, Russian hackers, whatever by their name, like the rank, whatever. I didn't see where I don't see a similar success from the other sides, if you want. So.

Ryan Naraine (01:13:41.198)
It's true.

COSTIN (01:13:41.983)
We haven't seen it for one reason either they're not competent enough or maybe they don't have the desire to name these people or to indict them or to put their names out there. I think maybe the OPSEC is better on the Western side of things and the correct and the desire to to use this tool like naming and shaming is less on the Eastern side of things. Maybe that's so but

Ryan Naraine (01:13:56.355)
A lot more carelessness on that side, right? Yeah.

COSTIN (01:14:09.814)
One of the stories by the way from this week and I don't know if you want to jump there immediately, but I thought it was fascinating that this Catalan court orders the former NSO group executives to be indicted for spyware abuses. So here we go. We have a Western nation, a Western court in Spain, a Catalan court who is ordering for three senior executives at NSO group.

JAGS (01:14:24.184)
Mm-hmm.

COSTIN (01:14:36.438)
to be indicted for their role in high-profile hacking scandals. So now we see how that starts to reflect and how we see more of this going on if you want against companies, private companies in this case from Israel being targeted in the same manner.

Ryan Naraine (01:14:56.684)
Right, and these were linked to the Catalan hacking scandal in the past in which at least 63 Catalan civil society members were targeted by this NSO surveillance thing. Do we think anything will come out of that, Juanito? This is a Spain court against Israeli companies. The three executives, Shalev, Omri, and Yuval, probably lives in Israel. Like, what do we think comes out of this?

COSTIN (01:15:08.32)
Mm.

JAGS (01:15:24.014)

I don't know what comes out of this, but like I wish it were a higher and more like important court I guess but But I think it's an interesting case. I don't know which way I want it to shake out to be honest with you because the the it's not that I support NSO but again, I kind of want us to define our Moralizing and where we're putting

where we want to put responsibility ultimately. And I'm not saying that NSO has no responsibility, but my point here is, are we indicting the leadership of NSO for enabling something and figuring out how much they knew?

but we're not like, are we doing it in the process of discovering and just and substantiating who is to blame for the actual operations? Or are we just coming down on NSO as a company because something bad happened and somebody should pay for it. So we're gonna go fuck with the enabler but we're not gonna put this at the feet of the perpetrator.

And like that's a, it's a not insignificant differentiation. I'm not def-

Ryan Naraine (01:16:47.01)
And when you say the perpetrator, you're saying the perpetrator is Catalan.

JAGS (01:16:50.594)
Well, I don't think it's Spain or like, I don't, but that's the point, right? We don't know, but they're not being called in. They're not being subpoenaed to testify or to provide evidence in the process of indicting or whomever, like whoever actually pulled the trigger and designated these targets. Cause like, don't think Shalev Julio or anybody at NSO,

Ryan Naraine (01:16:53.326)
or Spain, sorry, yeah.

JAGS (01:17:19.118)
pulled up a list of like Catalan civil defense people and said, these are the folks we're going after, right? Like that's the whole point of these stratified ops. They're providing the platform and they have some semblance of responsibility for how much they choose to not know and what they may have overlooked. But they sure as shit didn't pick the targets. They didn't run the ops themselves. So like someone is to blame at a different level. And what my point here is,

If this is a Spanish court basically saying, here and tell us who did what and where, who did you have contracts with, who chose whatever, I think that is a holy cause and I support them 1000%. But if it's some performative bullshit of bringing these three Israeli guys who just like, their biggest mistake was waking up that day, like,

and then putting this operation at their feet as if it's completely their fault or they chose to do this, I don't like this. I don't believe in what we're doing.

Ryan Naraine (01:18:29.324)

On a related note, have news that Apple has started sending out these threat intel notices to people who have been hit by this targeted mobile spyware. There's some emails going out, think Doncha from Amnesty International tweeted, and there's some emails going out from Apple saying, Apple has detected that you're being targeted by a mercenary spyware attack that's trying to remotely compromise an iPhone associated with your Apple ID and so on. So they're basically telling people, were part of this targeting.

One of the things I noticed, Costin, and I think you flagged it on Twitter previously is Apple used to call this nation state. They used to say you've been targeted by a nation state type attack. Now they're calling it mercenary spyware attack. What's the reason for not calling? The question is, has Apple stopped warning people about?

spyware that's nation-state related and are they only doing mercenary now? Mercenary suggesting its private sector.

COSTIN (01:19:29.686)
It's a well sure it's a way it's right there in the subject if you want it says a targeted mercenary spyware attack against your iPhone and I think that's you know it's pretty clear it doesn't say nation state now it may be hard to say if they stopped notifying on nation states in the sense that maybe it's the same as with the US cyber command maybe right

Maybe it's not like something they stopped because it wasn't happening anyways. They were only notifying about mercenary spyware and they just chose to call it differently now. For instance, like as a good example here, I don't know of anyone who was notified by Apple for triangulation infection. Nobody got a notification. I am familiar. Yeah, I am familiar with people who are compromised and they never got.

Ryan Naraine (01:20:00.239)
A little stand down.

Ryan Naraine (01:20:19.224)
Do you know people who are compromised?

So you're familiar with very specific people who were compromised by a triangulation, but they did not get an Apple warning.

COSTIN (01:20:29.098)
they never got a kind of notification from Apple and I'm talking people of course living in NATO countries or definitely outside Russia as well who never got any notifications from Apple. again, maybe this was never it maybe never happened. Maybe you never got notifications. And I think the issue here is what's probably making this alert special is the fact

that it appears to be huge. So Apple claims that the notification is being sent to targeted users in 117 countries, which is huge, if you ask me. So I was checking right before our podcast, I was

checking how many countries are customers of NSO as an example. And if you add everything up, like all available information, it will come up at maybe about 50 or 60 countries, not 117.

Ryan Naraine (01:21:22.306)
Yeah.

COSTIN (01:21:25.404)
So why this is so big? I guess it could be some different explanations. We don't know for sure if this is just about one thing like NSO or it is perhaps about like pretty much emptying the closet. Like everything we have it goes out. Why does like everything goes out? And I think I have a hunch here that it may be related to that blog post that iVerify put out in December if you remember.

Ryan Naraine (01:21:38.4)
All of them,

COSTIN (01:21:53.407)
and they were specifically highlighting. Yeah, and they were saying that some of the people that we found with Iverify that they had Pegasus on their phones, they never got a notification from Apple, which was in my opinion, was like a directed at Apple kind of putting them.

Ryan Naraine (01:21:54.594)
back assist infections.

Ryan Naraine (01:22:07.854)
Ah, so the Apple Threat Intel team is just kinda spamming everyone now, yeah?

COSTIN (01:22:14.902)
And now they're like guys look I verify says we didn't notify everyone so let's just not like open the floodgates and Just get everything out everything we have everything everything we have but just mercenary not not the other things those we keep them for now For us for now

JAGS (01:22:14.958)
oof oof

JAGS (01:22:25.846)
Oof.

JAGS (01:22:33.976)
This is a bad look, man. That's a bad fucking look. and I, I'm not, I don't feel bad for them because I think this is really well in line with what we've been saying about Apple this whole time. Or at least what I've been bitching about Apple this whole time, which is I don't, I don't believe them when they kind of put, when they basically like pat us on the back and say, we've got this, don't worry about it.

not your problem. We've got it. We're defending our backyard. We're making the best possible decisions. Smart people have got this shit. Go on kids. You just go and play with your window shit like somewhere else. then you, stuff like this happens and you go, hold up.

Even if what you're telling us is that you guys have great visibility and that you're aware of the breadth of the problem, which you're the only entity that is. If this is what you're choosing to do with it, which is to say nothing and not disinfect these people and not then then I, I, I fundamentally disagree with your project and I think

you should go fuck yourself. And frankly, like it's unbelievably patronizing and almost inhumane to have that level of visibility into a bunch of people whose lives are being completely turned inside out, whether legitimately or not, and just ride it out.

Like, we're just gonna sit here and wait for the O days to come. The important thing is the O days. We need to keep patching these O days. And you're like, why even fucking patch them? The implants are already there. You're letting the implants live forever. What difference does it make? And if you're not, then fucking tell us. Like, at least pop up a notification that says, we just disinfected your iPhone. We're still not gonna tell you who it was. Good luck, bro. Like, change careers. Something. But like, that's not happening. Like, I'm not getting a malware block notification from iOS.

JAGS (01:24:46.218)
or like, hey, someone in Cupertino is like, has deigned that you're worthy of protection. So we went ahead and disinfected you. Not those dudes, not the Uyghurs over there or anybody over here, but like you, you're cool. Like, so we disinfected you. Like where the fuck is the transparency? There is something extremely fucked up about how Apple has chosen to handle this at every level. And like the O days are this bullshit candy

They hand out every once in a while that somehow shows us that they're defending us. But what does it mean to defend people when they can't install security solutions? They can't have any visibility into what's happening on their device. Even if you do discover that they're infected, you're not really going to tell them. And if you have your hand forced by some third party company into admitting that it happened, you're not going to give them any details about it. You're just going to tell them after the fact. What the fuck are you doing?

Ryan Naraine (01:25:45.026)
Worse.

JAGS (01:25:45.102)
Like as an Apple customer, like that who submitted their shit to Iverify to try last, I literally sat there for like 20 minutes and was like, this could go either way. Like this, could real, it could be infected. It could not. I don't know. And like, I was like, oh, okay. Not infected. Cool. Feels kind of bad, but all right. Like, but, that, like what the fuck dude.

Ryan Naraine (01:26:06.008)
The other thing I question, the other thing I question, the other thing I question.

COSTIN (01:26:08.98)
You need to do more questionable things, Juan.

JAGS (01:26:11.755)
I know.

Ryan Naraine (01:26:13.676)
What's the usefulness of this Apple Threat Notification anyway? There's nothing you can do. Like what's...

JAGS (01:26:17.88)
out.

It's as bullshit as tags notification. Like the Google tag. Yeah, exactly. It's it's you do it so that you can frame the notification. You're like, look at like I I'll take it. But like.

COSTIN (01:26:21.27)
It's like a badge, badge of honor.

Ryan Naraine (01:26:30.23)
I to the Amnesty website and it says, you know, they have like a special section that talks about these threat notifications. It says, it's a big Q and A. I received an Apple threat notification. What should I do? And basically Amnesty International says, just hit our get help form and send us something so we can do forensics on you. Like there's nothing you yourself can do. I mean, outside of just patching your phone and turning on lockdown mode and doing all the blah, blah, blah. If you've already been hit, like there's nothing you can do.

COSTIN (01:26:36.235)
Mm-mm.

JAGS (01:26:43.916)
Yeah.

JAGS (01:26:55.726)
So here's the thing. Let's pause for a second and speak to our European friends because they're the only ones who are in any position who have the motivation, the willingness, and perhaps even the influence to do something about this and say, the real issue here is that there is no watchdog that serves as a

independent, adjudicating body that let's put it this way. If there existed a regulatory body in Europe that is independent, but staffed with people like, let's say like the Vigenum type organization in France, right? Expertise and whatnot that

If I get an Apple notification, I go to this body and I say, and I say, I have reason to believe that I have been targeted by some mercenary company with some kind of spyware. I, as far as I know, I'm a good person and have done nothing that would warrant this level of inter, you know, interference in my life. I would like you to figure out and adjudicate as to whether this was fair. And then that body behind closed doors goes and says to Apple, Hey Apple,

Give me the information you have on this infection. What malware is it, whatever, who did it? Like, and they can compel Apple to actually share this information behind closed doors and then go to Paragon or Quadrim or NSO or whomever and say, hey, Shalev, get over here. Who in your contract put this target on notice? And then they have to go, you need to go talk to the Moroccan government. And they go, okay, thank you. Morocco, what the fuck?

Ryan Naraine (01:28:49.102)
You

JAGS (01:28:51.7)
And if you don't answer to this complaint, we're going to make it public that it was you that targeted this individual. Then you create an actual chain of fact finding and responsibility where an independent party is going to gather all this information. And yeah, it's not the visibility that you want that we want where we want to watch the process, but at least there's somebody who says, look, we're not naive. We know that intelligence is important. We know that not everybody who looks good is good. So.

Come explain to us what the fuck is going on. And if we judge this to be a good faith investigation under these parameters, then we will just say this court has found no fault with whatever and good luck and, you know, fuck off. But if not, then we're going to reveal the information of this abuse. That's what you're missing. It's like, who's the body? Am I going to go to the fucking UN? Like, God, it's like, you know, it's like, who the fuck is supposed to say anything about this?

And in the absence of a process like that with implied like closed, open, closed, like sort of transparency mechanism and then project zero style reporting like deadline and dead drop type thing, we're fucked because Google and Apple are just gonna hold on to that information as if it's their intellectual property that your life is getting fucked.

Ryan Naraine (01:30:12.76)
Turn on lock down mode, patch your iPhones, cross fingers and hope for the best. I mean, that's about where we are. Last story. Last story I wanna touch.

JAGS (01:30:19.234)

Let just light a little candle to Yvonne.

COSTIN (01:30:21.558)
If you're in Romania, ping me. If you're in Bulgaria, Greece, I had people in Greece reaching out, people in Poland reaching out. Ping me. Yeah, for forensics. Sure. No, NSO actually, Pegasus. So I'm happy to help. mean, not just do forensics, look at your CISD eggs or backups or whatever, but also to set up some infrastructure like...

Ryan Naraine (01:30:25.294)
Huh?

Ryan Naraine (01:30:33.016)
For Forensics Help.

JAGS (01:30:33.198)
They had the big predator thing, right?

COSTIN (01:30:51.37)
private VPN if you want with Pi Hall, just ping us, ping me.

Ryan Naraine (01:30:53.784)
Ping the three-body problem. Ping the three-body problem. We will help. Lastly, I just want to touch five minutes quickly on a quick update on the Magic Money story with Bybit. We got a post-mortem report from Safe Wallet that kind of screenshots a Mandiant report that they got. They screenshot like sections of the Mandiant report and put it out. But the IOCs is actually...

JAGS (01:30:55.758)
You

COSTIN (01:31:14.269)
I

Ryan Naraine (01:31:17.39)
as photographs. I'm not going to get there. But the big story is there's no ODAs or nothing. It was just a supply chain thing that targeted a developer and slowly kind of worked on him and figured out how to have this JavaScript do this magic, moving of the money into the North Korean thing. Costian, what do we know? How can you wrap up this story for us? Because it's 1.4 billion. Usually we would move on, but I just feel like...

We figured out if the laundering has been done, what's happening with the mixers, update us on what we know so.

COSTIN (01:31:42.421)
Mm.

COSTIN (01:31:49.303)
Yeah, so let's start just very quickly with the technical hack if you want. I was just trying to understand how this was possible from a social engineering point of view because social engineering plays a very important role in this hack. And in particular, this technique, think it's been mentioned before in public reporting the fact that Jihad 10 not

Ryan Naraine (01:32:07.886)
Mm-hmm.

Ryan Naraine (01:32:14.392)
Gia 10. It's kind of like the slow long game, right?

COSTIN (01:32:18.556)
Yeah, it's a slow long game, but also like how to say quick pressure, also quick pressure that you need to in this case, here's a Docker container that you need to run. It's safe because it's a Docker container, right? And then you need to turn on the privileged mode for that Docker container. And I was thinking there's a lot of technologies nowadays that they're becoming super popular. Everybody uses them.

but you don't fully understand all the implications and risks that come with those. So just to give you an example, maybe one day I come and say, hey, here I have my own LLM. Like this is my own LLM threat intelligence LLM Ryan or Juan. Like you can run it on your computer and you go there, you load it in LLM studio or whatever and poof, you're owned. Why? Because they support Python scripts. So I can have a Python script in the air.

that just essentially owns your computer. So there's like all these inherent risks that come with the new technologies that people just don't understand. And with the Docker container, I guess the developer who got owned through the social engineering trick, he didn't imagine that the Docker container can actually pawn your computer and just pawn the entire infrastructure. So that's how it started from there. I mean,

Probably I would assume that the safe wallet guys were not maybe the most security protected or you know shielded guys in the world maybe they didn't have like the best security in the world which might have caught this So I think now they're gonna probably take some measures. They claim that they're working with Mendi and to Deploy new security

protections in their infrastructure. So nevertheless, like you say, it wasn't a zero days. was a relatively simple social engineering trick that relied on poorly understood technology, in this case, Docker, to own the developer. And kind of interesting that they knew exactly which developer to target. To me, that sounded interesting that he was specifically targeted in order to get in the company. And from there,

COSTIN (01:34:37.78)

The rest is history if you want. They launder the money incredibly fast if you ask me in the past. They were waiting and waiting and waiting and sometimes like there are even nowadays there are funds stolen in some heists that haven't been fully laundered. Nevertheless, according to Arkham, they've just laundered everything. Maybe not all, not everything is dark, but

in a way you can say longer at least they changed the funds from one chain to another apparently everything is going to to bitcoins in the end this is what they want to help hold and i think that well some of it went dark if not all of it went dark and in time it may be possible to retrack some additional funds but

Kind of the story and moral of the story is that the money has been laundered like they can move much faster. They can move magically faster, much faster than the crypto industry can track the funds. yeah, there was another kind of interesting news this week that the Garantex crypto exchange, a Russian exchange has been sanctioned by the US and they seize their domain and they're shutting down because

Ryan Naraine (01:35:36.267)
magic.

Ryan Naraine (01:35:57.579)
and the infrastructure here.

COSTIN (01:35:59.019)
the infrastructure and the US seized $28 million in USDT tether from their funds.

Ryan Naraine (01:36:06.059)
So there is a chance like some of this money could get rolled back in a future takedown of some exchange that was involved,

COSTIN (01:36:09.142)
Correct, they could be captured. Correct, yes. But this is what I was thinking that there was an exchange EXCH that played an important role here. There's a chance. I'm curious to see if they're gonna get the same treatment from the US government as they did with Garantex. well, it's a story. I think that...

Was it the CEO of say wallet who said like, yeah, it's kind of a call to arms if you want to me It sounds like a call to arms in the sense that Companies who deal with this kind of money and technologies they need to take security very seriously You can't pretend to you know, you build some technology and you think yeah, this should be good because we are experts in cryptography and this

be good and in the end you get owned by social engineering and a simple trick

Ryan Naraine (01:37:06.616)

Well it wasn't just not a simple trick though, there was like some JavaScript shenanigans on the real real real backend that did the transferring into the North Korean wallets. mean there was like some weird, You're right, right.

COSTIN (01:37:15.754)
That's like how the hack was executed. But to me, to me, the most important step in this whole chain, the heist was how they owned the developer. Yeah. How they tricked him into running this investment, allegedly investment app in a Docker container. And that's how it started. Like that was enough for everything just to fall apart.

Ryan Naraine (01:37:22.444)
was the supply chain, the social engineering.

Ryan Naraine (01:37:33.006)
I'm right.

COSTIN (01:37:41.13)
And it's maybe it's a call to arms in the sense that you need to take security seriously if you're if you're into this business of wallets and cryptocurrency exchanges and magic moneyism. Yeah, it's it's the 70s.

Ryan Naraine (01:37:50.447)
It's a wild west. It's wild west madness. Anyway, Costin, have to go take your ladies to dinner tonight. It's international.

JAGS (01:38:09.102)
Well, I think now we're starting. It's a lot of conversations around sort of like preparing for pivot con, know, booking hotels, folks trying to get the last round of tickets. Yeah. So I think it's going to be great. I'm also pretty excited for folks to like this is the first time the three of us will be at the same place. I say that with hesitation because I have flown all the way to Dubai before.

COSTIN (01:38:17.001)
Mmm.

COSTIN (01:38:22.538)
the agenda.

JAGS (01:38:38.815)
to be on a panel with Ryan and had Ryan not show up. So I don't, you know, I, I'm, I, I'll believe it when I see it. However, there's a chance there's like a sliver of a chance.

COSTIN (01:38:54.39)
19 right 19

JAGS (01:38:55.694)
Damn,

COSTIN (01:38:59.702)
Let's go for it.

JAGS (01:39:00.364)
Yeah. So, yeah. No, I was just going to say, mean, excited for that folks are like getting, you know, trying to get their foot in the door for the last one, but pivot con was great last time. I'm really looking forward to it. And then also more, more in the semi immediate future is black hat Asia, which I'm mostly excited to go hang out with, with coasts in and Vitali and some other folks that's in Singapore. So.

COSTIN (01:39:27.264)
Singapore again come you should come Ryan we can have minty mint tea

JAGS (01:39:30.432)
Yeah. Dude, come to Singapore. We'll have mint tea.

COSTIN (01:39:39.159)
To all the women in security, happy Women's Day. Keep up doing the things, the great things you are. I think it's a wonderful contribution to the industry and there some amazing women working in our field. We need to see them more at conferences, at workshops and yeah, that's happy Women's Day to all of them.

JAGS (01:39:39.63)
you

JAGS (01:40:10.99)
Bye bye.