Episode 30: Three Buddy Problem

CISA takes a victory lap, PlugX removal

LISTEN:
https://securityconversations.com/episode/inside-the-plugx-malware-removal-operation-cisa-takes-victory-lap-and-another-fortinet-0day/

Cast:

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

Ryan Naraine (00:03.502)
Good morning, everyone. It is Friday, January 17th and 9.30 a.m. here in Phoenix, Arizona. I'm here with the three buddies for the Three Buddy Problem podcast, Costin, Rayou and Juan Andres. How are you guys?

JAGS (00:19.03)
Good.

COSTIN (00:19.212)
Good.

Ryan Naraine (00:20.59)
That's all I get.

JAGS (00:19.03)
Good man. Good. just really, well, reeling from a week of like way too many stories. Like I, I don't know about you guys, but I felt overwhelmed trying to do my homework for, for this, this podcast, just looking at the sheer amount of, of stuff that's gotten piped out.

Ryan Naraine (00:39.288)
But this is cyber security. i mean, every now and then I go to the security week and I grab this trending stories list and post it on Twitter and every week it's just zero day after zero day, Ivanti after Fortinet after Microsoft patches.

JAGS (00:52.67)
You know what I'm realizing? I think this may be the first viable publication week after the New Year's. like, I think, think about it, right? Like the January 10th to the 17th, like it's the first week

where you think people are going to be paying attention again. So all the shit you didn't publish for like three weeks around Christmas to New Year's, all of a sudden just comes flooding out. That's my guess, right? As a marketer.

Ryan Naraine (01:00.492)
You think so?

Ryan Naraine (01:20.064)
Let's start with the news around PlugX and the Justice Department and the FBI announcing that they partnered with French law enforcement authorities and a private security company in France called Sequoia to remove PlugX malware from 4,000 machines here in the US. Without the user's knowledge, mean, they went and got a court order and basically did some point and clicking on removing this malware. The interesting part of this to me, Kostian, is

the Sequoia piece. Sequoia is a private cybersecurity company in France. And these guys had helped me understand what they did. from what I understand, does this qualify as what we have been talking about as hacking back?

COSTIN (01:59.094)
Mm-hmm. Mm-hmm.

COSTIN (02:06.209)
I don't think it qualifies as hacking back if you ask me. It qualifies as maybe yet another of these law enforcement operations where they essentially step into people's houses to clean up the garbage, essentially for the good of the ecosystem to reduce the risks and so on.

Ryan Naraine (02:31.084)
without the owner's knowledge.

COSTIN (02:32.935)
without even notifying the owners that they are infected or that they've been disinfected.

Ryan Naraine (02:39.052)
Well, they did. They did include a line that they're working with ISPs to notify folks post-disinfection that they have been disinfected. And in fairness, like if you have this plug X malware sitting on your machine, it's been sitting there forever. There have been multiple, multiple warnings. have been IOCs. I mean, we've documented this thing at length. And if you haven't removed it, isn't it like at some point somebody's got to do something about it?

COSTIN (02:52.897)
Hmm.

COSTIN (03:02.561)

It is, I think we discussed it maybe 15 episodes ago, like when we were talking about old routers and hardware that simply cannot be patched or disinfected and about the government doing something about it. So maybe it falls into the same category. Personally, what I liked in this story, because again, this is not the first time that law enforcement

takes such an action. the Dutch police, for instance, they've been doing this kind of operations for a very long time, quite successfully. So I think what is different here is the fact that, well, the concept of sovereign disinfection, right? So Sequoia created a portal which allowed the law enforcement from different countries to take care of their own backyard, essentially. So that would be opposed to

the Dutch police cleaning everybody or the Dutch police cleaning computers in the United States, which everyone was a bit uneasy about if you want. And the same idea maybe with FBI cleaning computers in Netherlands, France, Italy, Romania and everywhere else. So this portal where law enforcement can simply define what is their backyard.

through IP ranges or CIDR. So they can do that and do two things essentially, send the command to the worm itself to kill itself, which the FBI says they tested and it operates well. So it doesn't involve any kind of abusive access if you want. And the other option is to remotely deploy a tool. So that is like a binary, it's a tool.

Ryan Naraine (04:53.742)
What is that? What is that tool? Define a tool for me.

COSTIN (04:56.874)
a binary that you can run on your computer or the FBI can run on your machine to remove the threat, to remove it, to clean the computer. And here we are obviously opening a big can of worms. If you ask me, it's a Pandora box. I think this has been done in the past. The law enforcement deployed the cleanup tools.

Ryan Naraine (05:18.83)
Why is it a Pandora's box? What's the problem?

COSTIN (05:21.052)
Because like who's responsible if that crashes like it is code created or developed by maybe a law enforcement agency or by another company and then the law enforcement runs it and something bad happens right so who's responsible for it can you really blame law enforcement for something that can happen while on the other hand is if it's functionality built into the malware that is kind of one of the possible expected outcomes

It's inside the malware, it's like functionality. The only thing which you do, you send the terminate command. So it's maybe, I think, more acceptable from a legal point of view.

Ryan Naraine (05:59.712)

I read the affidavit from the Justice Department and they went a great length to make it clear that they used that specific thing that Costin just talked about, this self-delete mechanism. The malware has a self-delete mechanism and they just kind of figured out a way to go use the self-delete mechanism against the malware itself to do the removal. You've been a very, very big proponent of like, dude, we need to stop with this, like, there's a legal barrier here, there's a legal barrier there, we need to go in and do this infection. I assume you're happy about this project.

COSTIN (06:06.496)
Mm-hmm.

JAGS (06:07.283)
Right.

JAGS (06:29.462)
I, I feel like I'm supposed to be happy about it, but I'm not really. I, I'm, I guess I would want to, what I want to separate here is what Sequoia did and like, well, what, what Sequoia seems to have done is properly gotten themselves into,

Ryan Naraine (06:38.926)
Mmm.

Ryan Naraine (06:48.671)
Let's get into it. What did Sequoia do?

JAGS (06:57.748)
just the right position to be able to issue from a command and control server the command to all these different victims to either download and execute a file of their choosing or to run their self delete, you know, a command that was already a part of this. I'm not putting Sequoia down at all. Do not, don't get that impression from me at all.

Ryan Naraine (07:22.478)
Wait a second, it also means that Sequoia broke into a command and control server, right? Is there? Okay, so help.

COSTIN (07:26.277)
No, no, no, no, no, they didn't. So actually they explain it in the blog they published the last year. The malware had an IP address registered as a command and control and it just happened that that IP address kind of expired. There was nothing being hosted there anymore and they were able to rent a VPS with that particular IP address and that essentially allowed them to sing whole

JAGS (07:27.399)
No, not necessarily. No-

COSTIN (07:54.338)
the entire bot night if you want. It's all fair.

Ryan Naraine (07:56.974)
Sorry, Juan. Go ahead.

JAGS (07:57.366)
Yeah, I mean, you could have also done something similar at the telco level, like depending on what tie-ins you have with some of the backbone carrier type folks. Like there's different ways that you can approach this one. And just the standard sinkholeing, would also, in theory, depending on how the malware works, allow you to do something similar. So I want to separate sort of what Sequoia did, what actually happened.

from this kind of sovereign disinfection, FBI getting into the middle of the whole thing. And I say that because what Sequoia did and what, you know, French law enforcement seems to have done is pretty cool, but also things that have been done before. And so it's more of a good thing, essentially. The part where I think I'm supposed to be happy

but actually I'm not, is with the FBI basically like, they basically ran into like the last mile of a competition and like crossed the finish line and said, we did it. And they're like, what the fuck did you do? Like, what did you do? You signed some paperwork. You managed to find a lawyer in DOJ who was not a pain in the ass and decided to like, to just hand wave a yes.

so that the French can do your job for you.

Ryan Naraine (09:27.662)
I don't think that's quite fair. mean, has to go through a legal mechanism in some way. think Sequoia mentioned this very, very bluntly in the bottom of their blog. It's like, listen, this stuff is easy to do, but we can't really do it without the legal framework around it.

JAGS (09:43.848)
That's my point. That's my point. Somebody at DOJ created a problem and then somebody at DOJ this time around was sober and nice enough to invalidate the problem they created for the sake of doing a perfectly common sense law enforcement action.

Ryan Naraine (10:06.914)
And when you say the problem they created is putting these legal guardrails around anything you want to do that you've discussed in the past.

JAGS (10:13.842)
Yeah, look, there's two ways that you can, there's two ways that we can approach this one. There's the specifics in US law, which I am not at all competent to discuss, but like whether you go from the CFAA all the way to just like, just how ridiculous the standard has been set in the

US for what constitutes not just like law enforcement action, but an action in cyberspace, period. And then

I think more abstractly, looking at just how we are approaching and conceptualizing the cyber domain in matters of law and policy and law enforcement and even international law, which is we have, we're so desperate to map out the internet as a like physical mapping, one-to-one mapping to

state sovereignty. so like we were trying to latch on somehow to this space that is not at all constituted in the way that our physical spaces and we want to superimpose some kind of geographical distinctions to where those like you can say the devices are here. Okay, fine. Cool. But beyond that, why couldn't we let's say

think of this whole botnet in abstraction as something that's just essentially its own entity, its own activity, essentially as something that is controlled by whomever controls the command and control server, for example. Right.

Ryan Naraine (11:57.358)
But we're a law and order society though, right? I mean, we need to have these frameworks around it. We've kind of beaten this dead horse.

JAGS (12:03.094)
But what? No, no, But with stuff like that, I think that's where you get like the lawyers running wild and getting to make up their own shit. Because like when we talk about law and order societies, like there's also the concept that you don't generate laws for this for their own sake. Like you don't just curtail accesses, curtail rights.

because you get to have an opinion as a lawyer. Like there is a certain amount of reasonable limitation that you would hope to impose. And I say that because in this case, the overreach is so fantastic on the part of people wanting to come up with legal frameworks that it misshapes the whole of how we talk about cyber activities.

period, right? maybe in this particular case, since we're talking about somebody took an IP and you are affecting devices that are in specific countries. Fine. Fine. Okay. Like you can say that there's like a relatively easy correlate. Like we don't even have domains. We don't have VPS is necessarily like it's just IP to end points. but our discussion about this, were this to be, let's say a bunch of infected

VPSs or like cloud instances would be so much more complex and so much more like we can't possibly get a sign off from anybody at DOJ to do this that it starts to show just how ridiculous this gets the minute you start to even just try to manipulate the legal conceptualizing around it in a way like come on like

Guys, let's get really, really simple brass tacks. If we remove the aspect of this where they could have pushed their own code, because that's where you can start to have abuse, right? Like to Kostan's point, Who verifies what gets sent? In theory, well, but in theory, in theory, if you really like mistrust all government, you think that all government is just somehow out there to like abuse you in some way, then when we start to inject code,

Ryan Naraine (14:12.078)
The Dutch does it.

JAGS (14:25.898)
then you have genuine abuse potential, right? Which is why I think there's so much pussy footing around this notion of, well, we didn't inject any functionality of our own. We had the option to run the malware's native self delete command.

And I say like, want to treat those two separately because we can have arguments about where the limitations should be and how the ideal would be for us to push our own code.

But if we take that situation away and we just talk about the fact that like we're, there's like mountains of process that just came up for the sake of somebody pushing a single command to all nodes from one IP that just says self delete and like that cleans everything up. It's ridiculous. It's ridiculous that we need to think about it in this way. Where is every single victim?

Where is every machine? What country has a sovereign right over each one of these endpoints and like have reams of process and portals and whatever. When we could just look at this as the opportunity of a lifetime to go take a single IP and go every infection from here on out, from this, like routed on this IP, we can just literally type one command.

and be done with this set of activity. there's a disproportionality to it that just feels defeating.

Ryan Naraine (16:04.27)
There's a conversation that's happening quietly on Twitter, ex Twitter, JD Work, Andrew Thompson, this guy saying, listen, this salt typhoon and a lot of these infections are not necessarily or shouldn't be viewed as a law enforcement issue. It should be viewed a lot in a different context so that we can do a lot more aggressive response to it. Do you have a thought on is that what you're getting at? And I bring this up because in...

Three days we'll have a new administration that has at least publicly talked about being a lot more aggressive at going against China and some of these China hacks and so on. Do you think things change in a month from now, two months from now, throughout this year?

JAGS (16:44.79)
I think there's a lot of room for things to change. We actually had a S1 webinar yesterday with Dakota Carey and Steve Stone. I found myself turning it way more like, I think some folks felt

that I turned it a lot more political than I intended, but really what I was trying to do is like discuss just this general forecasting of what's going to happen with the administrations, right?

I think living in DC, it becomes a lot more natural to discuss this sort of thing. But really, if we're going to talk about policy, part of what makes this notion of like conceptual intransigence with cyber policy, like, nothing can change. This is the way it's always been. Part of what makes that feel so ridiculous is that's true for as long as some random person in DC thinks it should be true. And then

It can be not true because that one, a different person walked into that office and they decided, you know what, I don't care for this table. And they just flipped it. And that's it. Like we went from like, this is impossible to this is the way it is overnight. So normally when you get these like,

homeostatic administrations where they're just like more like let's just keep the regime everything going exactly the way that it is. You get that intransigence, sorry, intransigence with, but I mean, look, it means something very specific. It's like an unwillingness to move and budge something that could be budged where,

Ryan Naraine (18:13.656)
He's big words, man.

JAGS (18:26.516)
I think that's the main difference with the Trump administration. It's what we saw the first time around. Like, we need a new shop. Like, sissa. this is stupid. Remove this, like, remove this, change the whole process of how we do cyber operations. Like, the approvals change. Just change it. Done. Right? Like, that's what bugs me about people talking about cyber policy. Like, we should, we should, like, it should be this like Talmudic study of like, unchanging laws. And you're like, no, it's someone's ideas.

they're kind of shitty in this or that way, what's a better idea? And then why don't we just arbitrarily decide to switch this? That's what we're gonna see with this Trump administration is shit is unwritten. It is completely unwritten. And I think that's why you might, it's funny, there's some folks who are kind of frothing at the mouth at the idea of like, okay, take the fucking gloves off and let's go.

Let private companies and contractors get involved. Let people do whatever you want to call hack back, even though it's a dumb idea, but fuck it. Let's just let people do it. Right.

Ryan Naraine (19:32.366)
Yeah, that's why you've been advocating for the last 29 episodes.

JAGS (19:35.688)
Well, to some extent, yes, absolutely. That said...

JAGS (19:44.256)
we're gonna see what that looks like, right? Like we're gonna see what that turns into. I am not so naive as to think that this is just as easy as like, we're gonna take the gloves off and then these perfectly shaped entities come into existence that will do this exactly the way we want it to as opposed to this suddenly being a new thing that Raytheon bills for. And it's like the same assholes who've been like towing the party line in the beltway.

Suddenly have a new offering right like that's not that's not changing how this shit is done That's just changing who it's charged to you

Ryan Naraine (20:23.182)
Justin, if you look at the color of my hair, you've known that I've been around long enough when something like this would have been controversial six years ago, 10 years ago. Today, it's just another news story. So I think what Juan's point about our appetite for being more aggressive at these things is there. And I think we'll start, I think you're right. I think we'll start to see a lot of these things. Under the Trump administration, we'll start to see a lot more aggressive.

approach to doing this. There's a new executive order out that kind of clears the way for that. I don't know how long this executive order will live, whether it'll be three days old or what. But, Kostin, I want to go back. Why are we relying on a Sequoia to do this? And why isn't Sentinel One doing this or some US company doing this? Or do you or CISR have some stand up, some agency that has the capability to do this in tandem with help from researchers and so on? Why are these things so one-offs? Because one guy

in France has the ability to do this C2 thing. you like, help me understand why this isn't more normal and more regular?

COSTIN (21:24.883)
Yeah, sure.

COSTIN (21:29.121)
First of all, need to say that Sequoia are very good. I mean, we know the people there. know the people there. Shout out to our friend Felix who worked on this as well, but he also worked on many other interesting researches. It's always a good idea to take a look at the Sequoia.io blog and

JAGS (21:36.362)
Mm-hmm.

COSTIN (21:56.61)
see what they've been working on. And there's by the way, there's a lot of very interesting research there. I, I,

Ryan Naraine (22:01.294)

Yeah, but there's smart people everywhere. mean, Sequoia, there's nothing, they're smart and brilliant, but there's nothing special about like what they were able to do. Why aren't there more brains?

COSTIN (22:08.347)
Not necessarily. Let me give you an example. It's relatively easy to sinkhole the domain, the command and control domain of something. I've done that thousands of times. know people like Motosan who's done it hundreds of thousands of times. We're talking about hundreds of thousands of domains that got sinkholed.

now to sync all an IP address that's like kind of a bit more tricky because you need to somehow get a VPS that has exactly the same IP address as the command and control server IP and this is like not trivial like you either need to be very lucky

JAGS (22:39.094)
Mm-hmm. Mm-hmm.

Ryan Naraine (22:51.18)
Yeah, but the idea that only one person in the world can do it just doesn't sit right with me. I mean, that doesn't make sense.

COSTIN (22:55.618)
Yeah, but like a look it's the same as I know discovering America like anyone could have done it. Why hasn't anyone done it before Christopher Columbus? It's the same. So I think what's brilliant here is the fact that Felix had the idea and he managed to actually get that specific IP address. Yeah, Felix, I mean, so I think that yeah, that's kind of special. So I can't remember when someone

Ryan Naraine (23:14.968)
Felix IMEI, give the guy his full name credit.

COSTIN (23:25.837)
was successful at sinkholeing a particular IP address without law enforcement support, without a national security agency support and so on. But if you ask me, why isn't CISA doing this and why aren't others? Well, I think that CISA would be the ideal entity to do more of this kind of research. Yeah, yeah, yeah. Maybe they have different priorities. They have different things to care about. So.

Ryan Naraine (23:44.75)
They're very busy with the pledge, my friend.

COSTIN (23:55.412)

like we are getting into other problems here. I mean, if you ask me, yeah, sure, these are the kind of things that would be amazing to see coming from CISA and definitely coming from more companies.

JAGS (24:07.83)
So I think that's precisely my point, right? Like I am not putting down Sequoia at all. If this whole conversation were kicked off because we have the Sequoia blog, we would just be having a conversation about how cool this is. It's so cool, they figured out how to get the IP. It's so cool that they reverse engineered the malware, understood enough about how this is going to work. And they clearly have an understanding about law enforcement that

made them sensitive enough to say, look, for some of these organizations, it's going to require the shutdown command. For some of them, it's going to require a cleanup tool. Let's give them all the option. like, Sequoia was brilliant in essentially making this as frictionless as possible for organizations that have way too much fucking friction to be able to take advantage of what they did. Yeah.

Ryan Naraine (25:03.182)
Like they couldn't say no, right? They made it so easy point and click that you really couldn't say no. There's a self delete mechanism here. There's a way that you can punch a button and see everything in the U S and you punch another button and it's gone poof. Like you FBI can't say no.

JAGS (25:14.41)
Yeah. So Sequoia, Sequoia fucking killed it. But what I want to focus on is like, look at how much goes into somebody literally like putting your hand over the easy button and like, and yet like, what are you, what is the FBI celebrating? Like that they found a way they, in this particular case where somebody did everything

for them and and like and it's not even something they have to act on in any way all they have to do is sign enough papers to say we're not going to turn this into a problem for no reason like what the fuck are they selling like what is this affidavit where you're like my god this is great you're like

Ryan Naraine (26:06.744)
Well, somebody has to document it. think you're being a little harsh on law enforcement here. Like law enforcement had to do, law enforcement in the U.S. had to manage it and they had to get a court order. They have an affidavit. They had to put out a press release like me.

JAGS (26:17.406)
I know, look, no shade on the FBI agents who took care of this and actually made it happen. Had they not, yeah, had they not done the work, this would not have happened. At the same time, like, fuck the DOJ people above those agents who have made this so hard and don't seem to think there's a need to make it easier.

Ryan Naraine (26:22.68)
Shout out to those guys,

Ryan Naraine (26:40.326)
This does not get rid of PlugX. This is just one variant of PlugX that's being used by one group. Can you back up a little bit and help the audience understand what is PlugX? Just give me a little bit of the history.

COSTIN (26:43.935)
Yeah, it's the must.

COSTIN (26:51.316)
yeah so this is like this super flexible malware that's been around for at least 10 years maybe i've seen the first versions of that 2008-2009 if i'm not mistaken so it's been around for a very long time and there's like multiple versions there was another one that was super famous which was poison ivy if you remember that that's even older probably than plug-x

Ryan Naraine (27:04.017)
2009, yay, it was around the Aurora timeline, yeah.

COSTIN (27:20.693)
And then at some points we even saw like a mix between Poison Ivy and PlugX that some people called Poison Plug and I think that was particularly super popular with APT 41 for instance, I mean among others. Then at some point like even more sophisticated versions appeared like Big PlugX, PlugXB, PlugXY, PlugY

And most recently, think a lot of groups have just simply replaced PlugX with other platforms like PhantomNet, I think is one of them. And ShadowPAD is, let's say, the equivalent of PlugX from 10 years ago is ShadowPAD, basically. That we, I think we spotted for the first time with the NetSarang supply chain attack.

JAGS (28:05.494)
Shadowpad.

Ryan Naraine (28:07.404)
Is it all Chinese?

JAGS (28:12.63)
Mm-hmm.

COSTIN (28:19.947)
So nowadays it's, guess it's mostly a shadow path. But yeah, in this particular case with PlugX, this was a version of PlugX that had the ability to replicate. So I think this is why, because

typically with PlugX, you're talking about like a handful, like a dozen victims, but here we're talking about thousands, tens of thousands of victims. And the reason for that was this ability to replicate. And obviously it was important

to stop it and to disinfect it so it doesn't keep spreading like over and over and then eventually someone finds a way to hijack it and do a lot of evil with it. I was just thinking by the way when I saw the FBI press release I was like reading it very carefully and there was one line which attracted my attention and said like this amazing like somewhere in the middle very small like we are so good and this is amazing and look at all these fantastic things that we've done.

And all this was possible with the help of a French company. that was like every say. And I immediately clicked on the link. Like which French company? mean, this is like in my opinion, this is the big news. Like that is the biggest part of the whole FBI press release that they've done it with the help of a French company. I was like, which company? And then I clicked and it went to Sequoia. I was like, okay. Now it makes sense.

Ryan Naraine (29:44.62)
I think this is the point Juan is making, right?

JAGS (29:44.63)
I think that's a, and it's not just that. it's not just, like Kostin is nailing exactly where my discomfort comes from, but I would take it just a tiny bit further, which is to say that I wonder if this would have been possible at all if they had, if it had been a US company or if it had been a US law enforcement action in and of itself.

Like I wonder how much of this is just like, we found a way to legally not get in the way of these people doing this versus like, if it were here, if it was us, right? If I like, I made this portal, Silas makes this portal. That's much more plausible, right? Like Silas makes this portal and we go to the FBI and we're like, okay guys, like, let's go.

I'm not saying that I don't know FBI agents who would be eager to try to make it work. What I'm saying is I'm sending them like an uphill battle. Like I'm sending on an uphill battle and this is like an unalloyed good that we all want to see. So why is it so hard? Like why have they made it so hard? Because it doesn't need to be this hard.

Ryan Naraine (31:09.101)
The Sequoia folks called this a proof of concept for quote unquote sovereign disinfection and it's fascinating that the US and the FBI was not alone here. They did in total 59,475 disinfection payloads were sent during the campaign including 5,000 plus IP addresses and they made the point that the legal framework and conduct disinfection operation were done for like 10 countries.

So, you know, they created this point and click thing and we got the FBI press releases, but it was widespread around the world. And I repeat the question, like, why isn't this available for

more US companies? Like, why aren't more US companies doing this? Why isn't this the norm? Why are we sitting around with all this shitty malware running around our networks and we're blocking ourselves from removing it when it's clear that we can?

Ryan Naraine (32:00.376)
Nobody has it.

JAGS (32:00.618)
Because, well, because I think we've made this into this fake land of liability, right? Like, let's think about it, right? These are, there is no integrity to these machines that we need to really maintain, right? Like they are infected by a piece of malware that a threat actor has leveraged by, for God knows how long, at least this.

We know this one infection, they may be infected by multiple other things. They may have been used for this, that, and the other. this notion that like it's this perfect integral system is already flawed. And then we've kind of given ourselves this idea that like, don't know A, like how this Rube Goldberg machine of

computer software could somehow like spark a critical failure that we'd never thought of. And then we want to imagine that there's one machine amongst these 59,000 that's like operating a respirator for a baby in a hospital ward somewhere. And like everything is gonna go wrong and this malware is gonna blow things up.

And that baby's gonna die. And you're like, A, I mean, we made this up. We're not even sure respirators work this way. Like, this is like, it's a completely fictitious situation. No. Well, but my point is you're, you're protecting a

Ryan Naraine (33:40.814)
There's a risk of something going awry though. Not at all. We should just go in and delete malware everywhere.

JAGS (33:54.592)
fake notion of integrity that you by virtue of what we're doing know does not exist. Tomorrow, they could wipe every machine that's infected with PlugX and we would functionally be in the same situation as had we tried to disinfect it and then everything went wrong in some way that, you know, happens all the time for Windows machines, period, right?

It's, it's, there is some,

Ryan Naraine (34:27.598)
Fix it. Fix it for me. I make you king for a day. Fix it for me. What do you do? Do you give Sisa the power to create a little department that just does only this in tandem with private come like fix it for me.

JAGS (34:40.488)
I so this is it is a thorny problem insofar as you have so many gradations of what you can do. Like and that's not me copping out. It's to say that I think I can come up with some. Yes, but look just hear hear me out and how I want to parse the problem. I can come up with some scenarios that I think we would all think are OK.

Ryan Naraine (34:56.952)
Fix it.

JAGS (35:09.224)
And then when we start getting into the incremental sense of what's okay is when you easily get into where it becomes not okay. So I'm not saying that this is a one size fits all completely easy problem. What I, if you ask me how to fix it though,

This is an example of many operations that have been pretty thoroughly understood, have been studied for a long, long, long, long time. We know a lot about the threat actors. We know a lot about the victims in general, how the infrastructure works, how the malware works.

JAGS (35:59.432)
If somebody can get to a command and control server, if somebody is empowered at a big backbone network to get in the way of this, and we have such a clean, simple mechanism as just self-deleting the malware, we're not even going a further step into like, there...

Plugins is there a second and next capability? Would you restart the machine like that again? That's where you start to get into sort of more slightly more problematic areas But like when you have this clean a situation it's clear that the lawyers in the room are just there to inject friction and those are the scenarios where I say I think CISA and The FBI and whomever else is supposed to have a stake for some reason

needs to be able to come out and say like, look, we just understanding from what is understood about this operation, it is a reasonable enough action to mitigate existing harm. Something bad that is already happening and the probability of something worse happening on the basis of our action is infinitesimally small.

compared to the bad thing that is already occurring.

And those are the scenarios where like you should be able to just say that like this is this is the equivalent of like, you know, there's somebody getting kidnapped in front of you. And like the cop is not going to the cop that's standing right there is not going to try to help this person that's getting kidnapped because there's the possibility.

JAGS (37:52.938)

that they might spook the driver and the car goes careening into a school and it kills 400 children, it starts a fire, it burns down the whole city. You're like, guys, come on, like, existing harm versus potential harm.

Ryan Naraine (38:04.59)
That's a very...

That's a very, very long way of saying it's very hard to fix. Okay, so then fix it for me.

JAGS (38:13.266)
No, no, no, no, no, What I'm saying is. Because this is DOJ and this is lawyers and they love arguing for a bro. Hey, hear me out, hear me out. I like no, my point is it's there's no one size fits all solution. But if what you were if we could just if DOJ and CISA could tackle this as an opt out.

Ryan Naraine (38:22.104)
So fix it, fix it, you go up to the DOJ level and fix it like.

JAGS (38:43.318)
problem rather than an opt-in problem, I think we'd be a lot closer to just delimiting which scenarios are a no-brainer. And you already set one legal path because it's already been argued that in this scenario where, okay, let's say someone who is a Western allied nation has access to doing a thing and it will disinfect machines in our country.

based on an existing self delete mechanism and no further code being pushed. And you say, in that scenario, if you hit those six requirements.

Absolute green stamp, no problem in the US, disinfect anybody you fucking want. That has been legally argued and approved. Maybe you need to reach out to the FBI and they give you like a little gold sticker and that's just like there, done. Then you have carved a significant path forward wherein all these wonderful public servants who just want to do good shit, they know as long as we structure it this way,

We can get this done and we can go from this, like instead of celebrating disinfecting like 4,000 machines, we can do this on a weekly and monthly basis because you have delimited what is okay. Instead, we're sitting around waiting for some legal case to define some precedent that justifies why we can't do this and why we can't do that and why we can't do this. It's like, okay, well, what the fuck can we do? Can you just spell it out?

Ryan Naraine (40:23.514)
How is this different from the malware, the Microsoft monthly update of this malware removal tool that was that I don't know if they still do it to be honest with you haven't heard any reporting on it but on patch Tuesday every month Microsoft would like do a malware removal a mass removal of malware they probably still do how is this different from that

COSTIN (40:37.109)
Yeah, they still do it.

COSTIN (40:43.464)
Well, another good question here, I guess, is why isn't the Microsoft malware removal tool simply removing this plug X variant? So one of the possibilities here would be that these were all very, very old computers that just didn't get that thingy. That's one possibility. I don't know, honestly, if the malicious software removal tool, that's a full name, MSRT,

Ryan Naraine (41:02.582)
and get patches.

Ryan Naraine (41:11.796)
MSRTA.

COSTIN (41:12.445)
actually removes this particular plug X variant. I don't know if it does.

JAGS (41:15.36)
Well, what obligation does Microsoft have to disinfect anybody? And that's a conversation. like this is going to come off bad because I work at a competitor, right? And that's always been the issue with thinking about Microsoft, the ecosystem maintainer, as a security vendor as well. That's what makes it so bullshit. like, can you define to me

what Microsoft's obligation is to disinfect a computer it knows has malware on it. Because there are obviously circumstances where they don't.

COSTIN (41:56.258)
Well, for sure, I think it's in their advantage to clean up the computer. It's their advantage for sure. But I mean, I don't think that's probably the most important thing here. I was just thinking that there are like variants of this operation which can be done and maybe they're less intrusive and they do make a difference. So just as an example, pure, simple, random example is you...

JAGS (42:00.224)
for collecting signals.

COSTIN (42:25.673)
your SISA like and Juan is the head of SISA, new head of SISA Juan. So he starts working with ISPs and he says like, listen up guys, I want you all to keep tabs on people who are connecting to this IP address 45142166112. And if someone connects there like more than 20 days a month, then you block their internet and

like they're gonna call you and say, hey, my internet doesn't work anymore. You're gonna say, you have a malware, install an antivirus, remove it, and you'll get back online. So that's, think,

one of the things which is being done in other countries and which works really. So this can be very easily automated for many different variants, but you need the cooperation of ISPs because people will be calling like, hey, why isn't my internet working? Well, you have a virus.

Ok, what do I do? Install an antivirus. Which one? Ultra-EV.

JAGS (43:25.714)
See, that is that much more unacceptable in the US. But like, just think about this. I agree with you in some common sense world where cybersecurity is most important thing on earth. But in the US, the notion that I have taken away something that you're paying for and contracting because I've decided what is important for you to take care of in this given moment.

COSTIN (43:31.307)
To me it's not, to me this is like a soft, it's a soft approach.

JAGS (43:55.794)
is a paternalism that I look, I'm not saying that I'm not saying that this is what I agree with. I'm saying that it's a paternalistic attitude Americans.

COSTIN (44:02.081)
can ask you one thing. What happens if you drive on the street with an expired driving license?

Ryan Naraine (44:11.874)
You get pulled over and you get a ticket and you don't drive until you get it renewed. Not unless you renew your license.

COSTIN (44:11.969)
You get pulled over and you get in trouble, right? Can you drive afterwards?

JAGS (44:13.397)
Yeah.

COSTIN (44:19.931)
Alright, so it sounds similar to what I'm talking about,

Ryan Naraine (44:23.82)
Yeah, but what caused the what? Sorry, go.

JAGS (44:23.99)
It's not. It's not at all. Well, it's not at all because like we don't let like you don't you're not born with a natural right and access to driving. Like it's something that you have to earn. Like you have to go get a license in the first place. Right. Like children can't turn 16 and suddenly drive. They have to go through a course. You have to. And in a way, essentially, it's like a this tall to ride thing. It's not very tall, but like

there is a bar that you're essentially, somebody has to sign off and say, okay, you're not insane and your eyes work well enough and you kind of understand the rules of the road, you're allowed to do this. We don't do that, right? Like you don't have to pass a test to get on the internet. And in some ways, I don't think that that's what we actually want to happen, right? Like I think for technically sophisticated people, that's how we tend to view the internet. And you go like, ugh, why can't everyone be lit?

Why can't we just live in our cool internet of the 90s where it was like, you needed to have enough skill to even show up to the party. So much cooler people were chatting. The internet has become like essentially a universal human right according to certain organizations because of like the availability of information, education, et cetera. The notion of like,

telling people that it's so important that they become disinfected with something they were infected with for six months and like it didn't end their lives. And like, but we will take away some of your access to this thing. Like that's just a really hard sell. But I would posit an example that I think is in line to what I hear you arguing for, Kosen, which is if we know the malware will self disinfect, self delete.

Like when you remember like some of the equation stuff where like if it's if it can't reach the internet for three weeks or for 20 days, it will self delete.

JAGS (46:30.122)
That is a situation where we can literally, like, you don't have to cut their people's internet. You can literally just say, well, let's just block their access to, like, routing this particular IP.

Ryan Naraine (46:44.538)
How does it work in Europe? Like you mentioned, there some European countries that does this quarantining. They just kind of shut you off.

COSTIN (46:47.424)
like I said yeah yeah absolutely I mean I spoke to to people working at ISPs which they do they do this when not not for everyone obviously but for the big offenders which are actually starting to let's say affect the stability of the network or some count somehow let's say in fact other people send spam like these kind of things like this kind of

really abusive behavior. So they do cut their internet. And those people call and they said like, yeah, you need to install an antivirus because you're full of malware and you're degrading the internet for everyone.

JAGS (47:31.626)
That makes more sense though, right? Like I think that scenario makes a lot more sense in that you can argue that their existence and their connection to the internet is causing harm to others or degrading the system performance for other people, right? And that's where this is so

interesting that we're talking about PlugX where it's like, look, this is an espionage platform. It's a modular thing. It'll allow them to do more things. But essentially like this is an info stealer.

It's not a DDoS capability. It's not, you know, it's not something that will.

COSTIN (48:05.333)
But this one was a worm which infected other people's computers. So you would be responsible for propagating it to other people.

JAGS (48:17.846)
We're splitting hairs. Look, we're splitting hairs.

COSTIN (48:18.399)
But like, listen, like, of course, of course, and to be honest, what you were saying about internet being people's fundamental right while driving is not, that sounds like a lawyer talk to me. And to be honest, I'm not good with that. But there are all sorts of like shades of gray if you want. I was thinking like, what else is on the table? I mean, you were talking about

Breaking people's routers if they're like too old to patch what was it the? Not the appropriation, but you called it You use the specific term for it. What was it?

JAGS (49:02.39)
think we talked about eminent domain. Yeah.

COSTIN (49:04.125)
Eminent domain correct correct so just breaking people's routers because and again you're talking about hardware destruction when those routers don't actually post threat to to other computers on the network either and that would also effectively cut someone's internet access because their router is kind of dead if you want but I was thinking like what else is on the table and How about this? Let's say FBI

They make a website where you can go and download the disinfection tool for plugs. And the ISP tells them like, hey, go to this FBI site, download the tool, clean your machine and everything will be fine. Or then the next layer, FBI creates a website that if you visit that website, it uses a zero day to install the disinfection tool on your machine and you're fine. Like you don't need to do anything. And three, like the third layer,

JAGS (49:57.61)
Ha!

COSTIN (50:02.855)
FBI works with the ISP to simply inject an iframe to their side with the Zero Day and the disinfection tool in people's traffic and it's all like cleanly disinfected and nice and neat and everything's good.

Ryan Naraine (50:19.126)
Is that already happening in Europe?

COSTIN (50:21.089)
I don't think they have the zero days but I'm just thinking like this are this on the table? I mean we've been talking about being more aggressive we need to fight back we need to be taking a more solid position I'm just wondering are these like science fiction scenarios or is this actually coming maybe not this year next year is this coming?

JAGS (50:45.462)
It's all in the it's in the eyes of the policy beholders. I think I think that's precisely my point It's hard to respect the people that right now are keeping their foot down saying this is not something you can do when tomorrow somebody can just walk in and like Grab an eraser and be like, nope doesn't matter. Go do it like all the neat

COSTIN (51:10.625)
Everything is on the table.

JAGS (51:11.89)
All that needed to happen was one random bureaucrat being like, yeah, why not? And you're like, that's it? Like, that's what was missing? That's what was keeping us from being able to do this? I think that's what I'm getting at. It's not that there aren't good arguments to be had. It's not. It's just that there's almost like an arbitrariness to it that makes it.

There's an insane delta between the hyperbolic level of importance we give this when we talk about it and the complete inability to move the smallest thing when it comes to the bureaucrats and the folks that are actually managing the processes. You can't tell me this is the most important thing on earth and also tell me that it's not worth

filling out some paperwork, right? Like, just odd.

Ryan Naraine (52:13.262)
can't believe we're in an hour and we're still on the first story. Quickly, the White House issues an executive order, cybersecurity executive order, Biden's executive order as he's leaving. It includes a call for, I think it's kind of like an aim to make it easier for US authorities to penalize foreign governments that target US with cyber attacks. Is that related here or is this just sanctions related one?

JAGS (52:43.998)
No, mean, the EO is pretty interesting and I don't feel completely comfortable sort of even characterizing it because effectively there's what this is as a political act and there's what this is as like a matters of policy of like specific things. like to kind of air out the politicking here, this is a very

typical thing for an administration to do when there's going to be like a handover to another party where you say, we think these are all important things that need to happen in this area. So we're just going to make them law like overnight and make it so that the other administration has to undo what they have said. Like we think this is important enough to make it law. You need to make a point of

undoing this the day that you walk in. And I mean, like a Trump administration might not give a shit. Like they will just probably walk in and be like undo every anything and everything that Biden ever did. Right. Like that seems to be right. Like. Yeah.

Ryan Naraine (53:51.672)
Cyber security is a bipartisan issue in this country. feel like in general it's a bipartisan issue and like a lot of the goals and aims of the executive order fits with what the new administration has been saying.

JAGS (54:03.666)
And if even if they agree with them, why would they want Biden to get credit for having put them in place? You know what I mean? Like that's where the politicking bullshit takes over. So this stuff may not even be worth the pixels it's being displayed on. Like it may not live for longer than like 45 seconds, but it does give you a sense of what the.

the experts and the folks in this administration thought would have been the things they would have liked to accomplish maybe in a second term or in a camel administration.

Ryan Naraine (54:37.12)
issue at two years ago, like all these problems, all these problems are not new. This is not the problems that popped up three days before January 20th.

COSTIN (54:38.881)
Mmm.

I wanted to ask that.

JAGS (54:42.574)
Now, now you're speaking to what I was talking about with the plug X thing. Now you're talking about what I was talking about with the plug X thing. If this was that simple to just hand wave and you're like, OK, as of today, everything we said before that could not be done can now be done. Yeah, why the fuck couldn't you do it before? Why couldn't we have more comprehensively? And I'm sure the answer is

come down to all the, you know, a bunch of like bigger political problems. There is a general intransigence in these administrations and like unwillingness to like rock the boat and almost

like pussy footing about like taking big swings. Which is probably why we have a massive anti-establishment vote that just secured a Trump administration.

Ryan Naraine (55:37.006)
Just along those lines, we have Jenny Steele, Jack Cable and the CISA folks doing a big giant victory lap around how amazing they were at CISA, spent $3 billion a year. And what I found fascinating, and I hope this is the last time we're going to talk about this stupid pledge, but what I found fascinating was like, this is the highlight of what CISA has been able to accomplish. According to their own victory lab, Jenny Steele issued a...

an exit document that just describes this amazing secure by design pledge that suddenly Google and Microsoft is amazing at security now because of a secure by design pledge. Jack Cable is being interviewed by Cyberscope and again, doing a victory lap that they pledge. And more importantly, these progress reports that these vendors are issuing post signing the pledge is a sign that we run in the right direction when 90 % of all these stupid project progress reports is a press release that they signed a pledge. Like Ivanti, for instance.

Yvanti's progress report is that one, they've been given, they're now a CNA and two, they have a vulnerability disclosure policy. That's their progress report. And this is being held up and, and cyber scoop on these guys. I don't want to go on a Juanito rant here, but like, the fuck are we really writing about?

JAGS (56:49.45)
Do it, man.

Ryan Naraine (56:53.806)
Like there is no critical analysis, no one is questioning how this $3 billion was spent. What are the real accomplishments? And I want to throw the question to you, Juan. What do you think in your mind, in all seriousness, has been CESA's, on the journey to least, biggest accomplishment?

Ryan Naraine (57:14.35)
Good one, Kostin. No, I mean, this is a $3 billion a year agency. They've done a lot of work around, you know, issuing guides and guidances around, you know, securing critical infrastructure here. I'm pretty sure they're doing a lot of incident response. I mean, they must have been involved in a lot of this volt typhoon incident response. Like, why aren't we hearing those stories? Why aren't they, like, why is the pledge the big thing?

JAGS (57:41.226)
they must have been is not something I would assume. don't, you

I have a hard time. No, no, no, I'm having a hard time genuinely characterizing it, which also I think, you know.

Ryan Naraine (57:50.85)
You're holding yourself back, probably on purpose.

JAGS (58:00.594)
I may not be in a position to just like recency bias, right? Like to really remember. Like what have they done? You know, the CSRB is a nice step in the right direction. Some folks got some cool stuff going through there. There was, I think earlier days when it felt like Cisa was still in the game as far as like trying to enable some collaboration and stuff.

I think it really, it's hard to look back at some of those things without like having a very bitter taste in my mouth with how much work me and like a bunch of other people personally put into building things up. that, I think that's what, what makes it so, kind of painful to be on the out with Sisa, in that it's

Now I look like a complete detractor when it comes to this organization and that makes it easy to forget that Jen used to shout me out from stage at Def Con and that you had all this stuff with JCDC and whatever that me and a bunch of the usual folks were doing work with them. But that's just looking at me as a malcontent and forgetting that like...

I spent hundreds of hours literally doing free work for the US government, including CISA, on the premise of, we're all here to try to make this community stuff work, right? Like you want to put a house, like you want to say, okay, we're like doing this, you know, in good faith and good conscience, you don't just like act so cynically that you go, fuck you.

this is never going to work, you show up and you say, okay, you want to put in some effort, I'll put in some effort with you and like, let's see, let's see what we can accomplish. And it's, I think CISA ultimately showed itself to be very much sunshine friends, right? Like we saw that most clearly with the, the CTI league with the efforts for like the, God, what was it?

JAGS (01:00:24.35)
What they were trying to curtail for misinformation, disinformation, where they literally pretended to put a board together one day and then the next week they disavowed it and the woman they were putting in charge of that has been getting harassed on the internet for months on end just on the basis of this random bullshit initiative we decided thoughtlessly to make today and to leave behind tomorrow. So I think it's easy to forget

that CISA was not always on the out with the InfoSec or TI community. There was a period where everybody really, really, really tried to work with them. then, so there is a lot of bitter disappointment that comes with having put so much fucking work and time to trying to make their initiatives work, to try to make them real, to advise them.

to meet with them and say, hey, this is how you should be doing this. Hey, you can have all of our time. You call us like, well, you have my phone number. We'll personally sit down and like walk you through this thing. Like before you do something dumb, like call us. Like we can all sit

with you. We'll help you out. Like the amount of that shit that was put forth to them is what fuels the bitterness now where we're all kind of like, this place. Because what we ended up seeing was the only thing that mattered

was the PR. The only thing that mattered were the victory laps. The only thing that mattered was every time we go on. Yeah. Well, and I mean, it's at that point, I don't I won't speak for anybody else, but I'll say that I personally started to feel kind of used. I felt used being like called in for a photo shoot that just goes posted on Twitter within 20 minutes to promote a talk at Defcon. And it's like

Ryan Naraine (01:01:51.182)
The freaking photo shoots, the freaking photo shoots, like...

JAGS (01:02:15.848)
We could have met up and talked about like real shit that needed to get done and thank you for the challenge coin. But like what mattered was the photo shoot and then you would go, hey, we're going to follow up on this thing. Like this important thing is happening. Yeah, absolutely. Talk to so and so about it. Nobody calls you, nobody answers. And that's the end. You're like, okay, well, so the whole point was the photo shoot. And like that's what

Ryan Naraine (01:02:41.038)
I don't want to pick on Jack Cable, but by all indications, he's a brilliant guy who has done, I've only heard good things, but about a month ago, CISA did a panel discussion on secure by design, secure by default initiatives, and literally on LinkedIn, the invitation to this panel was, please come, you'll get to take your picture with the pledge. It's like, what are we doing? What are we doing?

JAGS (01:02:47.318)
I've only heard good things.

Ryan Naraine (01:03:08.942)
The reporting is that, the reporting of the political is that Sean Planky, a former US Coast Guard veteran of the Pennsylvania National Guard and US Coast Guard is the pick to lead CISA. CISA, remind folks, was implemented by Trump by law. So you really can't just get rid of it very, very easily. Do we know who the Sean Planky guy is? Juanito, have you ever met him?

JAGS (01:03:35.39)
Really, was, I don't know. I don't think so. Interesting to see like a sans profile. You're like, okay, cool.

Ryan Naraine (01:03:43.97)
Yeah, which means he's been around, in the security world for a little bit, worked under the Trump administration, the previous Trump administration. So hopefully, and just one other point on the goodwill thing you mentioned feeling used. This goodwill extended across the industry as

well. know, CISO had a black hat keynote, like I believe four years in a row. were on DEFCON stage four years in a row and in very, very like, you know,

positive, everyone's there to clap, take pictures, like, you know, Dark Tangent was like, you know, a big giant cheerleader for CISA. And I wonder if these folks feel like we've gotten what we were promised out of CISA. don't know.

JAGS (01:04:25.664)
I don't know. I think Dark Tangent in particular would have to... I would love to hear an honest sense of, now that it's all said and done. Because Jeff Moss personally has ascended in these ranks as well. And it's great. I think he is a good... Well, he's a good...

Ryan Naraine (01:04:47.331)
Yeah.

He's a cheerleader, he's become a cheerleader though.

JAGS (01:04:53.898)
He's an advocate for hacking as like what it's always been, right? Like hacking is not a thing that should be like considered a pariah. You shouldn't go after, you know, security researchers as like bad people. It's all been about creating like, it's like a 20 year journey or 30 year journey to like give a venue and a voice and a normalcy to what was before considered something deviant by nature.

And in that sense, okay, the mission continues. Is that the best advocacy?

Ryan Naraine (01:05:25.656)
Where's the anti-establishment spirit though? Where is the anti-establishment spirit into holding these people accountable, questioning authority, you know, demanding excellence from your government figures. we put them on stage and we clap. Like what is going on?

JAGS (01:05:38.774)
Well, let me, let me, let me.

Look, yeah, no, I'm remembering now like the beginnings of the sort of like the downfall with CISA and like Jenny Sirleaf, Jenny Sirleaf's love affair with like the InfoSec industry and like all these, you know, all these people sort of swarming around and supporting. I think it really starts to get telegraphed by

Ryan Naraine (01:05:43.778)
I'm aggravated.

JAGS (01:06:11.686)

a different Cyberscoop article, was like, surprisingly, I had a really weird time with it because we were all surprised by the article in some way. And I found that if you read it very carefully, there were a bunch of stories, a bunch of interesting stories shoved into it as like throwaways.

But the whole story was so about like the cosmetic elements of Jen Easterly stardom that none of that stuff got addressed because of the way that it had been presented.

And what was odd enough is like, it was so clear that a lot of people were speaking up about things that were not going well. Like wheeling and dealing with like Republicans and like all these issues where like, hey, yeah, JCDC is supposed to be like this whole thing on a Slack, like nobody's logging on. You know, they like logged everyone out and didn't realize for two weeks that nobody could sign back on. Like that's how much engagement is going on.

Things like that did not get any attention whatsoever, but you had people whom are big voices in the Defcon space and on Twitter, but who I believe, and at least in my experience, had no experience collaborating with SISA, coming out to defend immediately, rabidly.

that people were talking this way about Jen and Sissa and not giving any credence whatsoever to what was being sort of just glossed over about folks basically saying, hey guys, things are not working behind the curtain. And that was the beginning. Then there were many articles like that that kept sort of like just chewing a little bit and just kind of showing that there was some malcontent, but at no point was that ever.

JAGS (01:08:21.312)
given validity and at no point was that ever addressed. There was never a moment to say, hey, okay, like maybe we're not doing what we should be doing or like maybe we could be doing more or like, okay, like let's pay the bill for all of the goodwill that has been given to us. It's like, no, well, we can't benefit from these people anymore. Fuck them. Let's go, like what's next?

Ryan Naraine (01:08:43.288)
Yeah, I remember the article. think it came across very anti-Jen Easterly almost. I, I, there was some feedback I got. think I spoke about this with my, our friend Kim Zetter. It's like, if, if Jen Easterly was a man, would that story have been written? There was a little bit of that as well. And there was some tone in there that sound, that felt very personal. I remember at the time calling myself team Jen because of how personal it felt. there was like probably some reporting issue.

JAGS (01:08:47.082)
Mm-hmm.

JAGS (01:09:08.394)
I know we disagreed on that a great deal. I won't speak to, well, actually I will speak to it. No, I don't think that that angle would have been put on it had Jen been a man, right? Like the level to

which it hyper-focused on her image, it was not a good look. And that's not how I think it should have been reported, right?

Because again, what I'm fixating on is yeah, but read the paragraphs in between like there's a lot of things that had never been said before in here that are red flags all over the place and like they were never addressed at the time. It doesn't, you know, it doesn't do away with the fact that like, yeah, the angle and I think that's what defeated the article. It's what made the article a failure. It could have been reporting on like

finally a glimpse within what is actually happening at SysHunt, like maybe not everything's okay, and instead it became cosmetic.

Ryan Naraine (01:10:12.942)
Costume does this bore you?

He's sitting there rubbing his chin.

COSTIN (01:10:16.641)
No, but I was I was thinking that after you guys discuss all this American things, you'll come back to me and say, what is Europe doing? Like, how is Europe better than us? And yeah. Well, you can see is that in Belgium, that's the cybersecurity center, Belgium, which, by the way, doing some amazing things. So if you if you want like one recommendation there.

JAGS (01:10:17.411)
He does look bored.

Ryan Naraine (01:10:28.514)
What's your equivalent for CSA? Does the European Union have an equivalent?

JAGS (01:10:43.03)
It's not fair to any of them to say that.

COSTIN (01:10:45.217)
They are my friends obviously but they are amazing people. Copy CCB, like look at what CCB has been doing in Belgium and copy what they've been doing. If you want like some practical advice because I was thinking that the reason why this didn't go very well with CISA was that they were very strategic.

Ryan Naraine (01:10:49.058)
What should we copy? What should we be copying from them?

Ryan Naraine (01:10:59.63)
Give me an example. Give me like two or three examples.

COSTIN (01:11:08.363)
Like pretty much all these decisions they were making were strategic. Like let's build this framework. Let's do this pledge. There was like mostly strategic and marketing slash image building. But what was maybe lacking, not entirely missing, but lacking was the tactical measures, like the practical stuff. I'll give you some example. Like set up a MISP server.

Ryan Naraine (01:11:19.256)
Nothing operational.

COSTIN (01:11:36.48)
share IOX with the industry, share it like in a coordinated manner and constantly share stuff. Set up a alias where people can just forward all suspicious emails they receive. Start collecting intelligence from the wild and use that to enrich your own intelligence and share it back with the community. Create a training program where young people can...

Intern learn more about cyber security how what it means to be in cyber security Try to develop partnerships with university so that we have more people doing reverse engineering writing good. Yeah, I was All these things so like practical stuff not the strategic Paper signing things that Help with the image, but they're like not very tactical. So because if you want to win the war

Like if you want to win in this field, you need both strategy and tactics. And I think that the tactical side was kind of missing.

JAGS (01:12:41.268)
Yeah, I think that's a

Ryan Naraine (01:12:41.422)
How do we get this guy to come to the US and run?

COSTIN (01:12:45.419)
me?

JAGS (01:12:45.556)
I mean, you can come tell them that and maybe not teams done. You're already out. No. Look, I have to say it's not the first time they would have heard that. Right. Like that. That's I think fairly common sense advice and it's great to see how it's followed and enacted slightly differently by all. But like successfully by all these different countries like, you know, the Dutch.

COSTIN (01:12:47.987)
I can do consulting over zoom, definitely not teams but zoom is fine.

JAGS (01:13:15.616)
talking to the NCSC, you know, the Australians, the Spanish, the Israelis, like everybody's working, the French, everybody's working hard to like have some, you know, have skin in the

game and figure out. And I think in those cases, what's interesting is like almost a recognition on the part of the smaller European nations that they needed to be useful and practical and quick.

Ryan Naraine (01:13:17.838)
The Australians do a great job as well in some of this operational stuff.

JAGS (01:13:42.568)
somehow and to Kostin's point, right, it made them very tactical in a way that made the relationship feel like it was a relationship, like it was a two-sided thing. You're investing this much trying to do this one piece that you can do, let me help you and enable you and like you kind of have a back and forth. But to Kostin's point, that's a very bottom up and a very practical and a very tactical approach.

It does not make for good copy. It does not make for headlines. what made all of these different ventures so disappointing and why I'm okay with the pledge being a punchline is that it's right in line with what we always saw. Big news, big parade about how like, this is what we're gonna do.

and then no follow through whatsoever. Like you would go look inside of there and be like, so who here is in charge? Like who, no, who here is in charge of the initiative that got announced on stage last week? Is that even a thing? Like, is it real? Is anybody back here actually following up on that? It's like, no. So what are we talking about?

Ryan Naraine (01:14:43.394)
progress reports bro.

Ryan Naraine (01:14:59.758)
If you have any listeners who know this Mr. Sean Planky, please send the podcast to him. Costin has some really, really good ideas there. Just to close the loop, do you think the pledge has long term shelf life? mean, let's be, let's give them the benefit of the doubt that these progress reports will eventually shame these companies who did not do these nine things that they pledged to do.

down the road six months from now, a year from now, two years from now, as we continue to get these progress reports, we can see that Ivanti hasn't done much or Fortinet hasn't done much or whatever it is. And there's some name and shaming component to it. Do you think there's life there or do you think this just kind of, do you think it'll remain a punchline forever?

JAGS (01:15:46.798)
I don't think it will remain a punchline forever because I don't think it's gonna keep going. Like that's precisely my point with all of these things, right? Like the minute it's no longer the pet theory or the pet project of like the big headline person, Bob Lord, Jack Cable, Jan Easterly, once you don't have like, yeah, you no longer have your...

Ryan Naraine (01:16:03.128)

Right.

They're all gone, yeah.

JAGS (01:16:09.618)
your platform that you're feeding, now you're actually out there like trying to get that next high paying job that comes out of like, okay, now I'm done here. There is no life underneath it. There is no regime. There is no process. is no like that's why they they never even built a process into it. Right? Like where when is Avanti's check in for what exactly? What what is acceptable progress?

Ryan Naraine (01:16:29.71)
Bye.

JAGS (01:16:37.664)
How, under what metrics would you ever judge them inadequate? Has there ever been any discussion of what it would take to remove a JCDC partner from JCDC? Like what makes you a responsible partner? Like it was just, no, let's sign as many people up as possible to make them all seem like we're all friends.

Ryan Naraine (01:16:56.6)
Yeah.

JAGS (01:17:03.358)
And like we can have a press release every week about what big company decided to post with us today. And then, okay, but there's no enforcement, no, no standard, no requirements, no, you know, no activities, nothing tactical as Kostin said. So, so with that being the case, like I almost expect like a giant reset switch to go off in three days, like literally just click new thing.

Ryan Naraine (01:17:28.28)
Yeah, from day one.

JAGS (01:17:32.362)
Completely new thing.

Ryan Naraine (01:17:32.61)
Do you think the CSRB survives? Cause I feel like there's some value there.

JAGS (01:17:38.646)
I don't know. I think the other question is if it survives, to do what? Does it keep doing what we've been watching it do now? To what extent is there a culture and an ethics at CISA that's gonna keep people doing things in the same heart of what they intended to do versus it just becoming a

that transparent vessel for whatever the fuck Sean Planky wants to do, right? Like now it's the Sean Planky show and you're like, okay, now what is Sean Planky? Does he want to be a rock star? Does he want to sing on stage? What's he into? Does he like cars? Like do we do now, this is all car. Yeah, like is it car themed now? Like what is Sean Planky? What are Sean Planky's hobbies?

Ryan Naraine (01:18:26.318)
How's his singing voice?

Ryan Naraine (01:18:33.602)
Just quickly to close the loop on CISA because I have it in my head here. What stops Sean Planky from setting up an organization that just does what cost in us? IOCs and Yara rules. Just those two small things. Just releasing IOCs and Yara rules for things that we know about. Assuming, you know, we hire some people who actually know how to write Yara rules there. Is there like a policy legal thing that stops it? Like what is the friction point to just doing that small thing?

JAGS (01:19:00.094)
I think we had a conversation at some point about like, who wants to work at SISA to begin with? Like we've had this conversation before, like who? No, I mean, I don't know. That's different discussion. But I'm saying like, if you want to track tactical talent, like I don't know what stops Sean Planky because I don't really know what stopped Jan Easterly other than it seemed that the priorities were elsewhere. There were people who were

Ryan Naraine (01:19:08.29)
But you can become a rock star by working there,

JAGS (01:19:29.808)
way more willing to entertain the notion of going to work at CISA than I think they ever should have. And like, advised them personally, I was like, dude, like, don't do this, this isn't good for your career, it's not good for you. And they tried anyways, despite what everybody was telling them, they kept trying to run into the fire and CISA wouldn't finish the process of hiring any of them. So you go.

It's you know, is it that you don't have the talent or that your priorities just keep changing every every three weeks and you just You're not actually staying any kind of course

Ryan Naraine (01:20:07.64)
Are you optimistic? Do you have any sort of optimism about Sean Planky and what happens next?

JAGS (01:20:12.735)
No optimism and no pessimism. I have literally no idea what to expect.

Ryan Naraine (01:20:17.902)
Got it. Speaking of fires, Fortinet is the latest. Fortinet is the latest ODA this week. Last week we spent all the time on Ivanti. We'll give them a break this week. Fortinet is confirming critical zero-day vulnerabilities. CVE 2024 55591 affecting FortiGate firewalls has been under active exploitation since at least last November allows a bypass authentication, gain control of affected system.

COSTIN (01:20:22.241)
you

JAGS (01:20:24.502)
Dude.

There you go.

Ryan Naraine (01:20:46.178)
There's a patch and mitigation measures. Costin, do we have IOCs? Do we know who this is? What's the news here?

COSTIN (01:20:53.857)
I admit that I looked only very very briefly into this and I think there was another blog that Fortinet posted about this rootkit that was deployed by the attackers and I did look into the rootkit, I wrote my own Yara rules but like in terms of the vulnerability itself it's a bit tricky to play with this unless you actually own it.

Ryan Naraine (01:21:07.679)
Linux rootkit right here.

COSTIN (01:21:23.657)
these devices and I admit you know me I don't own Yvanti I don't use any of this I don't want to call them snake oil no I don't I don't use any of these things what I have like right here next to me is this PF sense net gate device that's what I have but to be honest I I don't know that much about that so

Perhaps one has a better understanding of what's been happening with this TV.

JAGS (01:21:55.926)
No, no, not at all. I can't tell them apart, not even in the slightest. I have no idea. I have no idea what makes this different to like the one from two weeks ago, the one three weeks before that.

Ryan Naraine (01:21:59.98)
Ha

COSTIN (01:22:00.435)

It's like you lose track, every week there's a new one.

COSTIN (01:22:10.581)
I tell you what attracted my attention here was this vulnerability which has been under active exploitation since at least November active exploitation allows attackers to bypass authentication and potentially gain control of the affected systems like I am always like you know

I wouldn't say I go mad when I see that like potentially gain control. Like what are we talking about? Like, of course, of course there's like why who would like just get a bypass authentication and do what change settings or reconfigure the IP address now. This is like much worse, but like the language in some of these press releases designed to minimize like the damage.

Ryan Naraine (01:22:37.55)
potential, yeah.

JAGS (01:22:59.318)
Mm-hmm.

COSTIN (01:23:01.101)
to make it seem that it's not that serious like you know worst case they just bypass authentication like yeah like it's not that serious right potentially maybe gain control of your device potentially but yeah

Ryan Naraine (01:23:13.122)
Meanwhile, there's active exploiting.

JAGS (01:23:13.494)
Possibly massively actively exploded.

COSTIN (01:23:17.441)
Impact, full remote control of a victim's device. It's very T-level critical.

Ryan Naraine (01:23:19.769)
Is there?

Ryan Naraine (01:23:26.392)
day

JAGS (01:23:26.486)
Kelsin is completely right. I think that's what makes it, I think last episode you asked me if I thought that like, Kevanti was improving and I'm like, why would we assume that they are when at no point do we get somebody who stops and goes, okay, this is the reality of the situation. Like this is how bad it is. It is actually really bad. And that's because of all of this stuff that

You know, we acquired all these companies and we thought that they had a higher level product than they did. And now we're kind of stuck. And our project is in two years to have a newly rebuilt software stack that is going to make us like the industry leader and like stick with us in the meantime, right? Like if you had a sober assessment like that, you could be like, okay, well these dudes, I mean, they're going to take a walloping for being honest, but...

they're also gonna be the adults from this point. So like, you know, like, okay, invest into them because in six months, 18 months, whatever, they're gonna be the only ones that are gonna have a good solution. Everyone else is still gonna be shit, right? But that requires leadership. That requires an actual leader to stand up and say, hey, this is why things are bad. This is how bad it is. We know that it is this bad. And now like, this is how we address it.

Ryan Naraine (01:24:50.952)
When Kostin mentioned that he doesn't have a device to do any inspection, which is something we've discussed on this show in the past, is there room for innovation here for a corellium like sort of like, how do I, you you click and virtualize this and give people some inspectability or am I just like thinking crazy?

COSTIN (01:25:09.921)
I think there is but in the end like this is CentOS so I think the main issue would be about copyright and things like that because I mean Fortinet these are like expensive things a subscription to like a low-end kind of devices $4,000 per year and if you miss a year like then you need to pay back like all the all the months and all the years that you missed and you didn't pay for which is

kind of crazy in my opinion. It's all about the subscription model and I think that's what makes it maybe a bit more tricky on how to get your hands on. But I don't know if you can share this page by the way Ryan, the one that has the information. Because there's a section now that people on Twitter were absolutely mad about and I was laughing so hard when I saw it. Like if you scroll a bit further, like the IOX, yeah.

A bit further down. Yeah, there you go. Yes So let's read it. The following IP addresses were mostly found used by the attackers in the above logs 1 1 1 1 That's like cloudflare DNS 127 001 That's localhost Of course, of course, but why would you even include this? Yeah

Ryan Naraine (01:26:10.015)
this one, this, this, this one. Yeah.

JAGS (01:26:15.318)
JAGS (01:26:19.081)
No.

Noooo

Ryan Naraine (01:26:26.242)
That's home. But in fairness, read the next line, because I saw this thing here.

JAGS (01:26:28.552)
No.

JAGS (01:26:34.954)
Why the fuck would you put them in there? Like you're just asking for people to block like anybody who walks in here and is not paying attention or doesn't know any better.

Ryan Naraine (01:26:35.82)
You

COSTIN (01:26:43.777)
What does this even mean? Please note. Please note. But what do you use them for? Please note that the above IP parameters are not the actual source IP. They are generated arbitrarily by the attacker as a parameter. Why are we even like... What are we talking about? Is it like only the attacker can generate 8888, which is like the Google DNS servers as well as 8 8 4 4?

Ryan Naraine (01:26:46.056)
But it says, please, because please do not use this for any blocking.

JAGS (01:26:50.964)
Why the fuck are they on here?

JAGS (01:27:00.758)
This is the dumbest. This is the dumbest shit I've ever seen.

COSTIN (01:27:13.153)
It sounded like so, so crazy to see this thing.

JAGS (01:27:13.683)
I mean...

my god.

Ryan Naraine (01:27:20.558)
What do you make of the quality of all the IOCs in general? What would you make of Fortinet's response here? Forget the downplaying of the language that exists in every freaking advisory. You go to Apple's advisory, this may have been exploited in the wild and they market the zero data that's already been exploited.

COSTIN (01:27:21.568)

and

JAGS (01:27:38.006)
actively, massively maybe.

Ryan Naraine (01:27:39.98)
What do you make of these possible IOCs? Are we happy that they're at least giving us some things to go hunting?

COSTIN (01:27:46.242)
There are like if you scroll a bit further down there are four or five other IP addresses which are unique Well, not let's say that kind of IP addresses But again, I I was thinking and others were thinking like what happens if you actually and I tried that I took this page I put it into chat GPT and asked can you please extract all the IP?

address IOX from this post so that I can block them in my firewall and there you go 111127 like 222 and I ask

Ryan Naraine (01:28:19.054)
Chachi PT should know better.

JAGS (01:28:20.47)
This is how you know these people have never actually like proactively done any blocking or detection work. This is like the classic mistake that like every SOC 1 junior person at some point is gonna block 8888 and like there's gonna and suddenly like Gmail or whatever stops working and everyone loses their fucking minds.

And you go, lesson learned, right? But that's who is responding to global crisis, Oday actively exploited, that's fucking entire enterprises. You're like, this is not up to standard. This is not up to par. You're not operating at the level of what we expect.

Ryan Naraine (01:29:08.299)
Isn't it crazy?

COSTIN (01:29:08.321)
On the bright side, just as a bright side to this, which is that after extracting all these IPs, ChiaGPT did write a paragraph, you know, there was like music to my ears. said, like, please note that 1111 is a cloud for DNS server should not be used for blocking 8888 is a Google DNS server 127 00 is like localhost.

So while these IPs can be indicative of a Tractors activity, they should not be blocked at Firewall level. So I thought that was smart.

JAGS (01:29:41.302)

So they didn't even run their blog through ChatGPT.

COSTIN (01:29:47.19)
But like listen, nowadays everyone's going to use more and more AIs to extract IOGs from blocks because nobody has time. And I'm like looking forward to see like all the mess that's gonna be caused by AIs just blindly extracting IOGs from blocks, feeding them to database, getting them deployed everywhere. The next CrowdStrike style crash of the internet for sure it will have something to do with blocking.

IOX blindly extracted by AIs in July 2025.

Ryan Naraine (01:30:19.982)
Costin, you heard of gravy analytics?

COSTIN (01:30:23.585)
Actually I did, yeah I do, I do know them.

Ryan Naraine (01:30:26.882)
We have news on hackers claiming to have breached Gravy Analytics, this US location data broker selling to government agencies. And three samples have been shared on a Russian forum, millions of location points across the US, Russia, and Europe. What's the context here for this?

COSTIN (01:30:48.385)
I thought this was an interesting story. I don't think we had time to cover it last week. So what happened here is that an intelligence broker posted about this on the XSS forum, which is one of the famous Russian speaking cybercrime forums, which is still operating somehow.

And they posted three archives, three zip archives with different amounts of data in there. But again, we're talking about tens of millions of location data extracted from mobile phone, smartphone applications that secretly, you want silently or like in the background, collect your location. So I'm sure everyone has seen things like a flashlight application.

snow prediction or rain prediction application all this junk stuff right some of them are maybe if you want quite useful like back in the days people didn't have flashlights on their phones so you just need an app that makes the screen white and all of them they were like riddled with libraries that would collect locations send it sometimes four or five

Ryan Naraine (01:31:46.23)
All this junk stuff, yeah.

COSTIN (01:32:09.345)
of these different libraries would be embedded into one application. And I did the research about this back in 2019. I think I presented it during one of the opcode editions by Matt Swish. And I

remember, actually I dug quite deep into that. I have a GitHub repository with telemetry endpoints used by these different

location collection libraries. But I think that people didn't really care much and I was thinking like, man, this is a huge issue. This is big, man. This is big. The fact that we're talking about billions of location points being collected silently from people, this is going to explode at some point. This is going to backfire. And it's interesting to see, you know, six years, four or five years later.

This is again back in the news and the potential for abuse is so high. So if you have time, go watch that talk from 2019. And if you have a pie hole set up at home, you can use my repository to block some of these endpoints. Sadly, you can't block all of them because constantly they just rotate them. They replace them with new ones like the telemetry endpoint changes. There's a new domain and so on and so on.

There's literally thousands of these libraries. One thing I'm going to say here is that based on my experience, the amount of this shit is much lower on the iPhone, like in the Apple ecosystem than on Android. On Android is like the Wild West. On iPhone, because of Apple's restrictions, the number of apps that collect your location this way is much, much smaller.

So I think that this mostly comes from people using Android devices. That's a reality.

Ryan Naraine (01:34:11.406)
Yeah, but there's a lot of people actively sharing their information and recording their location and sharing it. There's been some amazing research recently around Strava and Strava being used to pinpoint where Secret Service agents are running around the White House and so on. These guys are literally recording their location, uploading it to the internet and leaving it out in the clear. So I feel like there's a lot of human element here as well, in addition to these data brokers that just collect...

COSTIN (01:34:28.097)
Yeah.

Ryan Naraine (01:34:39.872)
all this location. Juan, you got a thought?

JAGS (01:34:42.886)
I mean, I think it's interesting in its tiers, right? There's the folks who are just obviously posting a ton of info, whether without thinking about it too much, because it's some niche thing, right? And we've seen it in every country or like some relatively famous person or some really critical function that's like outed by virtue of like tracking for the trails that you like to do by cycling in or whatever. Then there's like the folks

that get dragged in with sort of this ad tech stuff. What's interesting is I think to Kostan's point about like it being so much heavier on Android, it tends to also disproportionately victimize a

certain kind of user, like the kind of person who goes and installs like a random app for this and that and like installs a random app for a feature their phone already has without even realizing it, installs like has a child that like goes and plays some freemium game.

And then they never remove it from the phone and that kind of stuff. And I think that's where you get the reality of ad tech, is actually, it's sexy and not sexy at the same time. Like the promise of ad tech is very sexy and there have been periods when I think it was more valuable than it actually is now because it had much better infiltration of things that were much more.

widespread. But that's not the case anymore, not as much. You have a lot of blocking, you have a lot of things that have been outed, you have a lot of SDKs that no longer work the way they used to, a lot of different measures like what we discussed with like Apple blocking a certain, arbitrarily deciding to just block a certain amount of some of this ad tech stuff. So then what I'm thinking mostly is like, you're still selling the same data, but the

Quality of that data the spread of that data. I don't know is really up to par and that's where you get reminded that this is just the third party bastardized version of what the big boys actually play with at Meta and Google where like you're talking about unbelievable profiles worth of information and understanding at a granular level of what like

JAGS (01:37:08.714)
massive populations do. And that you don't see unless you are inside of one of these places or, you know, Cambridge Analytica your way to like harvesting a bunch of stuff you shouldn't be able to harvest. But it's just to say that this is all happening in gradations. And the quality of what you can do with it is mostly like, okay, well, how widespread, how much data can we get somewhere outside of here or adjacent to that?

And when you see it sold in its purest fashion, I think is when it's clear that it's value is not quite as high as what they pretend that it is.

Ryan Naraine (01:37:47.32)
But these data brokers and these collections, I think this the the extent of how much of this data is collected and being resold here, there and everywhere. Like, why are we worried about TikTok? Like, why are we worried about TikTok and the Chinese spying on our stuff? By the way, the story just broke that the Supreme Court here in the US has upheld the TikTok ban. Costing TikTok has been a big issue for you in Europe and your Romanian elections. And we've been through this in the past. Does this?

Does this story resonate there? Are you guys following the US TikTok drama?

COSTIN (01:38:22.773)
I don't think the people here are like immediately following it, but I mean the echoes will be felt everywhere. I mean, if TikTok is banned in the US, it will be banned next in Europe. We've seen that before with with other examples. And I think that the latest is that during the elections,

upcoming presidential elections here in Romania in March. Well, first of all, they announced some huge fines for companies that support

election interference up to 5 % of the company's income. Like I guess for TikTok 5 % would be huge. So they can get find some crazy amounts and still I think the option is on the table that TikTok may be blocked during the three weeks window of the elections that we're gonna have in March.

Ryan Naraine (01:38:59.277)
Really?

Ryan Naraine (01:39:18.336)
One, do you view this as having an economic impact here in the US? Let's just assume that a ban move forward. I saw some numbers that Americans generate about $10 billion in revenue from TikTok. Do you think this is going to be banned? If I you to guess, do you think it'll be sold or banned?

JAGS (01:39:37.43)
I mean, I imagine it will be sold like there's an interest of course in trying to like recover some value from it at the same time. Its value and value proposition could plummet overnight, right? If it genuinely does have an issue with users or people, you know, just scatter onto another platform like red notice or whatever it's like.

Out of nowhere, you get another shittier, even shadier, like thing you've never even heard of before, who like is the alternative, right? Which is hilarious. And I think it speaks to some of my concerns about previous US government actions where I'm like, you guys are just telling us what's bad. You never tell us what you recommend or what's good or actually consider what the alternative is. So what you do is,

Ryan Naraine (01:40:12.942)
That's no top of the charts.

JAGS (01:40:34.922)
You take a homeostatic ecosystem that you have a problem with and you fragment it and you weaken it, but you don't drive people anywhere in particular. you only have one, like you only have so many of those bullets in the chamber.

So what are we going to do? Like now we're going to bitch about TikTok all day long. And then everybody went to red notice and you're like, wait, no, we didn't consider that everybody would just go to this other even worse Chinese app. You're like, well, what did you consider? Right? Like, what are you trying to say? I think I'm glad we're going at this discussion right on the back of the ad tech thing, because I find it kind of fascinating that it's kind of an implicit admission of just how horrifying and

and insane the ad economy is at what Facebook, Meta, Google, et cetera, can see about what we do. That the idea that

a foreign alternative could become popular. And it just does what local companies do. And we're like, this is the most evil shit on earth. You're like, hold up. How is this different than Instagram, other than it's it's owned by a Chinese person instead? You know what I mean? Like, and that's where

Even you, get even me with the tinfoil, hattiness and everything because I know just how bad things actually are at these companies and how little we understand them. And the only solace we get is some like Boy Scout bullshit about like, yeah, but they're like, they're at least incorporated in the U.S. You're like, so what?

Ryan Naraine (01:42:25.802)
same thing with TP link. mean, Zuckerberg has kissed the ring now, so Facebook is fine. You know how we all forget that Satya and Nadella Trump almost forced Microsoft to buy TikTok back in the day? Like that was just kind of like skating over everyone's head. It's crazy. I want to

JAGS (01:42:32.31)
Facebook is getting crazy, dude.

JAGS (01:42:45.91)
because Microsoft's going to buy Greenland now, I think.

Ryan Naraine (01:42:49.518)
I want to shift away from China to Russia quickly and touch on the Star Blizzard story out of Microsoft. Microsoft had a blog post, a small blog post on Star Blizzard spear phishing some of their specific targets, but very interestingly using like broken QR codes to send people, to trick people into responding to email and then sending them to WhatsApp group and in these WhatsApp group they were doing the exploiting and the...

data collection. Two things cost in. Who is Star Blizzard? are you tracking this?

COSTIN (01:43:23.143)
It's a fancy name for turla, which is what everybody calls it.

Ryan Naraine (01:43:27.896)
Calisto. I thought I saw Star Blizzard was described as...

JAGS (01:43:30.13)
No. No.

COSTIN (01:43:35.11)
sorry, did I mix it with a cadet blizzard? I apologize.

Ryan Naraine (01:43:38.83)
He's messing with you.

JAGS (01:43:38.902)
No, that... No, could that blizzard was the...

What? Guys, come on. Come on. This is a serious podcast. There's like 50 people listening to this. Okay, we can't

Ryan Naraine (01:43:45.332)
In all seriousness, is this just a natural kind of evolution of trying different kind of tactics to hit these folks? Or are you impressed with this QR code WhatsApp group kind of targeting?

COSTIN (01:44:10.471)
I mean, this is happening a lot in cyber criminal circles if you want this hijacking of WhatsApp accounts. Maybe not necessarily hijacking, but what you're setting up is just a clone of your conversation so someone can spy on everything you are writing and receiving. there was like, it's interesting, there was like a

a very interesting warning from the Romanian CISA just the other week about a similar campaign from obviously like another Russian speaking cyber criminal groups or not APT like Kalisto that was using kind of a similar mechanism to hijack people's WhatsApp accounts. So in a way it's like a man's espionage campaign just setting up

a clone of your WhatsApp conversations but on the other hand is super super effective and it doesn't require exploits, doesn't require any malware, it works on iPhones without you spending 10 million dollars on the zero click chain so in the end it's effective and I think many people are just not aware of how this can be abused and how easy it works. What I was thinking like at

How capable is actually Facebook meta in spotting people that have been compromised this way? So do they have the capability to spot whenever this cloning happens and can they block those connections? think that would be interesting to know. In particular, like this attack was happening through two domains.

That wouldn't let's say be necessarily easy to spot from their point of view, but the attackers cloned instance running on certain IP address if it's not through VPNs. Maybe it's actually possible for meta or WhatsApp if you want to spot the attackers and blog them. So I think that would be interesting.

Ryan Naraine (01:46:21.59)
WhatsApp was able to spot the NSO group according to the lawsuit, right? So they have this ability and does does Meta have a threat intel team that does this full-time one?

JAGS (01:46:32.566)
Of they've had a threat intel capability and a lot of it maybe more focused on this info stuff for some time. At the same time, meta is changing apparently drastically. So I don't know what they're going to have in the near future.

Ryan Naraine (01:46:44.344)
Yeah, it's- it's going to going, yeah.

Ryan Naraine (01:46:52.462)
Sticking quickly in Russia, we've got more news on Ukrainians pro-Ukrainian group smashing Russian networks. This time, the largest platform for state procurement. Russia's main electronic trading platform for government and corporate procurement confirmed this week it had been targeted by a cyber attack. The Ukrainian activists claimed responsibility.

This is part of the course in warfare. I assume we've discussed this in the past, but is there any surprise at all that they've been so active and so successful?

COSTIN (01:47:30.389)
Well, in a way, mean, this is happening every week. What's new in this story is this particular group that claimed responsibility, which is kind of new. I don't think they've been seen before Yellow Drift. And what you see, I was wondering if this is imagined that in the US, they just opened the gates like it's open season.

Like everyone can do whatever they want against Russian hackers, against Chinese hackers. Is this like what is going to happen? Like, no, no, no, but this, this is let's say the outcome of just opening the gates. Cause like in Ukraine, yeah, like in Ukraine, when the war started, they formed out this cyber army of Ukraine telegram group with almost

Ryan Naraine (01:48:05.464)
Recursor to what? Yeah.

Ryan Naraine (01:48:13.314)
This is the free for all that one into wants.

COSTIN (01:48:24.533)
half a million people in there and just like it's open season on Russia like you guys can do whatever you want nobody will be prosecuted nobody will be stopped just do whatever you want so I mean if you open like again if you open the gates I mean this is what you get

JAGS (01:48:36.746)
Sounds pretty cool.

What's the what are we what are we worried is what are we worried is gonna happen? What are we saying is going to happen?

COSTIN (01:48:47.409)
No, what I'm saying is that some companies will get wiped, but I mean they'll restore from backups and move on. So how effective is that? That's my question.

JAGS (01:48:55.03)
they were gonna get what I think that's preside, like I think it's the difference. I'm gonna use something I know nothing about. But like, I think it's a difference between having a first child and a second child like this. There's this, you you always read about like first time parents were like terrified and like the whole time you're just like worried that every tiny thing that could go wrong will go wrong and will be the end of the universe.

And then the second child comes around and you're like, fucking does not, you like you've been through this, you're inured to like all of these like anxieties. Like I feel like that's where we're at the first child stage of cyber. And like we talk about everything as if like, you know, one person sneezing on a computer is gonna set off like a global catastrophe that we can't possibly come back from. And like I do.

It's not that I want the free for all. I think we already live in a free for all. It's just a one-sided free for all. And all it's keeping us from having is an actual perception of our own resilience, of what actually makes us a significant difference in defense, as opposed to the things we think make a difference in defense. And like, we're just, keeping ourselves from having an appropriate immune response.

by doing this homeschooling bullshit.

Ryan Naraine (01:50:18.926)
Yeah, and on the same free for all front, we got news out to the UK that the UK government is putting forward a proposal to ban public government bodies from making ransomware payments. There is a free for all in the ransomware world where there's a wealth transfer happening from the West to these places. Do you think this ban is practical and workable if a hospital gets popped or something very, very important gets popped and you have to pay the ransom to survive?

JAGS (01:50:47.872)
I think it's actually really interesting because when it comes from the NCSC, as is usually the case, it's more thought out. it's not like a, it's not just a, know, what we saw in the States where people were just like, we're gonna ban ransomware payments. So we're like, you mean you're gonna keep anybody from being able to pay, like what authority do you have to do that? You actually do not have the authority to do that. So no, you're not.

You can say that you'd like to, but you can't. In the case of the UK, what they're saying is, well, this part that's well within our control, we'd like to suggest is not going to pay any more ransomware payments. And in a way, it's an interesting, it's an interesting sort of field exercise

because if anything, saying it is signaling your intent. That means someone has to come test that boundary.

And then you have to stick it out and not do it. like signaling that intent is only the beginning. You're saying somebody has to come, someone has to screw us over, and then we still have to do the difficult thing of not paying. then you may reap the rewards of there being an established precedent that says, the UK doesn't negotiate with ransomware terrorists. We don't give a shit. We're just gonna figure it out.

And that's it. And then you can have a slightly different sort of response.

Ryan Naraine (01:52:21.454)
Dustin, you're our European correspondent. How do you view it?

COSTIN (01:52:22.539)
think, I mean...

We've discussed this idea before of just banning ransomware payments and then like having some kind of a provision that in some super special critical cases you can apply for an exception and like you know if people are dying, hospital is inoperational then you can still make the payment. So I mean it's been discussed before what I was saying here that if they're like at this point

It means that they are confident that Everyone will be fine with not paying that is everyone has backups everyone has a Recovery plan in place and they don't have to pay they'll just be able to restore operations in a kind of a decent number of days Moreover, I think they're also confident that the amount of ransomware attacks is now

maybe low enough so that it's no longer like completely out of control. This is now let's say kind of controlled phenomena. So it's absolutely fine if you tolerate a few companies going down for a couple of days before they just restore from backups. That's what I think.

JAGS (01:53:44.758)
Well, that's what I think is interesting, right? If you look at what they're pushing, it's not just we won't pay, but also, and here's like disclosure requirements so that expressly, so that law enforcement can have an intelligence as to how much of this is happening and what type of it it is and what it is. They want to understand the problem, right? Which I think is really, really interesting.

COSTIN (01:53:58.006)
Mm-hmm.

JAGS (01:54:13.684)

Like the discussions of disclosure requirements previously in the US and in other countries, they tend to focus on like, okay, like how do we tighten the screws in some regulatory capacity so that companies will tell us as soon as possible? And I think that it might seem like this is the same thing, but I think it's actually really interesting that it really isn't. It's saying, hey,

You need to, everybody needs to tell us just so that we know what is actually happening in the UK. And that's very different than what's happening in the US where there isn't even, there's no clear sign of who would handle half of it. If you call the FBI, but it's not an eye watering number, they don't even record it. Like who actually does it, does it matter if it's like a small, like most, most cops will just tell you that like if it's a small thing, like don't.

don't even call us, right? So there isn't a prioritization of understanding the scope and the trends in the problem. I think it's real, again, NCSC is always like really interesting coming in with an interesting understanding of the problem and being willing to put their stake in the ground in some form of leadership that it's an experiment. I don't know, right? Like if maybe NCSC says we're not gonna do this and then like,

there's a bad enough ransomware incident in an important enough part of the government and they backtrack. I mean, that would be, it would be catastrophic in setting that precedent, but it would also probably let us know that if even one of the most cyber capable regulatory regimes in the Western world is unable to stand by that line, then we should probably retire that fucking idea.

Ryan Naraine (01:55:48.76)
it.

JAGS (01:56:09.269)
Just stop talking about

Ryan Naraine (01:56:12.172)
I might just add for cloud just for purpose of clarification that it's just a proposal and it's a it would apply to government agency. It would apply to schools, hospitals, local councils, critical infrastructure operators, places that they have control of. It wouldn't apply to like British companies, for instance, let's say British telecom and so on. So it'll be interesting to see how that plays out and how it applies to here. Ransomware is still a big problem. mean, Costin, you you intimated that you feel like it's starting to play off, but I

Just listening to CISOs here and the top priority people for defenders here, ransomware is still the number one thing they're going to ask for budget for.

COSTIN (01:56:48.619)
Yeah, clearly not playing off. Actually, I was looking at a report that the UK and CSC reported a 16 % increase of mostly ransomware attacks in 2024 compared to 2023. So it's not going down.

What I was thinking is that they are, let's say confident that they have like a good grasp on the phenomenon and like enough control that

makes it feasible for them now to ban these payments. And like from a pure magic money people point of view, I think this is good. mean, if we can reduce the abuse of magic money and their usage by cyber criminals, that's only good.

Ryan Naraine (01:57:34.598)
I want to close the episode very quickly with a quick mention that I'm currently reading this new book. It's called Infected by Bernardo Quintero, one of the founders of VirusTotal from a side project to Google and the journey behind VirusTotal. It is the English translation is coming very soon, but more importantly, look, Mr. Costi and I see you're in there. So one of the buddies is well representative. Really, really good book, very.

COSTIN (01:57:38.614)
Wow! Beautiful!

JAGS (01:57:57.654)
fancy

Ryan Naraine (01:58:03.662)
honest, transparent look at entrepreneurship, the emergence of VirusTotal from a newsletter to a pen test company, the idea for VirusTotal and kind of all the intricacies about going through how companies responded to their engine being in there. It tells a story of Trend Micro insisting that their engine not be in there and then they came begging and they put them at the back of the line.

Another little tidbit here before CrowdStrike was even a story, Dimitri Alperovic and George Kurtz flew to Malaga to try to buy VirusTotal. Google got wind of it and ended up buying VirusTotal. So there's some really, really, really good stories, good pictures. See again, on amazon.com it's available in Spanish only. So maybe only Juanito can go buy it and read it.

COSTIN (01:58:41.963)
How do we bite? How do we bite, Ryan? How do we bite?

JAGS (01:58:51.732)
just ordered the Spanish version.

Ryan Naraine (01:58:54.016)
It's called Infectado. Look for Infectado, Bernardo Quintero. And Bernardo tells me that the English language version should be out in a week or two. for the folks interested in this, it's really, really good for first time entrepreneurs, for anyone interested in the business and anyone in the threat intel world to kind of get a feel for like the start of this thing all the way through.

Interestingly, nothing much post Google is included in here. So that's something to pay attention to.

JAGS (01:59:22.934)
interesting.

Ryan Naraine (01:59:23.02)
With that, some quick shoutouts. Last few seconds, Juanito.

JAGS (01:59:29.15)
I mean, enjoy not living in DC or in America for the next like week. It's just like, I think we're a lot of folks have been look, it's not about whether you you support or don't support, you know, right, left wing, whatever, but like, whatever you think is about to happen, that that grace period of like burying our heads in the sand before the chaos really kicks off.

is ending as of this weekend.

Ryan Naraine (02:00:00.332)
I feel it's less chaotic than 2016, 2017 though. I feel like there's a lot more adults in the room.

JAGS (02:00:04.052)
Is that better or worse? Is that better or worse? Like, I don't know. And that's my point. Like, we don't know. We haven't known. Most of my answers, whenever you ask me about what's coming, are I don't know. And we're about to enter the find out era, right? Like, let's see.

Ryan Naraine (02:00:07.822)
I don't know.

Ryan Naraine (02:00:23.832)
We fucked around and now it's time to find out. Cost him some closing thoughts.

JAGS (02:00:25.746)
Yep

COSTIN (02:00:28.641)
I was just listening to you guys talking about the imminent I assume that you're talking about the imminent UFO disclosure this weekend, right? Like I'm like I said, I'm with Jeng I'm all about UFO disclosure. So looking forward to the to the video that's gonna drop this weekend about the retrieval of the UFO if you know what I'm talking about if not like that

Ryan Naraine (02:00:36.75)
Exactly.

JAGS (02:00:36.854)

Of course.

COSTIN (02:00:55.135)
Shout out to our friends in Belgium at CCB, Kevin, Pedro, Nils, everybody there. They're amazing folks doing amazing work. So hope to see you guys soon and keep up the good work there.

JAGS (02:01:01.002)
Pedro.

Ryan Naraine (02:01:12.526)
Shout out to Sequoia as well. With that.

COSTIN (02:01:14.473)
So we did that mid show, but cheers.

Ryan Naraine (02:01:17.358)
Bye Bye

JAGS (02:01:19.286)
Thanks, everyone.