Episode 29: Three Buddy Problem

Hijacking .gov backdoors, Ivanti 0days and a Samsung 0-click vuln

LISTEN:

Cast:

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

Ryan Naraine (00:08.462)
Good morning everyone, it is Friday January 10th. This is episode 29 of the Three Body Problem. I have with me my friends Juanito and Costin Rayo. I'm checking in from Bucharest and Washington DC. How are you gentlemen?

JAGS (00:23.036)
Man, good. Just getting more into this limbo scenario we seem to live in where we keep repeating the same horrible situations over and over again and nothing quite seems to improve. So good times, exciting, positive times.

Ryan Naraine (00:25.685)
Yeah, I...

Ryan Naraine (00:39.343)
Good times. And on that note, let's start right there. We have very fresh news of an Ivanti ODE already exploited in a while against this Ivanti Connect secure product. What is this product cost and is it a VPN?

COSTIN (00:55.918)
It is a VPN and I guess we were joking like is this like a new zero day like a new new zero zero zero zero day because like we've been here how many times how many times we've been here like yay another one

Ryan Naraine (01:16.76)
Yeah, it feels very much like we're repeating the same things on the podcast over and over. We discussed this in the pre-call here. It's like the podcast is starting to become kind of repetitive. The news here is that they patched two vulnerabilities, CVE 2025, 02A2 and 02A3. And only one is being exploited. According to their information, only one is being exploited. We have news. We have news.

COSTIN (01:40.046)
was funny, if I may inject a comment here that Florian described it in a very funny manner on X. said, if you do an IR with the company, the first thing, it never hurts to ask, do you guys have Vivanti? And they say, yeah, why? Well, just in case, just in case. And later you can send them links to these blogs. And I told you, you see, I knew it from start. I knew it from the beginning.

JAGS (02:06.94)
Luke.

It's a good bet. It's a good, you could just.

COSTIN (02:11.03)
It's a good bet. And there's like no, there's like absolutely no downside to it, right? Cause eventually there'll be a new zero day. You know it, it'll be a new one.

Ryan Naraine (02:22.033)
We've got some reporting from Mandiant. Mandiant published this report that you're seeing on the screen here for the folks watching this. You're seeing it on screen. Mandiant was pulled in to do the analysis of this. And one of the things that stood out from the Mandiant blog post is they say, Ivanti and its affected customers identified the compromise based on indications from the company supplied ICT, which is this integrity checker tool, along with other commercial security monitoring tools.

That stood out to me because Juanito, when we discuss Ivanti and a lot of these network device things, you've repeatedly said there is no inspectability, there are no tools to do this. Do we have any guesses about what these other commercial security monitoring tools are and how they were able to detect this?

JAGS (03:04.73)
I have no idea. I actually want to ask these folks basically what they're referring to with the other commercial stuff. Which it could be as simple as, you know, if you already are able to get, let's say a dump of the memory or something like that, you're using other commercial tools to analyze that. Or is there some quiet, like new offering that allows you to inspect these things? I'm not sure.

What I will say is like on the ICT side of it the integrity checker thing. I feel like there's some like Bullshit afoot in this right because it's not to say that You know, it's great that they have provided some kind of integrity checker like that's part of what we hope for with something like You know saying that we we want inspectability and blah blah blah I don't know the terms under which you get this integrity checker out and all the terms under what you can use it but what I will say is if you look really carefully at the

if anti advisory itself, they talk about, they basically say like, it only works as of this particular version. And the best thing you can do is just like update the firmware and like wipe the device, like wipe the device and like update the firmware and start from scratch. And then you can run the ICT thing and you're like, but that's a way to like, you're basically disinfecting the device, right? Like that it's a way to kind of

from what the way I read it, they're basically like, if you want to make sure you're good, wipe away all indicators of like compromise from your device and then run this checker tool. And like, I'm not saying that that's like the way they necessarily are angling it. It's probably more about how the tool works and what you need in the firmware, but there is definitely some like fuckery of foot here where you go.

You clearly are not prioritizing knowing whether you have been hacked already because you're basically just saying, if you want things to work well, just blast everything away and start over and then you're good, which is it's kind of insidious in a way that's like particularly disconcerting to me.

Ryan Naraine (05:23.507)
I'll get to the ICT in a little bit because there's another bit of it that is...

That doesn't make sense to me, but Kostin, I just want to go back to you on this commercial security monitoring tools that they mentioned. Any guesses at all as to what they're referring to? this a, when you say commercial security monitoring tool, it suggests to me that there's something that you can buy that in addition to this ICT, you can put some layers of things there to do some checking and to do some spotting of threat actor activity. What do you think is happening? Is this your Proxmon thingy?

COSTIN (05:42.936)
Mm.

COSTIN (05:55.278)
I was saying that what they're referring here is redirecting things like syslog to a SOC or to another cloud monitoring based system which can analyze the syslog and potentially warn about, let's say, suspicious behavior. So, I mean, when it comes to appliances, I think this is one of the most powerful and to be honest, one of the few

things that you can do, right? You can try to redirect the syslog from that appliance somewhere else and hope to spot some unusual signs of malicious activity in the syslog. I mean, this is what

I am doing myself for pretty much all my network devices. Everything I have around like routers, switches, I just redirect everything, all the syslogs to a central server.

And I try to perform analysis there. use, like just to name a practical solution, use Wazoo, which is a nice option. But I have also Wazoo, Wazoo, W-A-Z-U-H, Wazoo. It's, some people may call it like, it's CM, but to be honest,

JAGS (07:02.086)
What is it?

JAGS (07:09.914)
Never heard of this thing. Yeah.

Ryan Naraine (07:10.102)
What is this?

JAGS (07:17.978)
Open Source XDR?

COSTIN (07:19.946)
is more than CM. It's definitely more like it has an IDS, it has other things inside. So it's pretty powerful. You can redirect the SysLock and then to a machine and then the Wasu agent running on that machine will look at the SysLock events. And I've seen Wasu finding interesting things like crashes, reboots, application crashes, obviously suspicious things.

So that's one of the things that I'm thinking about that you can do with this network appliances. The other one would be SNMP based monitoring. So leveraging SNMP to look at, I don't know if there's new users being created or things like that, anomalous activity. Unfortunately, nobody can guarantee you that any of these tools will spot the malicious activity. You can only hope.

You can never say for sure that yeah, if we do the Wasuk Syslog SNMP thingies, we'll catch the hackers leveraging their zero days against our network appliance. There's no guarantee for that. So you can only cope. Absolutely.

Ryan Naraine (08:30.165)
But you should be doing this, right? You should be adding multiple layers of things now that you know that this, it's very, inspectability is difficult. You should be setting up multiple layers of.

COSTIN (08:39.743)
Yeah, I would do multiple things. I would never leave the Ivanti devices exposed on the internet by themselves. I would always put them behind another firewall and kind of try to limit the amount of ports which are exposed on the internet and then I would log the hell out of them. And the logs I would keep them outside of those devices. I would try to save them in a separate network, so-called out of band.

network logs, is again what I'm doing for myself, totally separate the networks for logging traffic packets, net flow and so on. And whenever something happens, even if your Ivanti device is compromised, the hackers wiped all the traces and everything, you may still have the Syslogs and you may still have the network logs, which could allow you to potentially figure out when it started, how it started. And yeah.

Things like that.

Ryan Naraine (09:37.497)
Is that a trivial task to parse those logs and figure out what happened post-incident? Are there tools for that?

COSTIN (09:42.062)
I know what you're asking. Because people buy these things, it's like you buy and forget. So you buy the... And this is a magic, this is a selling point of all these things that you don't have to worry too much. I mean, I have money, I want to spend money and to sleep well at night. So they spend money, they buy these things and sign the pledge and then they don't sleep well at night, guess. Or they sleep until they don't.

Ryan Naraine (09:49.44)
Yeah, you buy it and you dump your logs everywhere and then what do do with it?

Ryan Naraine (10:11.438)
Speaking of signing the pledge, might add that the Vanti was the very first to sign the pledge. In fact, it might've been, it worked. I want to come back to this, I want to come back to this ICT, this integrity checker tool. I'm reading from the Mandiant report here. It says recent versions of Vanti Connect Secure have a built-in integrity checker tool that periodically scans the file system to detect new or modified system files that may be indicative of six-stem compromise. Perfect.

COSTIN (10:18.05)
That seems to work. It's very efficient.

JAGS (10:21.745)
Much pledge.

Ryan Naraine (10:40.896)
It uses this manifest during the scanning process. But one, the first thing that pops out is that the attacker immediately circumvents it. In an attempt to circumvent it, the threat actor recalculates the SHA-256 hash of the modified, this upgrade file and inserts it into the manifest. So like, feels like, hey, use this integrity check.

JAGS (10:56.594)

Listen to how fucking stupid the design of this thing is. It's just like a hash checker. Like it's not like they the files are like signed. It's not like you're you know, you're checking like some kind of like digital signature that means it came from Avanti or whatever. They just made a fucking list of hashes for what the default thing is supposed to be and clearly they're not even protecting that list because the attacker can just add the hash into the list and then the ICT goes like, yeah, it's good.

How fucking dumb is this?

COSTIN (11:27.63)
This is if I may comment, this is I 1990s level security. This is how we were doing things in the 90s. And the other thing which attracted my attention, which because it's a it's another 90s kind of vibe. So we were talking about two CVs here, right? 2025, 282 and 283. And they say a stack based buffer overflow. And the other one is a stack based buffer overflow too.

Ryan Naraine (11:27.663)
Yeah, bo.

JAGS (11:32.589)
Right.

Ryan Naraine (11:52.987)
Waffle or waffle? Yeah.

COSTIN (11:57.806)
And like, come on, we're 20, what 2025 January and we're still talking about stack buffer overflows in this network appliance. I mean, this is again, nineties vibes.

JAGS (12:07.74)
So there's no ASLR, there's clearly no stack guarding, none of the things that have been developed as what are considered base level exploit mitigations are enabled on any of these fucking devices. I think that's ultimately, that's why the CEO hostage video for Avanti works so well, the ROI on the development of that video.

It's just excellent because it's been nine months and you can just keep reposting the same fucking video over and over again and it's going to keep paying off with their heartfelt apologies. But like the obvious thing here is there are no proactive technological attempts to like button shit down. It's just continuing to plug the holes on the hull of the ship with like with your fingers and they're just going to keep doing it indefinitely.

Ryan Naraine (12:58.877)
And we've consistently been picking on Ivanti, but it's the same across the board. If you go to the CIS, non-exploited vulnerabilities list, and you start looking for these network devices and these VPNs and so on, it's like across the board, all these vendors are dealing with the same

memory safety issues, the same old stuff. I want to pivot quickly to the Mandiant blog on this Ivanti thing, because we got some IOCs, we got some Yara rules thankfully for Mandiant. We don't get it from Ivanti, but we get it from Mandiant.

And we have some attribution costing. can you tell us about the attribution? Is it reliable attribution quality of the IOCs? You have a rules. I'm sure you went over it. What do think?

COSTIN (13:36.403)
how you put me in the spotlight knowing that I'm a fan of mendient attribution, right?

Ryan Naraine (13:40.283)
Yeah, according to you, according to you, Mandiant attribution is the best.

COSTIN (13:44.846)
It is, it is. Maybe not here. I mean, we are seeing here that Mendyan says there's two Chinese groups that are somehow connected to this. That's one UNC of 53, 337. And there's another one 5221. And the funny thing here is that I don't think I've seen this before, at least not publicly mentioned.

that the fact that UNC 5337 is a cluster of activity says with moderate confidence to be part of UNC 5221. like that's a yeah, yeah, it's like an unk within an unk, which is interesting, right? So to me that immediately attracted my attention. I think they do talk a bit in the attribution section.

Ryan Naraine (14:26.621)
So it's an unk within an unk.

COSTIN (14:42.518)
more on this from the point of view of UNC 5221. Sorry about its tongue breakers, the big numbers, right? And I think that there was another interesting report which covers some of this activity. Remember when we discussed this little lamb, Wulty or Wultea a couple of episodes ago? That's pretty much

this stuff like it is somehow those guys kind of got heads up that this was coming or somehow they had a hunch and actually that that research and that release about the little lamb ulti it it kind of overlaps with this cluster of malware that they are talking about here so i looked a bit at the yara rules i i ran them on on my systems they're all solid of course kind of things that you'd expect from

from Mandiant. Unfortunately, there's not many samples. I think some of them are still missing. We don't have them. But nevertheless, it's good. mean, we have IOCs, have YARA rules, we have information. And this is like things that people can use to dig deeper, learn more, find out if they've been compromised, things like that. Again, according to Mandiant, this is Chinese activity. And again,

Ryan Naraine (16:03.967)
It's China,

Ryan Naraine (16:10.463)
and they got their true disconnection to the spawn ecosystem of malware, spawn ants, spawn mole, spawn snail, SSH backdoor that we've previously seen used by Chinese. So the attribution you feel is a little solid here.

COSTIN (16:14.99)
Correct. Yeah. Multiple tools. There's multiple tools.

I see what's interesting here that I really wanted to mention this that this cluster they're not targeting Ivanti only, right? So they're like for instance in the past they were targeting Cisco if I remember correctly. And to me this is, it's interesting because sometimes these groups are like really specialized when you have a group targeting.

trying to find zero days, remember like in the SOFO appliances or they were working on a specific platform then they kind of become experts in that and they focus on that. So it's good to see probably what they mean here like these are the Ivanti specialties within the larger umbrella of that Chinese threat actor. what I see like my conclusion from this whole story is that Chinese actors

They finally understood what probably everyone else understood decades ago that network devices are the best because there's no security, 90s level, know, no stack protection kind of measures. It's the heaven. It's amazing. The moment you have zero days for that and you get the foothold within your network through these VPN appliances or

rights management or control, then you can do whatever you want and people will just scratch your head, scratch their heads and not understand where it comes from. how did we get hacked? Where did it start? Like where are they? Are they still in the network? Did we kick them out of the matter? Right. We can't save with a hundred percent full confidence that we remove them from our networks because they may still be in some appliance somewhere that we don't monitor because we don't know how to monitor.

Ryan Naraine (18:17.795)
With all these typhoons and stuff, you have to imagine this is nation state stuff at the typhoon level. Where are we going? What happens next? Costin says this is ripe hunting ground. We've seen the hostage video, we've referred to the hostage video, which in fact is the ex-CEO, Vivanti, in a hotel room.

basically saying, we'll take security seriously. We are going to remake everything. We got security religion. Everything is going to be fine. We're going to work heavily and we're to do all this massive investments. Do we believe that this is actually happening in the background? Do we give them some grace and a year or two to really get things fixed? Or how do you feel? What, is this level of confidence that we'll somehow get a grip on this?

JAGS (19:02.834)
I have no hope whatsoever that the situation with Avanti is getting better. And I'll say that not out of just being completely jaded as much as I don't see what the actual pressure is. Right. Like, I would love to think that the company goes, hey, you know, this is an existential threat to us. The entire market is suffering because of our

you know, poor practices across the board. Maybe if we invest heavily right now, we will be the market leader in a year and a half by virtue of actually being like more secure and able. And I think that would be like a healthy, long, like medium to long-term strategy. But this is not a time for mega companies to take on medium to long-term smart strategies. They're almost all thinking on like a short-term

a time scale as possible. So in that sense, this is where I go back to like my umpteenth rant about like misaligned incentives, which is, you know, I know that we shit on the pledge all day long for good reason, but the reason that we do, or at least that I do, is that that was such a clear moment for applying sensible pressure of some sort, right?

Whenever you say people should pay with their pockets, we know that that's that's a very disingenuous statement when there are no other options on the table. So what you really have is okay when the market is dysregulated and like just in such a sick place, normally that's when you get some type of regulator or some kind of market alliance or some sort of

certifying organization or somebody who objectively comes out and says, this is bullshit. You have a low quality product. You all have low quality products and like, fine. Don't like, let's not keep ranting about regulation. How about liability? Right? Like I would love a lawsuit that establishes a sense of liability for, Hey, you know, just to pull a random name out of the hat. Pepsi got hacked.

JAGS (21:25.104)
by the Chinese because of this, of an Ivanti appliance. They had an amazing network that was perfectly secure. They had logs, they had everything, but this Ivanti shit on their perimeter opened the door and they lost access to their formula. Not that anybody wants the formula for Pepsi, but like, yeah, this, you know, fuck it. like, anyways, so, you know, you get that. My point being like,

Ryan Naraine (21:43.206)
I was just gonna say.

Ryan Naraine (21:51.078)
See you.

JAGS (21:54.34)
I would love to see a Pepsi lawsuit against Avanti that says, hey, fuck you. We paid you. We did our best. We were on it. We hired the right people. We put all the right appliances. We monitored. And instead you like left us in this sort of completely porous open environment and look at the material damage to our company. And like, I think that's the last bastion of, you know, where I hope to sort of salvage some sort of,

of accountability and pressure, but it is dependent on something that may not be an option at all, which is software liability and like sort of this notion that you are actually responsible for what you cause in those environments. But like, that's what I'm waiting for. Without that, the notion that Ivanti is just choosing to fix itself or Cisco or anybody else seems massively optimistic in a way that I'm not ready to give them.

Ryan Naraine (22:53.318)
risk of boring the audience, Costin, want to ask what is the alternative? I want to make a decision with my pocketbook and say rip Ivanti out of my network completely and go here, where do I go? I don't go to Fortinet because they're also in the list. Where do I go?

COSTIN (23:10.382)
Again, think it's this kind of catch here that people who buy this appliance, they just want to take my money and just I want to forget about it. I need my network to simply work. I don't want to bother myself with settings or configurations or Syslogs or virtual machines.

ideas, things like that.

Ryan Naraine (23:40.742)
Yeah, but you're being popped. You're being popped on a monthly basis. At some point you gotta do something.

COSTIN (23:44.558)
I know what you're saying. So I'm far from from the guy who can do the marketing pitch for any of these solutions or recommend you the straightforward replacement. But to be constructive, I wanted maybe to suggest one thing, which is can we get the Dave Weston of Yvanti come on the podcast and tell us what they are doing effectively?

to improve the security, reliability, patch, buffer overflows and all those things. like the same way Dave Weston does it for Microsoft, right? When he published about Rust in the Windows kernel, things like that, isolation, leveraging the latest features in TPMs, modern platforms and so on. Like, can we get whoever's in charge of that at Ivanti?

Ryan Naraine (24:20.54)
What should they be doing?

COSTIN (24:40.782)

come and explain to us like what they're doing.

Ryan Naraine (24:44.061)
What do you think they should be doing? Let me put you in charge, Devanti, there. What should be the priority? Is it bringing in external experts? Is it going and getting a big giant pen test by a Bishop Fox?

COSTIN (24:46.242)
Mm-hmm. Mm-hmm.

COSTIN (24:51.598)
The easiest thing is just to do pen testing of their solutions. Like this is the easiest. So first of all, hire a reputable company to do pen testing and try to weed out as many bugs as possible. That's one. Obviously a bug bounty program to motivate researchers to contribute and try to find bugs in their stuff.

I would establish a department inside Ivanti who is responsible for finding bugs like leveraging AI specifically to find buffer overflows and the likes in their source code base. Or the dedicated department with five, six people specifically for this task because I mean, this is one of their biggest issues. Then I would get someone to review what is like the...

the platform that everything is based on, like the version of Linux, what is the foundation, and investigate how to update that to the latest versions of the Linux kernel and mitigations and security protections that we have in the latest versions of Linux, or if it's even feasible to switch to something else as, again, like the foundation of the whole platform. Then I would also...

try to rewrite all the backends, try to get the read, identify what is the reason for all this buffer also. Is it like C code? Is it C++? Is it again, like what is the reason for that and replace it with better memory safe alternatives. Rust is what everyone is talking about nowadays, but I would just try to replace that, rewrite it.

And very important in my opinion, if you ask me, I would commit to like every quarter publish an update of what has been done and what like has been achieved. This is what we have done. We got rid of this. We rewrote that. And at the moment, we still need to work on that and that and that and that. Like to see like a transparency and the roadmap and not just Ivanti. I mean, this is a

COSTIN (27:13.518)
you can apply to any company selling these appliances.

Ryan Naraine (27:16.085)
Yeah, all the guys.

Speaking of China and typhoons, we barely touched on it last week because it was breaking at the time when we were on the air, this US sanctioning this Chinese integrity technology company for the link to Flux Typhoon. With all this typhoon activity and China activity, do you expect to see a lot more of this OFAC sanctions coming down the pike for some other companies? Juan?

JAGS (27:47.018)
I think we hope so. Right. Like the, the idea being that these indictments kind of tend to either reveal or cement some understanding about where, sort of what the infrastructure is that's supporting some of these different threat actors, right? To us, they're just threat clusters or just unks. And, you know, maybe you got lucky and you stumble upon something that lets you know, Hey,

There seems to be like a company here or somebody messed up and like you can kind of relate and like the kind of work that like folks like Dakota Carey do so well, but you never have A, either you never have that kind of clarity on your own or B, you can't publicly substantiate it in any meaningful way, right? Like it's a lot harder for a private sector company to come out and say, hey, we see all of this related to this company in China.

There's usually like liability concerns about that. don't, you you can, it's like the bullshit that we saw with, with Appen where it's like, yeah, that's enough. You know, just mentioning this name or whatever is enough for them to try to use some bullshit legal recourse to try to like stop you from, from publishing. So you don't usually get that information coming out. And it's why something like intrusion truth worked so well where it was like, basically somebody just whitewashing.

this information and maybe parallel constructing it or maybe just pointing to what was already there. But essentially somebody was putting it in the public record and the fact that it's in a blog somewhere means that we can all finally just point to it. So I see the indictments work in the same way. don't expect them to have. Yeah, like, you know, I don't expect indictments or sanctions to in themselves materially affect how these places operate.

Ryan Naraine (29:27.095)
Sanctions.

JAGS (29:37.158)
but they give us enough to be able to find other ways to latch onto these things, publicly discuss them, and then hopefully add some friction and some capacity. Or at least understand how the MSS, PLA, et cetera, are working where you go, yeah, they seem to always outsource things in this way. There's a company that looks like this. Their registrations look like that. This is what the kind of profile people that are working there. This is the kind of a...

profiles that they're putting up for like job postings, like all those things allow you to in some way round up a bunch of other possible vessels and vehicles that are being used for this. So it is useful from a research perspective. So I hope there's more.

Ryan Naraine (30:16.693)
this intrusion truth. Do we know?

No, we got some, we are on this podcast and here in the United States, all these blog posts are blaming China, blaming China, blaming China. But we've got news out of China Daily, a Twitter account, I'm showing it here on the screen. says, the legacy media blames China for hacking, but reports reveal Volt Typhoon is linked to US intelligence using tools like Marble to shift blame.

JAGS (30:22.162)
Fuck it, wait no.

COSTIN (30:36.376)
Who are they blaming?

JAGS (30:49.189)
Wow.

Ryan Naraine (30:49.252)
Who is the real hacker? Let me play this video for you guys, because it's fascinating to me and I want you guys to respond to it in real time. This is a video that was posted on X by China Daily.

Ryan Naraine (31:20.816)
Let me pause it right there. Let me pause it right there. Apparently there's a bombshell report. don't know. Are you guys familiar with what a bombshell report is?

JAGS (31:29.65)
actually don't know what it's referring to.

Ryan Naraine (31:32.269)
What is marble?

COSTIN (31:32.43)
What is marble that's that's a good question by the Marble is a library that was originally leaked by WikiLeaks I think in the vault seven sets which was allegedly used for false flag and string obfuscation so To be honest like if you ask me, I don't think we have ever seen this being used for real so I don't think we've seen any kind of tool or

any kind of binary that was leveraging something that looks like marble So it's it's a bit funny that they would be using this story from almost 10 years ago if you want to somehow shift the blame from Volt Typhoon, which again Nobody's saying right that there's Chinese keywords or strings inside the tools used by Volt Typhoon, right?

there's like no such claims anywhere like typically the bombshell report doesn't say there's Chinese writing inside vault typhoon scripts I don't think it says that

Ryan Naraine (32:32.998)
Well there is a bombshell report that says it.

JAGS (32:35.666)
bombshell.

Ryan Naraine (32:43.09)
Let's finish up the video.

COSTIN (32:46.222)
Let's go.

JAGS (33:14.917)
Wow.

Ryan Naraine (33:19.412)
Wait a second. Is it US intelligence? Is it Microsoft? Or is it Lumen? I'm really laughing about this, but like this is the official, we have to treat this as the official government attempt or response to this. Juan, what do you make of bringing in a Microsoft $9 billion deal and Lumen US defense deal?

COSTIN (33:20.142)
Who benefits?

JAGS (33:39.014)
I mean, I've said this before, like I wish that $9 billion bought the US government some actual cooperation from Microsoft, you know, to this level. But it's actually, I mean, the whole thing is pretty hilarious just in how patently idiotic and obviously grasping at strings it all is. I'm laughing.

I'm also feeling like a little breathless in the sense of like how completely shameless this this whole setup is. There's no I don't give a shit what your bomb. I hope there is a bombshell report just to be able to like, you know, highlight and quote like how poor the reasoning has got to be behind this. But this is just straight up innuendo at this point in a way that makes them look fucking stupid.

And this is the argument that we had before with that, that publication that was going off about Dakota carries research and how like we don't take threat Intel seriously out of the Chinese and look at, know, how much they've contributed to all this research about Stuxnet like fucking 10 years ago. And you go, yeah, but then we see stuff like this coming out and none of you, like there is no Chinese company that will come out and say, actually China daily, like

What you're saying is stupid because of X, Y, and Z. And we all know why that's not happening, obviously, because it would fly in the face of the party line. But that's precisely our point when we look at the Chinese threat Intel companies and teams and say, yeah, we can't take you seriously at the level of anybody else, right? Like at least out of Russia, we've seen Russian companies

you know, come out with research about Russian APTs and Russian companies come out and say, yeah, this is, you know, this, this claim from whomever is, is kind of spurious. We've never seen so much as a hint of that coming out of the Chinese research team. So yeah, I'm sure you have brilliant people at the same time, whatever sort of tongue, you know, biting is happening over there. It doesn't make you look anywhere near as good or objective as, you want. And this is a prime opportunity.

JAGS (35:54.342)
for Tencent or 360 or whomever to come out and say, actually slow your roll, this is fucking dumb. Yes, you could argue this, that and the other and on legitimate terms, but this argument is fucking stupid.

Ryan Naraine (36:06.911)
But just last week we talked about being naive to suggest that China doesn't have the ability to do much better. Like why is it so amateurish and rudimentary and almost like comical when we know for a fact that they have the technical chops to do it? Is this just kind of a political top-down? We're going to just stay quiet. What do you think is happening there?

JAGS (00:11.183)
So, sort of claiming that this is some kind of like conspiracy, sort of top-down sort of thing, entails a level of like overt coordination that I think is more nefarious or yeah, more planned out than it actually needs to be. When you live in a place like this, when you live somewhere that is this sort of restrictive and punishing and, know, fascisty, you...

You also get a certain amount of self-policing that is enough, right? Like we're not saying that every company, every threat intel company in China is collaborating for this disinformation campaign. What we're saying is they just happen to be very quiet about things that are clearly relevant in their space that they having the talent we know they have are in a position to come out and say, yeah, no, that's not how this works. What you're saying is not true.

There are real instances of the US hacking the Chinese and there are real instances of misattribution. But no, that this is a stupid tabloid story. And the fact that they all stay quiet, we can all understand why in that government and that regime and living in that place, you are not going to take your life in your own hands and decide to go correct the China Daily story that seems to follow the party line as you would expect it.

But that also means that we don't get to respect your objectivity and contributions in the space. So you have to pick one or the other.

Ryan Naraine (01:46.034)
Let's continue.

Ryan Naraine (02:14.067)
It's a disinformation campaign by someone to enrich themselves. I mean, this really strains. I don't know. I don't know what to say. do we closing thoughts on this video, Costin? You're taking deep breaths.

COSTIN (02:30.972)
First of all shout out to our friend Will Bushido Token who sent us the video to comment. Go follow him on X. That's Bushido Token. What can I say? It's interesting to see this kind of disinformation videos claiming to expose this information. And I think that it's interesting that this where does this obsession with the marble framework come from? This is not the first time by the way that

they're trying to mis-redirect attribution efforts. I Russians have in the past also leveraged this marble framework, like as an example of why Russian operations may be something else, right? Based on the strings alone. So I think whenever you see signs of someone using this as an example, it's typically just very poor, poorly engineered.

attempt at spawning new disinformation fake news campaigns to misdirect attribution efforts.

Ryan Naraine (03:40.502)
We also got news out of Japan. The Japanese National Police Agency published an advisory on Wednesday accusing the Chinese hacking group of targeting and reaching dozens of government organizations, companies, and individuals in the country since 2019. What was the name of this campaign? Mirrorface. What do we know about Mirrorface? What do we make of this? What's the attribution? What's the quality here?

COSTIN (03:57.751)
Mirror face.

COSTIN (04:08.38)
This is another interesting situation here because so mirror face I think the ones who have also published about this are Trend Micro who call it Earth Kasha and what is interesting here is that the use of this load info malware which has also been associated with the APT-10 so if you're kind of wondering is this mirror face APT-10

I think nobody can say nobody can actually say that for sure so for instance in one of their VB talks trend Micro says that They use the term a PT 10 umbrella so they think that this earth kasha or mirror face is maybe a subset one of these subsets of another Thing is so related to to a PT 10 now a PT 10 has been targeting Japan and

a lot more for many many years like a long long time they've been around for a lot of time.

Ryan Naraine (05:14.891)
The public, the Japanese report here mentions 200 cyber attacks over the past five years. mean, when you say a long time, longer than five years?

COSTIN (05:24.732)
So I guess that the first reports about Mirrorface slash Earth Kasha, they do go back to 2019, but EPT 10, it goes back maybe more than that, like at least eight years, according to my own research, if you want. I think it's interesting that there's a lot of new research coming out of Japan these days.

not just the Japanese government, but there's a lot of very good Japanese threat Intel companies. NTT, for instance, has a research group that's been publishing a lot. Itochu, they're also pushing very, very good solid research on Chinese attacks. And there's a lot happening from China targeting Japan these days, a lot. It takes the form of supply chain attacks.

takes all sorts of different interesting attacks like for instance targeting update mechanisms of certain Chinese or Japanese language text editors so targeting yeah like those kind of things for Japan and for China that are being used in Japan or even like Wi-Fi style attacks similar to the one that

Ryan Naraine (06:33.749)
Hangul and these word processor type tools,

COSTIN (06:47.26)
Villexity and steve there was talking about so there's a lot of happening in Japan these days from the point of view of China and for sure a PT 10 they've been super active and earth kasha There's a lot of documented evolution of their load info toolkit, especially from trend by the way

Ryan Naraine (07:08.953)
Juanito, you've consistently said that China, Chinese APT bores you. But you've also said quite bluntly that China is kicking our ass. It feels like China is actively kicking everyone's ass. Or are we picking on China? Are all these governments kind of colluding to just China, China, China, China, China? What is going on?

JAGS (07:27.471)
you

No, I don't think we're picking on China. think China is just the most bracing out of all of them. It's just scale and bracing this. There's not even a need to really hide things. Nothing seems to stop the drumbeat. And you just have these operations of scale that dwarf everything else that's going on. I would also point out that it's not necessarily that the Chinese are

so super spectacular as much as I think they have, like I said before, like they've engineered their way into our blind spots. What I think they've really figured out is just like, everyone is systemically weak in this way. And then they've optimized operations to just like basically laser dance in just the right way in and out, up and down, and just in such a way that our telemetry sucks.

that they don't get collected on. They don't actually get meaningfully stopped. You're not going to see any sinkhole and you're not going to see any redirecting. You're not going to see any blocking. You're not going to see clear infrastructure that you can latch on to. They've just been incredibly smart in understanding how just in what way we're all weak and leaning into that programmatically. Now, I don't get the whole picking on China.

Ryan Naraine (08:59.515)
Spy spy, all spy spy, all governments have an espionage unit that spies. Like why are we making a big deal out of China being caught spying?

JAGS (09:09.391)
It's more, know, spy spy and spies will continue spying and there's perfectly good reasons for spying. I think it's more along the lines of what are you spying for and what are you using that for? And for some reason we find it more objectionable that we, yeah, when it's not for freedom, you know, when it's for like economic warfare of sorts. But I mean, it to me,

Ryan Naraine (09:24.74)
it's not for freedom.

JAGS (09:35.351)
In my very rudimentary understanding of Chinese five-year plans and how their whole manufacturing endeavors and general economic planning goes, there's been an understanding that this espionage, at least the economic espionage, is a key tenant and a key pillar in how they're meant to succeed. You have all this manufacturing capability. You have this cheap labor.

what keeps it cheap is not spending on R &D. It's not spending on trying to catch up with so-and-so or figure out how it is that they did X, Y, and Z. So I think what's interesting about it is seeing, how brazen it is, while also, B, how clearly established, systematized, entrenched a part of the way that this government and this sort general country structure is propped up on that notion.

That said, look, everything we've been talking about with the typhoons and stuff, it's not economic as far as we can tell. It's about war prepositioning. It's about actual espionage. It's about counterintelligence. It's about just plain old fucking intelligence of like, what is a president-elect planning? What is like, those are all well established things that you do. What I think is interesting about this is

I think if the Chinese are feeling picked on, they're only suffering from success because the conversation I hear us having, or at least the one I hope we're having, is one about the extent of our failures. It's not about the extent of their successes. We really, I wish we were having a more clear conversation about like, look at how, just how successful the Chinese are, right? Like it's.

super hard to run agent networks inside of China. It's super hard to keep the Chinese from having all of this infiltration, insider threat type espionage inside of the United States. It's super hard for us to keep the Chinese from buying property in strategic locations of the United States the way that like Kristin Del Rosso and Maddie DeVos research from LabsCon clearly showed.

JAGS (11:52.299)
super sensitive military base in the middle of God knows where America and the there's massive plots of land near those bases that are owned by Chinese companies with like barely anything hiding that type of ownership. Like there's so many ways in which we're getting played. And so there's the discussion that we could have about look at just how successful the Chinese are being in setting up this sort of like intelligence checkmate that is very hard for us to

to navigate just on the basis of our own laws and our inability to help ourselves. And then there's the alternate conversation, which is look at just how fucking weak we are in this, that, and the other way. you know, yeah, China can feel picked on, but they're suffering from success. And I think we need to be a little more sober about treating this all as a discussion of like categorical failure that we should use to pivot rather than wait to make it a postmortem.

Ryan Naraine (12:51.338)
Do you have a thought on the incoming administration response to this? Because they're going to be taking, we're 10 days away from inauguration of a new administration that's actively aggressive against China on tariffs. You expect this to kind of be folded into a lot of those diplomacy efforts upcoming. What is your feeling on how the new administration treats this?

JAGS (13:15.983)
So, I have a very specific way of thinking about this administration, this incoming administration, which is actually that...

I think of it as like grifter city, which means that I can't predict how these things are going to play out. I can tell what some of the usual dog whistles are going to be. like China is an easy drum beat for this administration, right? Like there's very little reason for them not to come down on China or treat them as categorically evil and categorically bad, which I think is narrow minded in the sense that

the US and China have a symbiotic relationship and that's what makes it so complex, right? If we were talking about Vietnam, you go, yeah, Vietnam has some manufacturing, but if Vietnam were to vanish off the face of the earth tomorrow, God forbid, it's not like the US finds itself like without any kind of mooring in trying to figure out, my God, the place that we relied on to make

everything has suddenly vanished. What are we going to do? Right. And that's, that's where I think we, I'm not trying to be naive and sort of say that we need to be more supportive of China or whatever. But I think that when we categorically think of them as a complete evil and a complete like morally absolute reprehensible place, which you can make that argument on the basis of their human rights record and blah, blah, blah, blah. But that

undermines the fact that we're in a symbiotic dynamic with them. And the argument in that case, if you're smart, is to say you want it to be symbiotic rather than parasitic. And that's not something that we are handling very well. What the US is not, like every conversation about China fails to account for the fact that if China were hit by a meteor tomorrow and disappeared, we would be mega fucked a bunch of different ways.

JAGS (15:22.509)
because we are reliant on them for all kinds of manufacturing that we cannot just snap our fingers and replace. Like it would take a categorical change in lifestyle, change in production, change in import-export dynamics, change in everything to suddenly account for a non-existent or non-functioning China. So that's where I see us being a bit smooth brained in how we consider them, how we talk about them.

That said, you asked about this administration and my problem with them is not what they're willing to do. It's not what they're, it's not what they're gonna say they're gonna do. It's the fact that what you get with this type of administration is, like I said, grifter city. Like what con man, what convenient person finds themselves in a position to suggest whatever harebrained scheme they think is the right way to go.

And that's not all categorically bad. I've heard stories of specialists in given areas who were able to drop off a proposal in just the right office during the previous Trump administration. And that shit became law without anybody taking, like it became.

policy without anybody taking so much as a red pencil to what the original proposal was. So clearly they're completely asleep at the wheel and somebody can come in and be like, I think it's important for us to, you know, sanction or put friction into the import, export and production of bicycles. And you go, we never would have thought of that. But it's like, this is a major economic tenant. like, I thank Demetrius for this story. And you go, this is like, that's actually brilliant.

Ryan Naraine (16:57.74)
Yeah.

JAGS (17:06.871)
Like that's something that somebody who understands very well what's happening in China and where it's going to hurt them has decided to like put this forth and they happen. And because

there's no barriers, no friction, no pussy footing, nobody's sitting there gatekeeping. This clever thing has made it out to see and become policy. But the fact that there is such little gatekeeping and there is such little discernment can also mean that Rudy Giuliani or whomever like what other other

random idiot happens to be in the room can also push an absolutely idiotic idea like let's tariff this thing that we have no like homegrown alternative to and you go well that's just fucking stupid but that's also an idea that will make it out to sea because there is no discernment. So my issue here is it's a fucking free-for-all. What is gonna happen with China? I don't know tell me who was in the room at the time and what their brilliant fucking clue.

was and like what they decided to do. And that's what happens when there are no adults in the room. Like when Bolton looks like the most, when that walrus looking motherfucker is the most adult looking person in the room, that you're in trouble. And that's what's going to happen next. It's like, we just don't know where things are going because we know what they care about, but we don't know how they're going to decide to manifest that.

Ryan Naraine (18:29.414)
But we have to, there has to be a response though. You can't publicly be saying the Chinese are living all up in our telcos and listening to all our phone calls and downloading all our text messages. we just kind of go on, we move on with some sanctions. I don't know, Costin, you have a thought on how the US responds to this?

COSTIN (18:50.812)
I think the well first of all isn't it's probably not just us because I think it needs to be a more global answer like the kind we have seen for instance with Huawei in the past just to tell your story about a decade ago we wanted to buy a Cisco switch for maybe less sensitive network and that Cisco switch was like really expensive you know typically Cisco equipment is super expensive

And our hardware provider, you know, we told him, man, that's expensive. And he said, like, listen, I have like, if you want that, we have an alternative. We have a Huawei switch, which is five times cheaper and faster. And we're like, no way. Can we test it? we got it. Yeah, it was faster. Clearly it was much, much faster. The hardware was amazing. It was five times cheaper. We ended up buying it. We deployed it.

I think that maybe it hanged once, once like two years, like in two years it hanged once. We had to manually reboot it and then it worked fine. But we are seeing the same kind of analogy nowadays. Just this week I saw a big, big advertising for a Chinese electric car called BYD. Maybe you guys are familiar with that. Have you seen it in the US yet? There. No?

Ryan Naraine (20:13.861)
there are no Chinese electric cars here

COSTIN (20:16.134)
They're pushing very hard in

JAGS (20:16.887)
Rivian. Rivian. We do have some, right?

Ryan Naraine (20:20.539)
Rivian is Chinese? Rivian is a US company? No, no. Rivian is a US company with factories here in the US. I'm pretty sure about it.

JAGS (20:22.285)
I thought so.

COSTIN (20:28.7)
BYD, google this BYD So there's like this huge advertisement of Chinese electric car BYD which is all over Europe It looks like a Porsche Cayenne It is a Porsche Cayenne I mean it's copied, it looks identical maybe it's 2 centimeters longer something like that This is a BYD So they have like

JAGS (20:52.158)
wow.

Ryan Naraine (20:54.353)
That's Chinese BYU ID.

COSTIN (20:57.228)
lot of different models, but the one that I saw it looked just like a Porsche Cayenne and it was 33,000 euros the the electric Porsche Cayenne is like five times more expensive and

JAGS (21:11.951)
I stand corrected, Rivian

Ryan Naraine (21:15.368)
We don't fact check but we need to fact check on that one. Yeah, Costin, go ahead.

COSTIN (21:18.628)
So I asked

JAGS (21:22.625)
We'll at least try.

COSTIN (21:24.346)
Yeah, so I some people like, hey, would you buy that? mean, it looks amazing. It has a 1000 kilometer autonomy. can drive a thousand kilometers with it. It looks like a Porsche Cayenne

and people who own these cars, they say they're formidable. They're amazing. And it kind of reminds me of that Huawei story. Like the hardware is good. Maybe it will hang once every two years. So the pitfall here is that, yeah, being much cheaper.

The only risk and everyone's saying like, yeah, but like there must be a catch. What do you get? Like telemetry, they're recording all your trips. What are they doing? They can remotely lock your car or maybe remotely break it or can they spy on your conversations in the car and come to think. Yeah, like that's what I meant. Like Tesla Elon Musk can unlock your Tesla if he wants, right?

Ryan Naraine (22:12.137)
How is it different from Tesla though?

Ryan Naraine (22:18.206)
Yeah, we just had this issue here in the Las Vegas incident from New Year's Day. Tesla remotely opened the car. Tesla was able to give law enforcement every stop that the guy made on the way to all his charging stations. So everything is recorded anyway. I mean, this is the future.

COSTIN (22:30.534)
They recorded everything. Yeah.

And there was this story also about contractor like a subsidiary of Volkswagen who leaked the history and the locations of all the electric cars from the Volkswagen group. And again, the question is, why are they recording all the locations? So they're tracking, they're tracking wherever you go, wherever you stop, they're tracking that. So I guess the issue here is that what China is doing, yeah, that's cheaper, perhaps sometimes more

like modern hardware, better, faster, or whatever you want. The only solution is tariffs alone in the US will not fix it. Only maybe tariffs everywhere, like European Union coupled with the US, with the great state of Canada, with Greenland and the Gulf of America, America and Panama can all together

Ryan Naraine (23:25.684)
Panama. And the Panama Canal.

COSTIN (23:31.836)
putting tariffs might make a difference. But otherwise, we are no longer 2012 when China was stealing technology and trying to create replicas. It feels to me that we are in a totally different position when sometimes these are, let's say, on a pure capitalist market, the solutions are more attractive, if you want. So that's the true issue.

Ryan Naraine (24:00.788)
And this is active all over Latin America, all over Africa. mean, I'm from Guyana. In Guyana, we have Chinese Huawei equipment being deployed at scale there because of this. It's cheaper, it's

faster, it works, and they simply can't afford American technology. I mean, if this is the future, Juan, we're going to continue to have this boring conversation about China on the podcast every week.

COSTIN (24:04.279)
Lure up.

JAGS (24:26.031)
Yeah, I mean, to the extent that what we're trying to espouse as foreign policy are effectively unfunded mandates, right? Like going to these different countries and, we've talked, like I said, we talked about this before, right? You go into a place, you say, hey, you know, Huawei is garbage and it's part of like Chinese hegemony and you shouldn't buy their stuff. You should buy this stuff instead. And like these people look at you and they go,

This is a $250 million project to get cutting edge technology to an African nation. We didn't have $250 million sitting around. We don't even have $50 million running around. The State Department is gonna come and offer me $20 million to spend on US tech, however they see fit, which isn't gonna be mindful of like what the grifting economy.

in its real politic pragmatic form, how it actually works in Africa, Latin America and so on, where like greasing palms is a part of doing business. So you're complicating the use of that money. And you're offering me 20 mil compared to the Chinese who just showed up here and said, oh, yeah, this $250 million project will give it to you for half and will finance that half over 35 years on like natural resources. And we'll send you all the people to build this shit. And you go,

I mean, it's not a contest. There's no discussion to be had. It's do you want 5G and cloud or not? It's not do you pick between this thing and the other? So in that sense, the US and Western alliances were never going to succeed in Africa and Latin America because all they've done is finger wagging instead of actually logistically making things possible.

So there is there's just no argument on the financial hegemony side and what we need to admit is when we go spend however many trillion dollars terraforming portions of the Middle East you're no longer in the position to then go and spend however many trillion dollars subsidizing a better Western aligned order in these other places and we are going to really feel the suffering as we keep trying to move this stuff forward when we realize that we allowed

JAGS (26:40.429)
Russia and China to have a complete fucking free for all in Africa and just take over all these places where like rare earth, like rare minerals and all kinds of important materials are being mined. We've just let them go like crisscross the place and literally slice it in half and choose what they want and influence elections, influence financial policy, influence all these different things and just not even try to compete there. And we are going to

really feel that burn if we're around for long enough to figure out how that's going to impact us.

Ryan Naraine (27:14.951)
I got one more story here just staying in China just so we can close the loop on this is a new report out of threat book on APT32 poisoning GitHub and targeting Chinese cyber security professionals and specifically large enterprises. This is a Southeast Asian APT group Ocean Lotus. Do we know who is behind Ocean Lotus, Kostin?

COSTIN (27:33.654)
We know, we know, it's a Vietnamese team. So they've been around for some time.

Ryan Naraine (27:36.972)
Oy, oy, oy.

And what's the story here?

COSTIN (27:42.556)
So I mean one of the top targets for OCEAN LOTUS slash APT-30 to have been Chinese government and Chinese companies and Chinese researchers I think is kind of an interesting variation here. So what they were doing in this case, they published an interesting exploit I think for Cobalt Strike it was

that was poisoned with a trojan and then they seeded this all over Chinese cybersecurity forums so that the Chinese researchers would actually download play with it and get infected. APT32 is a kind of, I think it's an interesting fish and they've been around for some time. Even I think if I'm correct, leveraging Zero Day. So they were leveraging.

zero-day exploits. don't think they were developed by them, but they were acquired or purchased from other tools, from other groups or from other exploit vendors, if you want. But it's kind of funny to see how the the traffic chain looks like. China is spying on the US, Vietnam is spying on China, and like so on and so on. Everyone has their nemesis. Everyone has like a neighbor.

that is always interesting to know what they're doing in their backyard and of course in case of ocean lotus they're not targeting just China but for them I think China is a top interest.

Ryan Naraine (29:21.289)
one is Vietnam and some of these South East Asian countries are they pretty active is this something you track closely?

JAGS (29:28.055)
I mean, definitely on the ocean lotus side of things, Like they have, they're actually impressively keyed into some of the intellectual property theft stuff as well. Like you could see them going after a lot of different manufacturing adjacent companies in the United States that you would have expected the Chinese to be at. And they're probably there too. But I think it suggests

sort of a similar approach to how they want to handle their economic standing. That Vietnam, you know, it might not be operating at the same scale as China when it comes to manufacturing, but I think they see a similar avenue to their survivability and their thriving. And in a world where

You do see mega companies like Apple trying to back out of being solely reliant on China and they're trying to go to India and they're not getting the results that they want from Indian manufacturing standards. There is opportunity for places like Vietnam that I think they're quite clever in making sure they're positioned for. We obviously are not taking that financial, quote unquote, quite the same way as with the Chinese, but

I think it is very interesting to look at something like Ocean Lotus and say, well, clearly some part of this is very similar to what we see from the Chinese, similarly minded. And then you have what you would expect of like traditional espionage, especially of the Vietnamese going after the Chinese. And I love that for them.

Ryan Naraine (31:00.465)
Austin, got a handful of IOCs here related to Ocean Lotus ATTAC C2s. Have you been able to look at them? What's what do you make of the quality of what the threadbook put out here?

COSTIN (31:10.958)
Well, Threadbook by the way is a Chinese thread Intel company and I think it's one of the more let's say serious ones in the sense that they are not hyping things up like others, you know that have been sanctioned by the US do. So from that point of view, Threadbook, I think they are on top of things. They do publish things like this against

other companies in the sense that they find it before others, which is quite impressive. And I think that over the time I've seen Threadbook publish other research that was quite interesting. So I mean, again, no objections from my side. It seems like super, super interesting stuff. And like I said before, it's good to see a bit on the research capabilities of Eastern

security companies, be it China, Russia, it's interesting to understand what their capabilities are, how often they find things, how they find these things, and the fact that they really do care about them and who they care about. In this case, obviously China cares about Taiwan, they care about Vietnam, probably they care about India obviously and the US.

Ryan Naraine (32:31.09)
If you're not in China, do you care about these IOCs? Do you want to go hunting if you're not Chinese?

COSTIN (32:35.892)
sure because Ocean Lotus is known to target entities outside of China, not just China. So I wouldn't be surprised if they try this in other places or if they will try that in other places.

Ryan Naraine (32:52.569)
Also, I want to pivot to a story out of Watchtower on government backdoors. Pretty interesting research, commandeering expired domains used in backdoors, allow them to hijack over 4,000 systems and intercepting communications between compromised systems and abandoned backdoors for minimal cost and effort to end all the domains. Juan, you looked at this research. What do you like about it?

JAGS (33:16.481)
I mean, I don't love the tone and the memory of it too much. Like it seems so like very satisfied with itself in a way that maybe it's a little too much. but you know, we'll take it for for what it's worth and like sort of its own value, which is to say it is very interesting to see what you can do with all these sort of zombie infections. Right. Like when we talk about targeted attacks and sort of the emphasis on targeted attacks having been sort of the staple of

what made something advanced. think we were kind of, for a period there, we were maybe a little just too impressed with ourselves or too wrapped up in what seemed to speak to us as sort of like poetic, high-minded types of attacks. And instead what you see with a piece of research like this, which, know, just to take a, to skip a beat and say, what is it, right?

These guys are talking about how they went ahead and they registered some, you know, certain types of like defunct domains. And that meant that they, effectively what we would have done for sinkholing to them, it's like, well, you are taking over, what Kostin and I would have referred to as like victim stealing in our fourth party collection paper, which is to say, you know, I take over some of the infrastructure or I hack existing infrastructure.

And therefore all of its downstream victims are now my downstream victims. And that's what we saw with things like Turla taking over oil rig or like Turla trying to sneak into sort of Pakistani operations, Turla trying to piggyback on Andromeda infections and stuff like that. Now, I think that there is a more nuanced point to be made about just how much

how much is out there that is just casually infected with non-targeted things. And I think folks kind of undermine and like laugh that kind of stuff off, right? Like we'd always talk about, hey, there's a shit ton of devices out there that are still infected with Conficker. And people will laugh and be like, ha, Conficker, so fucking old, how ridiculous is that? And you go, yeah, that is ridiculous. But also it says something about the state of security and the fact that like there is nothing about security.

JAGS (35:31.247)
as a state of homeostasis, as like a thing that you return to as something that's just guaranteed, that doesn't actually happen. It doesn't actually exist. You don't just wait and the computer heals the way the body heals and you just kind of move past a given infection. Those things just stay there. And there is a shit ton of value to be gotten out of.

going after these old school type ops, these old school botnets, all these things that have just been left behind, especially when you go after, when you try to like disinfect or curtail some of these infections the way the FBI has done so many times of like just kind of squashing one piece of infrastructure, squashing one existing mechanism for how these things are infected and managed.

but leaving all of this zombie shit just living in memory, living in infected devices and whatever. And then somebody comes in, in this case, sort of a couple of clever folks with a nice blog, but it says so much more about what's out there to be gained by just being clever enough to understand the infrastructure. Go, here's a weak spot. I'm just gonna go hack it, buy it, redirect it. now defenders are in no position.

to leverage a command to disinfect those machines. That's supposedly a liability and supposedly illegal, but attackers are in a perfect position to just go and take that shit over and go, hey, here's my 200 new infections that I'm now going to leverage in some strategic fashion.

Ryan Naraine (37:06.177)
Kostin, do you believe Watchtower, the only folks came up with this idea and doing this or you think nation states are already there like Juan mentioned with the Pakistani piggyback?

COSTIN (37:11.785)
you

COSTIN (37:19.879)
First of all, we did some internal research on this about 10 years ago. I think I made a presentation around 2016, maybe 15. Maybe some people still remember it if they're listening to what's that. It was a presentation I did in Amsterdam at one of our meetings. I think that probably you are there as well.

Ryan Naraine (37:34.583)
Remind me the name? Remind me the name of that project?

COSTIN (37:47.504)
Ryan I think it was before Juan's times But this was like one of the things I noticed as I was investigating Compromised infrastructure there was a web shell in there and the web shell had an encoded payload that would send the Login and password to a remote dot CN domain like a Chinese domain that was expired so registering the domain you would get

pretty much the location of all the web shells that were backdoor that it was thousands, thousands of cases like that, absolutely insane. The other case, the way, which I remember is of the NSA developer that infected himself with a smoke bot variant. And it came from Keygen for Microsoft Office. And at the time of the infection, someone else took over the cnc from that smoke variant so it was no longer the original people but somebody else so just imagine how many of these smoke loaders from key gens are out there with their cnc's expired and imagine how many people actually download them yeah not not just like let's say fake or infected key gens right with gold but with many many other things like even like

JAGS (39:00.815)
Gold and God tech, right?

COSTIN (39:37.766)
The worst thing you can do is just disinfect it and move on, because in reality something much worse could have happened.

Ryan Naraine (39:44.812)
Is there follow on research to be done here from this or is this?

COSTIN (39:48.944)
Well, I was thinking myself to collect a bunch of older key gens like from, bless you, from five years ago, something like that. And try to run them in sandboxes, see where they're beam up and see which expired domains. And again, think whole maybe with the help of our good friend Silas and see how many people are actually still infected out there or could potentially be attacked this way.

I think that would be interesting as another dimension of this pure web shell research.

Ryan Naraine (40:23.706)
And this abandoned infrastructure is not an issue one that's going to go away, right?

JAGS (40:33.347)
Yeah, no, for sure. There's no way that goes away. You actually don't even want it to go away in some ways because it's a corollary that goes hand in hand what we do as far as like sinkhole and redirecting and what folks like the FBI have taken to doing for the sake of like trying to break up operations, which is also why the takedowns tend to be so shitty. Like if they don't actually listen to the researchers and do it carefully, they'll lop off like a half portion of

what the infrastructure, like some connecting node in the middle of things. And then you go, well, but that means that somebody else can come in and sort of revive this or take it over in some other capacity. So in some ways I would even say that some of the takedowns we've seen before have actually furthered this and like made it even more plausible in some ways. I think the problem that you get is more along the lines of what can people do with what they take and what they get access to. And

I think that's an area where we're obviously shooting ourselves in the foot by playing boy scouts and saying, look, like there's this massive botnet. We have access to this piece of infrastructure. We could just push one command and disinfect 30,000 machines and then take out this control node. But instead they go, no, no, that's hacking. What happens if you, you know, issue that command and one of those machines is actually like,

it connected to a baby that's intubated in the in a in an orphanage hospital somewhere so innocent so so so pure. So you know what that abstract completely ridiculous possibility means that we'll just leave them all infected and we'll take out this one server will go to do our press you know conference I'll get a promotion will pat ourselves on the back until our hands fall off. And then like we'll all move on. Yeah, it's like fuck off. But

Ryan Naraine (42:02.342)
Yeah, what happens then?

Ryan Naraine (42:26.15)
Mr. Hawk back over here.

JAGS (42:31.245)
But it is to say like it is the general sort of background radiation of insecurity. And and like Kosen said with the key gens, right? Like you get interesting groups like gold and Gattac. You get interesting components like both like if I remember correctly, Dark Hotel and Animal Farm sort of pushing to make these big bots based on things that were like seeded torrents and things like that, where you go. There is a value to having a bunch of

am I remember that correctly? Kostin, like with some of

COSTIN (43:03.292)
Dark Hotel did have this self-propagating worm, Animal farm, I don't recall it, but I may be wrong.

JAGS (43:07.129)
Yeah. With Animal Farm, I'm thinking about what was it? NBOT maybe? Where you get sort of infected components and the idea is like there is a value to having a fuck ton of infected machines either for like presumably DDoS, but also because the exact same thing we've been talking about. I infect, right. You could have redirection, you can have false flag.

COSTIN (43:15.582)
Mm. Mm-hmm.

COSTIN (43:27.94)
Orbit networks.

JAGS (43:33.867)
implications or you can just go the new Chinese route and you go, I have 30,000 infections. Are there any of them that are in interesting places already? And let's, you know, let's go from there. So there, there is a value to, taking on that sort of operation. and with things, I keep bringing up

gold or GATTAC, whatever you want to call it, because there's something to be said for proactively seeding insecurity in a clear, self-motivated way. You.

Everybody's going to want a copy of Photoshop. Everybody's going to want a copy of Microsoft Word. Everybody's going to want a copy of Windows. Most of these other countries don't make a habit of actually paying for licenses and getting official update channels. So let's see the key gens that are infected already. And coming from the AV or EDR, XDR standpoint, we're not even in a position where we can just proactively kill these things too easily because you could very well

kill the Windows install of some customer, let's say in Ukraine, because you took out the thing that was like the activation bypass for their whole Windows installation, or you stopped their Photoshop from working because they were using a cracked version of Photoshop. This is clearly a source of massive insecurity, but economically, I can't look at them and be like, yo, go spend

$2,000 per computer on software licenses so that you can be secure. It's not an option.

Ryan Naraine (45:10.146)
Speaking of Ukraine, have another story here on my list about Ukrainian hackers wiping a big Russian ISP called Nodex. Ukrainian hacktivists operating under the Ukrainian Cyber Alliance Group claim responsibility for the cyber attack. The attack resulted in the complete destruction of Nodex network infrastructure leading to significant internet outages. Costin, do we have IOCs? Do we know what's happening here?

COSTIN (45:33.064)
IOCs that I know of and actually I was trying to find any IOCs associated with UCA, the Ukrainian Cyber Alliance, which has been around for a very long time, like since 2016. Originally there were like several activist groups that they joined hands and then they brought a few more groups on board and I think over the time

They've done a lot of these wiping attacks, so they've been responsible for a lot of them. This statement from Nodux is funny. There are no deadlines or forecasts. First, we will raise the telephony and the call center. That was the focus. The network has been destroyed. And they've done these before.

Ukha in particular they've done this many times including they've done this to a ransomware group a Russian ransomware group I think Trigona ransomware which was funny in my opinion that they managed to hack that ransomware group and wipe them kick them out of business so it's interesting part of the ongoing cyberware between Ukraine and Russia there's of course the Ukraine military intelligence

who have been doing this kind of operations for a few years already and bragging about it and it's also a lot of these hacktivist style groups on both sides by the way that operate from the shadows some of them with a lot a lot of members like patriotic hackers if you want super super active like for instance some of them especially Russian groups have been targeting

Romanian ISPs as well and for instance they were trying to shut down the DefCamp website, the conference I attended in December in order to disrupt this Western technology conference in Romania. yeah, the hacktivist cyber war on the internet affecting big ISPs.

COSTIN (47:46.876)
I don't know if it's really the largest ISP in Russia, Nodex. Personally, I haven't heard of them before. But it's definitely, I think, a significant event. And again, I have not seen anywhere any kind of UKA IOCs. I checked the Kaspersky website, which recently they've been publishing only about Ukrainian attacks or mostly about Ukrainian attacks.

activists and so on and even Kaspersky who is now exposing this Ukrainian cyber attacks doesn't have anything on UCA.

Ryan Naraine (48:23.411)
This is bar for the course in wartime.

JAGS (48:28.067)
Yeah, at least for what we've seen with this one and it's been a back and forth, right? Like we've seen Russian both state and possibly non-state hackers go after Ukrainian ISPs with some success, right? Like that's what we saw with AssetPoor was, you know, what looks like proper Russian ops. Look, man, if you don't like it, you better suggest a standard or an RFC of some sort and set this straight. But...

Ryan Naraine (48:45.23)
You guys and these names, my god.

Ryan Naraine (48:52.194)
Hehehehehe

JAGS (48:55.983)
That's how I spent, I think, my 4th of July weekend. So you just take it. But in any case, yeah, we've seen it happen back and forth a great deal. it's kind of cool as far as infrastructure goes. You go in and you actually wipe out a bunch of servers and you take out what is effectively important infrastructure for large swaths of the country of just like, yep, the ISP is down.

God knows how much else sort cascadingly falls apart. yeah, it just comes as par for the course and you're gonna see this continue to be leveraged over and over.

Ryan Naraine (49:37.06)
of small stories I want us to touch on because we're starting to go along here is a new story from Kim Zetter actually covered this drone swarm stuff that's been kind of floating around the

United States, New Jersey. mean, everyone's like, my God, everybody's seeing a drone and no one knows what's going on. No one is saying anything. And she kind of, she wrote a report on fake radiation readings in New York and New Jersey in addition to this drone swarm kind of fueling this some sort of nuclear scare.

And Juan, you mentioned the Ruben Santamar research when you were doing our annual report thingy. She went back to Ruben, Kim went to Ruben and was able to confirm that this was some sort of fake readings. Help me understand what the reporting is here.

JAGS (50:27.737)
Yeah, so what you end up getting is actually something that I think Rubin started to sort of detail in a kind of terrifying way when he put out his own research, which is like apparently a lot of this radiation telemetry, for lack of a better word, seems to be mediated by really duct tapey, MacGyver-y, shitty sounding, like very rudimentary sounding mechanisms like

you know, websites that don't necessarily have like proper auth and like all these different bits of like connective tissue that make it sound like it's more of a hobby project than what you would expect for like monitoring nuclear like radiation in different parts. And to that effect, it looks like folks were able to abuse that like rudimentary system to be able to put in a bunch of fake readings for like effectively radiation spikes in different places.

And then you let, know, that's one aspect of it. And then the other aspect is you have folks that are so primed for conspiracy theories and like expecting to tinfoil hat they way to everything that you go, my God, this anomalous thing that we can't verify must be connected to this other anomalous thing that we don't understand the whole drone thing. And you go, they're flying drones because they're looking for a stolen nuclear weapon. They're looking for this other nuclear.

you know, potential nuclear disaster that's happening. I think more than anything, I am more aghast at seeing what the quality and standard of what is fueling something that you would consider as important as monitoring of sort of like nuclear radiation spikes. That's not necessarily the most official system, but just one of, you know, the ways that this is done.

then the other side of it is how, how terrifying it is that we are so primed into this, with the whole drone nonsense, which, I have no idea what's happening because I have no idea what's actually happening here, but I also have this to me looks like the kind of, panic. I'm sure people are seeing things and it, but I treat it the same way as like reports of UFOs like

Ryan Naraine (52:35.497)
What do you call a drone nonsense?

Ryan Naraine (52:45.331)
You don't think people are seeing drones?

JAGS (52:53.561)
people see things and then they misreport what they're seeing and then they post a shady video and then somebody else makes a comment and another person speculates and then, you you never go back to the fact that like that video was like of a Starlink satellite or that video was of, you know, somebody flying a balloon somewhere and like maybe there was something off or shady to it, but we are forgetting how much potential we have for like bizarre mass panics and how much like people are

people who want to see things will see things. And then you have all this completely unfiltered social media like network effect that makes people think that there is a massive set of incidents that are unaccounted for. And in reality, what you have is, like I said, network effects where you can effectively convince a small population that there's a whole set of other people substantiating.

something that in reality is just a bunch of unverified claims and grainy footage and people who just want to believe something bigger is happening.

Ryan Naraine (54:00.157)
costing back to UFOs.

JAGS (54:02.217)
Hey.

COSTIN (54:02.972)
Brothers, I am such a sucker for all these stories. I mean, I believe everything. I want to believe that's my motto. And back in the days, I think in 1988, I've seen a new I've seen a new F4 myself. mean, nobody can take that away from me. I've seen it in Romania one evening. I've seen it like moving just like a satellite in the sky, but taking sharp turns.

at impossible speeds, would be like, I don't know, 10,000 kilometers per hour flying in triangles, like in a zigzag pattern for half an hour at least before it quickly sped away. So I want to believe, I mean, if it wasn't drones looking for what is called a broken bow, then maybe it's UFOs, maybe it's aliens. We can still hope.

JAGS (54:59.203)
I think we all hope that it's something like that. And that's precisely the point. We want to believe. I think it's not to say that everything is hysteria and there's nothing out there that we don't already know about. I think the world is much more composed of things we don't understand than we'd like to think in this sort of like human, very human, very flawed hubris.

But in this particular case with the drones, I think we're in such an obviously bad state of like information fidelity that I'm not saying nothing is happening. I'm not saying that no one has seen anything that would be worthy of investigation, but I am so suspicious of the network effects right now as far as like how it's affecting our ability to just sensibly point to these are the three interesting

something is actually there, instances that we should investigate. And these are the 200 instances of random people whose standard of truthiness is too low, who are also amplifying, adding.

putting up pictures, putting up a shot of a UFO from Romania from seven years ago as if it is a drone footage from New Jersey yesterday. And like there are no community notes, there's no verification, there's no fact checking and the thing just keeps snowballing into something bigger and bigger and bigger.

Ryan Naraine (56:30.678)
We just got a new Samsung S24 update that rolled up all the Android fixes. And in addition to all the Android fixes that came, we got a word from Google Project Zero yesterday, Natalie Silvanovic tweeted about, let me just share this quickly.

Natalie Sylvanovic tweeting about unrestricting an issue that shows a fun new attack surface. Android RCS locally transcribes incoming media making vulnerabilities in audio codec now fully remote. Bogging an obscure Samsung S24 codec is zero click. There's a little bit of confusion, not confusion, uncertainty over whether it's exploitable. When I see zero click in Android, know, costing my hackles raise and you start to think about these mercenary groups that.

Target folks is something people should be paying attention to do you use a Samsung s24?

COSTIN (57:25.84)
don't use that, no. But I know a lot of security people are very fond of the latest Samsung phones, so obviously, I mean, honestly speaking, this is like what, a million dollar bug, maybe two million dollar, four million dollars bug, zero click remote code execution on the latest Samsung hardware. There is like this, there is this small note at the end that we talked about where

Natalie says that it's unclear if this exploitable, if this condition is exploitable. So I would say that the bug just, it can be triggered, maybe crash the device or crash the particular app, but it's unclear if it can be weaponized. I would assume that, you know, smart people can eventually find ways to weaponize it. And yeah.

If you're using a commodity partner like this, like Samsung, if you, for instance, you were targeted as a company massively on iOS and you replaced all your iPhones with Samsung, then I think that you really should care. And this is a good example that it means nothing if you

just switch from iOS to Android, you're just as vulnerable. Nothing changes. Maybe it's even worse because the logs are much worse on Android.

Ryan Naraine (58:57.72)
a thought on or click on Samsung devices.

JAGS (59:01.077)
Who uses that shit? No, I think it's actually really interesting. It's so funny to see how I was trying to understand where sort of this audio codec bit comes in, right? Like it's how exactly you would trigger this. And Kostin, do you understand exactly how it is that this thing is being triggered? Because it's it's some kind of like audio codec before the message comes in. Is it for the transcription?

COSTIN (59:30.052)
Yeah, simply because they process incoming rich messages in Google messages, right? And the parsers, which is something that we've seen a lot being exploited on iOS devices in the past for zero-click targeting, I think is probably what was driving Natalie and Project Zero to look into this particular.

Kind of things like similar attack vectors to proven zero-click exploits on iOS What what is the equivalent on? Android phones particularly Maybe Samsung the latest generation And yeah, that's the reality is that There's ways to get this kind of code execution zero-click on Android as well

Ryan Naraine (01:00:25.075)
Is there still an issue where you have to wait for your carrier? Cause I don't have a Samsung device. Is there still an issue you have to wait for your carrier to roll up these, these with all their new features and you get this patch three months from now?

COSTIN (01:00:28.602)
Mmm.

COSTIN (01:00:37.052)
If it depends, I think a lot of what phone you have. If you have a Samsung, if it's like from Samsung, then yeah, Samsung will patch it. But in some cases, and I think this was maybe more popular in the US. In Romania, I haven't seen it much when the carrier was selling you a phone that was kind of a rebranded whatever with their name. So it was even called, I don't know, like Carrier Phone A.

carrier phone one, things like that. And then yeah, they need to send the patches because it has their logos and integration for billing and everything. So you can see your billing real time.

Ryan Naraine (01:01:21.426)
Last story, last story before we go, Kostin, your favorite VPN, Mulvad. There's some big news out here. Favorite VPN, Mulvad. Tell the folks what's happening.

COSTIN (01:01:33.308)

Well, this is the kind of VPN news that your government doesn't want you to see, The fact that Mulvad deployed the quantum resistant wire guard tunnels on their desktop products enabled by default, which is I think it's pretty interesting. They were in the actually in the past, they were experimenting a lot with the quantum resistant tunnels and

Obviously, what is the reason to care about quantum resistance at the moment is because people worry that big players, big intelligence agencies are capturing all the traffic on the internet, including like tunnels and storing them indefinitely until a powerful enough quantum computer emerges that allows them to decrypt pretty much all the traffic. I think that Mulva, they've been kind of pioneers in this field.

by caring about quantum resistance. originally implemented the crystal-skybur algorithm, but recently NIST finished their standardization efforts and they put that under a new kind of standard called ML-KEM. But it's pretty much the same again as crystal-skybur. What I think it was interesting in this story is that Jensen Huang, the new messiah, right?

the Nvidia CEO stock keeps climbing and climbing and climbing and he found I think a very nice way of getting people to invest more into Nvidia as opposed to other things by saying that useful quantum computers are like 20 years away so the moment he said that the stock market for all these companies like D-Wave

They all experienced substantial declines like some shares dropping by 40 % simply because Yen-Sung Huang said that these computers are just not practical. They're maybe 20, to maybe even 30 years away. Probably they did. Correct.

Ryan Naraine (01:03:40.757)
The US government has set deadlines for migration to, which is not 20 years away, it's more like closer to 10 years away.

COSTIN (01:03:48.592)
Yeah, and I think by the way in this field, I think we discussed it before that China seems to be experimenting and maybe even some people say they have a lead because some of the fastest quantum computers in the world are in China. Their methodology is a bit different. think a lot of Chinese technology is based on photons and yeah, using using that as a kind of

based technology which is a bit different from what the others in the West have been using. I'm still unsure like to be honest nobody if somebody tells you they know why quantum computers work they're wrong like nobody really knows why quantum computers work we can only guess why they work so when it's it's guessing like this 15 30 years 20 years I think that nobody can really

safe for sure when useful quantum computers will appear.

JAGS (01:04:50.455)

I wish we'd, like, I'm actually wishing we had put more into the story notes and the prep time for this NVIDIA announcement. I mean, the amount of stuff that Jensen Huang talked about, like, that was, it was amazing. Like, genuinely mind-blowing.

Ryan Naraine (01:04:50.527)
So this story.

COSTIN (01:05:06.426)
Yeah. And some new, again, some new products, which are like a desktop level supercomputer for AI purposes, all these things, they look super, super exciting to me.

Ryan Naraine (01:05:07.925)
Messiah.

JAGS (01:05:14.19)
Yeah.

JAGS (01:05:18.445)
We need to monetize the podcast just so that we can start buying some of this hardware, man.

COSTIN (01:05:23.196)
Can we get Nvidia to sponsor us? And I would be so, so curious to see if like in a year or six months, Yansung Huang comes and he announces the Nvidia quantum computer leveraging AI and blockchain.

JAGS (01:05:26.351)
We'll take an Nvidia sponsorship for sure.

JAGS (01:05:39.353)
That would be hilarious.

Ryan Naraine (01:05:47.362)
We can leave it right there. By the way, this is only available on desktop. They're saying they're going to push it on mobile. This is just a press release that there is no real threat yet, right?

COSTIN (01:05:51.196)
Mm. Mm. Mm.

COSTIN (01:05:56.988)
By the way, WireGuard is quite an interesting implementation and there's actually some quantum resistance built into the WireGuard protocol so you can define some kind of pre-shared keys which offer protection against quantum attacks so this is like on top of that like another layer of resistance if you want by doing this quantum key exchange

true NIST approved algorithms. If you ask me, it's good that we are worrying now as opposed to just waiting and then trying to fight it like it's an emergency or the fireweights. So we don't want to wait until the Chinese have the 3000 qubits quantum computer that can break RSA keys, right? We need to start worrying now.

Ryan Naraine (01:06:52.632)
Alright and we'll close I just want to close with a quick mention of the Mark Rogers GoFundMe. Wanted to share some quick thoughts on this.

JAGS (01:07:01.433)
Yeah, so I mean, think a lot of us know and adore C Junkie or Mark Rogers, however you know him as like head of security at Defcon and he's been an amazing contributor to so many different parts of the industry and has made so many friends and actually supported quite a few of us. mean, the amount of, you know, when we got the...

presidential volunteer service awards. mean, Mark was a person that was there side by side getting this award as well for the amount of work that he's put forth just on a volunteer basis to try to support all these different efforts for policy, not just in the US, but with the UK and a bunch of other folks. So Mark is an integral part of this community and a very good friend. And he's had a pretty rough year health-wise, right? Like he's had some open heart surgeries, he's had some stuff.

his eyes and then the latest is a whiplash incident that crushed a portion of his spine and he's, I mean he's an unbelievable fucking trooper for effectively in the process of relearning how to walk, relearning how to brush his teeth and on like he's of course as always CJ is improving in leaps and bounds and really putting the effort into

into doing things well as he always has. But the reality of what our country is is one where I'm glad, I'm incredibly grateful to Katie Vogel and some of the other folks that have really rallied around this and said, you know, we don't need to wait for Mark to get into some horrible medical debt when he's already kicking ass trying to just get back to full function.

And I'm incredibly proud of this industry that has really come together to take care of their own as they always do. Like the amount of one three three seven donations that are in that top is just fucking phenomenal. And I'm just grateful that we can all rally around supporting a pillar of our community that has done a lot for all of us. And this is our moment where we can at least make a meaningful difference in one space and come out and support.

Ryan Naraine (01:09:18.203)
Absolutely get well soon to mark I mean there's no one in this industry that's counter security conference or hang around in incident response circles that hasn't crossed paths with With mark and has benefited from his work. So what are we pulling for you? Hopefully we get you out of that wheelchair speedy recovery and then the last thing Absolutely

COSTIN (01:09:34.926)
the recovery.

JAGS (01:09:38.133)
hopefully get them in the podcast at some point too.

Ryan Naraine (01:09:41.627)
And then the last thing is the passing, not necessarily sudden, but the passing of Amit Yuran, CEO and chairman of Tenable. This happened last week. Amit had been struggling with cancer for quite a while. I've interviewed him over the years. I he's an OG of cybersecurity as well. He's been around forever and ever. I remember him when he was, geez, the precursor to US certainty. So he was there in the early days.

passed from cancer or sympathies to his family, his brothers who we also know in cyber security industry, everyone over at Tenable. You have our, you're in our thoughts. I don't know.

JAGS (01:10:21.453)
to hear that their financial outlooks are still good though.

Ryan Naraine (01:10:25.745)
Yeah, it's pretty much of a bummer that, know, Tenable puts out a press release on the passing of Amit and right buried, not buried, but bluntly right in the middle of it, you're trying to read it and it suddenly says, by the way, our financial outlook is still going to be great. It's like, what the fuck?

JAGS (01:10:42.137)
There has not been a single person who's read that and hasn't commented on the slimy capitalist disgustingness of it all.

Ryan Naraine (01:10:51.74)
Yeah, I was reading it on mobile and I had a pop up, you know, one of those bot pop ups that says, hey, are you interested in buying some tenable products? And I'm like, dude, I'm just trying to read about the passing of your CEO. it's like capitalism at its worst. anyway, rest in peace to Amit. Our thoughts are with his family and friends. I don't do well with bad news.

JAGS (01:10:58.159)
God damn.

JAGS (01:11:12.931)
Yeah, I think while we're on the, since we decided to end on the bad, the bad news side of the podcast, reach out to your friends in LA. It is amazing just how horrific and genuinely widespread and affecting the situation is with, with folks in LA. I actually heard from a good friend today who has had to be evacuated from his home. I hope that, that, you know, that, isn't

You know, that doesn't actually mean that they lose their home because it's just such a horrifying circumstance. look, the videos, it might as well be like if anybody ever watched that like stoner comedy, This is the End, which is supposed to be about the rapture happening in L.A. The videos look like stock footage from that movie. It is genuinely horrifying.

Ryan Naraine (01:12:01.872)
It is, is. Shout out to our buddy Alex Matrosov who also had to bail out from LA. The binary office had to be evacuated out to Santa Monica. Alex is in a hotel room in another city now with his wife trying to piece things together and figure out what the next thing is. yeah, reach out to your LA friends. It's just terrible. It's just impossible to look at and understand that this is happening in real time.

JAGS (01:12:08.142)
nobody

Ryan Naraine (01:12:31.506)
Hi, on that terrible, terrible note, have a great week, everyone. Thank you, gentlemen, for hanging in. It's been a long podcast. I'll catch you again next week.

JAGS (01:12:39.993)
Just remember, start every incident with, you don't happen to have a Nevanti firewall, do you?