So throughout my life. I've had this recurring dream
It starts out with me being in my front yard and coming down the street is a wild bull
It's typically white in color and it's just on a terrace
Running around the neighborhood smashing up cars knocking down trees trampling everything in its path
Nothing can stop it and then it for some reason turns and looks at me and I can tell it's coming for me
I mean, it's so wild. It's like falling down tumbling running into houses and stuff trying to turn to come towards me
So I quickly run into the house slam the door shut lock it and then go to the window to look to see what's going on
But the bull just runs right up to my house hits the front door and just busts through it like it's paper
It's suddenly in my house and it's trying hard to turn corners and navigate through my house to get to me
but it's falling down and smashing into walls and furniture and
I'm frantically trying to find a safe place to go
But every room I go into it just smashes through those doors or windows to get to where I am
I keep going into room after room shutting doors locking it, but it just keeps getting in I
Usually wake up around here heart racing. I'm in a panic and what I often feel after this dream is helplessness
Complete vulnerability. There's no place that feels safe
And it doesn't matter how many locked doors I have or hiding places
I know of that bull always finds me and
Smashes its way to me. I
Tell you this because after listening to today's story
I get that same feeling of feeling afraid and helpless
These are true stories from the dark side of the internet
I
Am Jack reciter this is dark net diaries
Support for this episode comes from Exonius
Complexity is increasing in IT and cyber security
Adapt to the demands of your modern environment with Exonius and say goodbye to manual asset inventory approaches
The Exonius solution provides an always up-to-date inventory
Uncovers gaps and automates action giving you the solid foundation
You need to stay dynamic in the face of complexity
Go to exonius.com slash dark net to learn more and get a demo that's spelled a
x o n i u s
Exonius comm slash dark net
This episode is sponsored by Linode which is now Akamai and this is exciting news for developers
Linode is now part of Akamai connected cloud the massively distributed edge and cloud platform that puts apps and
Experiences closer to the users and keeps threats farther away
Increased performance and speed to market with cloud computing services

You're used to now running on the Akamai connected cloud all the developer friendly tools that have helped you build on Linode for the past
Two decades are still available now that Linode is part of Akamai
In fact, they're expanding their services to offer even more cloud computing resources and tools while providing reliable
Affordable and scalable solutions for businesses of all sizes as part of Akamai's global network
They're also expanding data centers worldwide giving you access to even more resources to help you grow and serve your users
Experience the power of Akamai connected cloud for yourself and see why developers worldwide choose it for their cloud computing needs
learn more at akamai.com or
Linode.com that's spelled a k a m a i
Dot com or Linode is spelled l i n o d e dot com
Okay, y'all have seen this talk at the stick conference earlier this year, right?
I don't speak Spanish so I have to use YouTube to auto translate for me, but hmm
Now that I'm looking at it. There are only a hundred and fifteen views on this video
So no, you absolutely have not seen this talk. Okay, let me find another
Okay, what about this one? This is a talk from hack the box meetup in Santo Domingo in the Caribbean sea
You know what this video only has 500 views so no you did not see this video either
Well, both of these talks are by a guy named Omar Avales
And he's talking about the worst day of his life
It's a chilling story
But since you haven't seen this talk, I really want you to hear it and since it's in Spanish
I'm gonna have to call up Omar to see if he can tell us the story in English
This story start much earlier, you know
Then we even knew that you know something was happening. So this is started May
2022 on Costa Rica
Okay, so this is Omar and he lives in the Dominican Republic, which is an island in the Caribbean sea
Across the Caribbean sea next to Panama is Costa Rica and what Omar saw happening in Costa Rica struck his curiosity
The new president of Costa Rica has declared his country is at war with a ransomware group
Which has been carrying out cyber attacks on the country's government the cyber criminal gang known as Conti has disabled agencies across the government
Since April using ransomware attacks. Whoa, that's kind of dramatic. Isn't it declared war?
Seriously, like you go in to deploy troops and send fighter jets because someone put ransomware on your computers
Does Costa Rica even have fighter jets?
Anyway, because Omar is in part of Latin America. He was watching this story unfold
Let me introduce myself
before I you know, I
Start talking about it the intense
So I used to work in the Dominican Republic National C-Cert

Which is the national cyber security incident response team
Sorry, I had a bad connection with Omar when we were talking. So let me repeat that for you
Omar worked in the C-Cert for the Dominican Republic
C-Cert is an acronym which stands for Cyber Security Incident Response Team and this C-Cert Unit falls under the Department of Defense in the Dominican Republic. So when cyber attacks threaten national security
Omar was there to review it
But what's more is the Dominican Republic C-Cert is part of a community of other incident response teams within Latin America
So when the incident Costa Rica happens they contact us, you know, just to ask for help
What he saw was that 20 different government organizations in Costa Rica were hit with this Conti ransomware
This was a very widespread problem within their government. So it's no wonder they were reaching out for help anywhere
They could many parts of the Costa Rican government came to a halt and they were frantic over there
But this gave Omar the ability to research and understand this Conti ransomware better
You know, it was like a massive malware campaign in Costa Rica
They were talking government organizations through phishing, political vulnerabilities
But they, you know, compromise all the departments separately. Wow, that's really remarkable
See when I hear that 20 departments were hit
I immediately think that there must be some central connection that allowed the malware to spread internally
You know, like if you can get in through the front door now
You can take a tunnel to all the other buildings or something
But no what Omar saw was that each of these 20 departments were infected separately
Some of which were infected through phishing emails and some from malware put right on systems that were connected to the internet
But just because the malware got inside each of these places
It didn't actually turn on until the right time
It was coordinated that when enough systems got infected it would trigger the ransomware to lock all the computers at once and demand payment to unlock them
Now the motive behind putting ransomware on systems like this is typically just to make money
I believe they were asking for 20 million dollars to unlock Costa Rica's systems
So whoever did this seemed to be there only for financial gain
Costa Rica got their systems fixed up and I don't think they paid the ransom
They had backups and restored but Omar saw how this malware operated and worked
And he saw the methods they used to get in and took this new knowledge to scan the Dominican Republic's national computer infrastructure
To see if anything matched what was on Costa Rica systems
After all the malware seemed to be present in Costa Rica's network for a while before it actually executed
So he looked through computer after computer and scanned lots of systems looking for things that matched what he saw in Costa Rica

He didn't find anything actually which seemed like the Conti ransomware gang wasn't targeting the Dominican Republic which was good
But then while looking for malware in the network, he noticed something
Someone had defaced a Dominican Republic government's website
They found a vulnerability on the web server and changed the pictures and text to something else
So he zoomed into this to investigate
We found an impact a piece of malware
Now typically when someone defaces a website
It's a small time hacker being able to show your friends that you changed the text on a government website
Makes you look cool in some hacker circles
But it wasn't this person who defaced the website that put the malware on that computer
See when Omar was investigating the defacement
He checked to see if any malware was left behind and it was just not by this person
One of the places Omar likes to look for malware is in the temp directory
The temp directories used by programs to temporarily hold data
And it's kind of a free space for any app to use to dump data in there if it needs it
So this directory often has open permissions
Anyone can read or write to it
Not many directories are like that on a computer
So that's why Omar looked in the temp directory
And that's where he saw that someone had stuck this malware in there
But the malware the implant was on the system
From 10 to 11 months ago
So someone had exploited this system 10 months ago
Stuck some malware in there and then left quietly
But when someone else came and defaced the site
That's when he discovered that it was there
And just imagine that sinking feeling for a moment
Malware had been here for 10 months and nobody noticed
Your worst fears start racing through your head at this point
Did they steal anything? Did they access stuff? They shouldn't it?
Did they jump around to other computers?
It was a malware that did privileged escalation
So he exploited that window vulnerability that was unknown to the
Windows to the windows people so we may call that a zero day
Okay, this just got worse a zero day means that not even Microsoft knows about this vulnerability
And the reason why it's worse is because whoever left this here must have access to some pretty advanced malware
It's not easy to find a zero day exploit because if it was Microsoft would find it too and put a fix out for it
So it's supposed to be secret
No, specifically this malware's purpose was to escalate privileges
So that means if you get on a system as a low level user, it'll promote you to a user with

administrator rights
So now you can do anything you want on that system
Kind of like if you were to just walk into the front door of a prison and convince the guards that you actually own the prison
And to give you all the keys
Being able to escalate your privileges is a crucial step at getting full control of a computer
And this could be the beginning of a big deal
And just as omar was about to tell someone about this news broke out the dominican republic's agricultural department has suffered a
ransomware attack by the quantum ransomware group
The attack disrupted multiple services by encrypting four physical and eight virtual servers
Compromising most of the information including databases email and applications
Wait quantum ransomware
Gosh a totally different group hit them
It makes me want to make a meme out of all this ransomware news
Enough is enough. I've had it with this mother flipping ransomware on these mother flipping computers
Just when you tune your eyes to be able to see and detect a certain kind of malware
You get blindsided by a totally different kind
And whatever that malware was that omar found on that web server that had nothing to do with this quantum ransomware
They exploited a vulnerability an unfortunate firewall
That allowed them to have a vpn access to the infrastructure
So with the vpn access
They managed to compromise the entire
Organization and then try to run through the organization
Luckily, they detected this quite quickly and called omar in very early
He got in his car and drove down to the data center that was infected
And when he got on the systems there he was able to see the people who were behind the quantum ransomware typing out commands
Infecting more systems. So because he reacted so quickly he was able to stop the spread of it from getting on more machines
And this is a stressful situation. I don't know if you've ever gotten your computer or phone infected
But anytime this happens you have to wonder did you clean your device good enough?
Are they still in there?
And you never actually know you sort of have to cross your fingers and hope the attackers will let you know if they're in there
Still even though he's kicked them out of this one system
It's hard to tell if they just come right back in or what other systems they may have access to
It's like trying to build a dam in the dark with just sticks and rocks
so
That went very public
So on the investigation we found out the attacker
that into the network

via
A phishing attack, but that didn't tell us you know more information. So
We concluded the investigation of the report without any attribution. So we just know that somebody compromised
assistant
No attribution on the final report for the quantum ransomware infection. Okay
The attribution means figuring out who did this and they couldn't figure it out. There just simply wasn't enough clues
It seemed to be fairly common malware with no clear path leading to anyone in particular
All it seemed was that it was financially motivated
They wanted money and that's the whole reason why they did this
And I think there's three main categories for different types of attackers. There's the hacktivist type people
Or hacking into things just for fun or to make a point like those defacing websites
And then there are people who are financially motivated. They're only there to make money
And then there are more sophisticated groups there trying to steal state secrets or something
I mean, they might even have spies on the ground of the place. They're trying to break into
If you know who your adversary is you can combat against that particular threat more effectively
You can prepare better and be more alert
So it's important to understand the landscape of who can and who is and who should and who would be attacking you
When you're dealing with ransomware, you're typically up against someone who just wants money
And if you don't pay it or make it really hard for them, they'll probably just move on to an easier target
So after this attack things settled down. Omar went back to his normal duties
One day, uh, we got a tool to analyze all the the dns queries
that the organization made so we implemented that
Technology all around all government organizations
So we can have a full visibility of what was happening on the government
Okay, so they got a new tool to look at the domains that each organization is reaching out to and each domain
That's connecting into the government's network
Now they took this data and cross-referenced it with known malicious domains in the world and this is called threat intelligence
There are companies out there that try to classify every single ip address and domain name to try to determine if it's malicious or not
So if you see computers on your network contacting known malicious domains
Then you can double click on that and see what's going on while he's scanning the network
I want to take a quick ad break, but stay with us because you're going to want to hear what he found
This episode is brought to you by foronis
So many security incidents are caused by attackers finding and exploiting excessive permissions
All it takes is one exposed folder bucket or api to cause a data breach crisis
The average organization has tens of millions of unique permissions and sharing links
Even if you could visualize your cloud data exposure

It would take an army of admins years to write size privileges with how quickly data is created and shared
It's like painting the golden gate bridge. That's why foronis built least privilege automation
Foronis continuously eliminates data exposure while you sleep by making intelligent decisions about who needs access to data
And who doesn't because foronis knows who can and who does access data
Their automation safely remediates risky permissions and links making your data more secure by the minute
Even when you're not logged in
Foronis is classifying more data revoking permissions enforcing policies and triggering alerts to their ir team to review on your behalf
To see how foronis can reduce risk while removing work from your plate
Head on over to foronis
Dot com slash dark net and start your free trial today. That's foronis spelled
var onis
Dot com slash dark net
Omar was scanning the dominican republic's dns queries to see if anything unusual was going on so
We've covered a c2 server that was you know utilized by the company
Oh, no a computer within the dominican republic government
Was connecting to a command control server otherwise known as a c2 server
That is known to control systems infected by the conty ransomware
This is bad. This indicates that the government is about to get hit
Someone has them in their crosshairs and just needs to pull the trigger
And perhaps they're gonna get hit as hard as costa rica got hit
Whoever was behind that attack on costa rica clearly had a lot of time and resources to make a very deep and wide impact there
crippling their systems and government
But lucky that omar has such a keen eye and is tuned into the threats of his government
So he can detect this early
And so he zoomed into this alert and he saw that yes
In fact a system did get infected and it reached out to the command and control server to download cobalt strike
Cobalt strike is like a full suite of hacker tools
It's equivalent to finding a bad guy in your building and also finding his huge sack of tactical spy tools
But because they spotted this as it was unfolding
They were able to delete those tools and clean that system and start hardening that system
So it doesn't get infected again on top of that with this new found activity on their network
Knowing that they're in the crosshairs of somebody
It was important to start alerting the users in the government agencies
Be on alert
We are seeing some bad weather on the horizon be very cautious of any phishing emails and please please please report anything suspicious to the security team
Thank you. So that's when everybody started sending us sending out emails and emails and emails

We analyze hundreds of emails
There is hundreds of emails
So the weird thing is about these emails that they were reading perfect Spanish
Like they were not English, but perfect Spanish like perfect Spanish
Okay. Well, so they were seeing a lot of phishing attempts
emails posing as someone else trying to get users to click links open zip files or attachments
And in every one of these emails the attackers spoke perfect Spanish
This is really curious since a lot of these ransomware gangs would be coming from
Eastern Europe or Russia
They wouldn't have the ability to speak perfect Spanish on such a large scale with hundreds of phishing emails being written
At that time it was June 2022
We had over five to six hundred emails different emails and all of them
Were different. So we didn't have one single email that was sent
But all of them, you know, share one one thing all the things were about bad interactions or money or payment something related to money
and also all of them had
a backdoor
the attackers were using which was
a
Backdoor known as band duke
band duke
Okay, if I google band duke malware, I immediately get an article saying that this malware
Gives remote access to a computer and it was written by someone named prince Ali who's from lebanon in the middle east
More specifically the band duke malware has been known to be used by a group called dark caracal
Well, that's what the eff named them at least and while we aren't sure exactly who they are
There are quite a bit of clues that lead us to believe that the lebanese government is somehow behind this dark caracal group
Now I want to paint a clear picture for you
Hundreds of phishing emails are flooding into different government agencies in the dominican republic
All of which are trying to get the recipient to open an attachment or click a link
Which will infect them with this band duke malware, which typically seems to be the work of this threat actor group called dark caracal
As omar looked at these emails coming in he noticed something even more scary
They compromised a company. So it was an important target
So what happened here is that the attackers knew that the dominican republic was doing business with a certain company
And they infiltrated that company
Just to pose as people from there in order to trick the victims in the dominican republic government to open attachments
What they did is that they used a user
That was having a conversation with existing administrator

So the existing administrator was waiting for that user to send him an attachment
So in step of the legitimate attachment, the existing administrator received the back door
I mean this seems to be the start of a horror story where it feels like
You're home alone at night and someone is throwing rocks at your window at all your windows at once
Constantly pinging them and you just know at any moment one of those windows is going to break
But there's just no way to secure everything at once
It just takes one user in an agency to get infected
And then the attacker can jump off their machine to infect the whole agency
And for dozens of agencies to be attacked at the same time
is horrifying
On top of that the attackers are scanning web servers looking for vulnerabilities trying to find an exploit to get into the network that way
So it's like endless banging on the doors and you know, they're not going to hold
Where do you even put your attention in a situation like this?
The bull is trying to get in your house and there's nothing you can do to stop it
And we found out, you know, something I was very terrified for us
Over 30
Government organizations were compromised by that campaign like really big organizations
The hacker group dark caracal had successfully made their way into 30 different government agencies
And each came in through a different entry point too
And to see that this was coming to know the bull was headed towards you
But to have no ability to stop it has got to be one of the most terrifying feelings
the feeling of helplessness
despair
vulnerability
Suddenly a huge portion of the dominican republic government's network is now in the control of someone else
Someone you have no idea who they are
But may be related to the lebanese government
Let me tell you, you know, it was not just government organizations
But also critical infrastructure
Holy flip critical infrastructure is things like power plants water treatment facilities or dams
Disrupting or destroying these systems would absolutely bring this country to its knees
Yeah, it was a very complicated moment. We didn't know what to do
Now, of course omar isn't working by himself on this when he says that he did all these things
It was obviously a team effort
Then his team consisted of like seven or eight people
But then every agency in the government has their own it department and some of course are bigger than others
But everyone was working extra hours to help out
But it just makes me wonder, you know
How robust is the dominican republic's cyber security?

I mean, they may not be able to afford the most up-to-date network infrastructure
And they may be running old systems in place
They may not have the funds to employ high quality employees to react to this
But when you're on the internet, it means you're only one click away
For every threat actor in the world
So you absolutely need to secure your government's networks
Just as well as the largest governments in the world
Just because you're a small island doesn't mean you get to skimp on cyber security
You need to be just as good as everyone else
And it feels asymmetric in so many ways
You have to be prepared for the most sophisticated threat actors in the world
And I just wonder how advanced was the cyber security of the dominican republic
But after, you know, they did some things on the system
They now
It downloaded or insta a second malware, which was a coalesce strike implant
Which was communicating to
Conti C2
C2 means command and control server, but I mean what you you're telling me that some advanced adversary who may be in the middle east
Is now starting to install the Conti ransomware on these systems
This is boggling because Conti has been widely attributed to be from russia
So first of all, why are these two groups even allies or working together? Second, holy crap
You now have two sophisticated attack teams working together to attack your entire country national agencies and critical infrastructure
Just when you thought you were in the thick of the storm the storm got worse
It was man
On that moment we wanted to disappear
Then he got alerted of another problem
A big bang overnight stopped working for over a month
So if that bank cannot operate all the people that have the money on that bank, you know
What how they are going to get their money out or how that can affect the the government or the economy
So that was something big and we involved even more people to investigate
The dominican republic was in trouble and omar's job was to help
So one of the first things that I did or I tried to do
Was call the people Costa Rica because that happened to them
And I wanted to know, you know all about the incident
Now this is what I love about omar is his awareness and his social skills
I used to work for a company doing incident response and guess how much cyber security news my boss paid attention to
None guess how many other companies my boss interacted with to understand what threats they were facing
none
The attitude in our company was to put your head down and do your work

Not look around to see what everyone else is doing or meet other people in the field
And I hated that I can't stress this enough
That having allies in this business and going to conferences and meeting people and sharing stories with them
Will help you do your job so much better
So please it managers
Stop thinking you're in some silo and your problems are just yours
Encourage and support your it employees to go to conferences meetups talks and workshops
It will help your business trust me
Omar has gone to conferences
You heard two of his talks at the beginning of this episode even and he's gone to meetups and he's made friends across the sea in Costa Rica
Specifically it was the conference called first where he met them and you can learn more about this at first.org
First is a forum for using response. So
Like all the answer response teams all over the world
Just have a conference once or twice a year
So we all go to the conference and on each other. So if anybody needs help so we know
Who we can call
Well, first is just one conference in the world
There are so many more going on these days. In fact, I think any given week you can find two or three security conferences going on somewhere in the world
So just google cyber security conference near me and see what's coming up near you
And having these connections were very valuable in this situation. I mean it was a force multiplier even
Dominican republic doesn't have the biggest cyber security incident response team in the world
And so knowing who to tap for help creates a battalion of people who can help you in different ways
One thing they did was compare their malware and indicators with other countries in latin america to see who else has seen anything like this
Then he started creating a playbook with help from other nations to start remediating this
Of course, he was also calling up security vendors the people who made the software that was supposed to be securing his network
He'd call up and say things like hey, we pay you to block these attacks and you didn't please help us fix it
And of course the security vendors want to make their tools better
So they wanted like a sample of the malware and what methods they used to get in
And we're working quickly to fix their software
So they would be able to block these attacks from continuing and this was happening on windows machines
They were getting infected even though they were fully patched and updated
So a call to microsoft was important to show them what they were dealing with and to ask
How can you fix this?
They were calling out to other network vendors too because their systems were compromised
And by the way, when you call up one of these companies to try to report a zero day exploit

It's not easy
The first person that you get the first tier support tells you stupid things like okay, sir
Did you try rebooting the system and you're like come on?
Please please please please please connect me to somebody who knows what they're doing over there
And they simply cannot
So you need to like ask for a manager and then the manager doesn't know how to fix it
And they don't want to admit that their software has vulnerabilities in it
So you go back and forth trying to troubleshoot it for days
It's tedious and time consuming
Before they escalate it to the next tier support and eventually you get an engineer or a developer
Who knows this system inside and out and can recognize the problem and replay it and fix it right away
It's just that that person is behind like eight layers of support tiers before you can get to them
Now there's this quote from bruce schneyer that has frustrated me but also educated me on the reality of cyber security
The quote goes like this
You can't defend
You can't protect
The only thing you can do is detect and respond
I get frustrated from that quote because I feel like
We should be able to defend and protect. Why don't we have secure software that can do that?
I mean how many more years and technical advancements do we need before we can
defend our networks
But the sad truth is we may never get there
And so what bruce is saying is we need to be
Assuming we're breached and to work on improving our ability to detect and respond to cyber threats
Somewhere in the middle of the storm omar realized that too
Instead of trying to build those walls up higher and higher to stop people from getting in
He needed to get better at detecting when they did get in
So he started installing more monitoring tools into the network so that he could watch more closely
What was going on in there and this allowed him to understand where cobalt strike was
And spot it and the banduk malware and kanji ransomware and dark caracal and where it was in the network
And how it was moving around giving him a beautiful view into which systems were infected
We found out that the predactor was under system over
Ten months ago. They were in these agencies for ten months
Geez
So when we discovered that
We tried to to get to somebody else that may have more information than us
And we get to our partners
So when we reached out to them and we showed them, you know, all the information that
we have

they
Thought of something that, you know, make me very afraid
So they told us that it was not just that caracal. It was not just county
But also it was russia was also involved
Russia as in the russian government
It was very strange for me why russia would compromise the Dominican Republic in that way
What interest interest they would have here because in the Dominican Republic, we have a lot of russians
Like a lot of russians living here
Uh, what would be their location?
And what that organization told us is that they were trying to experiment with some countries
And something that may do in a big scale. So they could not target some
More mature countries like the united states or united kingdom because they have better defense
So they were trying to do it in this part of the world. So what happened in costa rica?
Even though it's not publicly
Saying that on behalf of any government is just my opinion and what I know
From what happened and for what I learned on the process
What happened in costa rica was part of that and what was happening in the Dominican Republic was part of that
And it was not just costa rica and the Dominican Republic
But also all the countries in the latin american region were involved on on that. So we
As soon as we knew that we started reaching out to those countries
To let them know that this was happening to send them in the process of compromise. So that way
They find out even earlier than us that something
Dangerous was happening in their country. So they were able to
Do things, you know
Before something really bad happened. There's now a third threat actor involved in this attack
Uh
Just before all this happened in the Dominican Republic
There was some crazy drama going on in the conty ransomware gang
So conty we know is based in russia
And they came out publicly in support of russia's invasion of ukraine
Well, I guess someone close to conty did not like this and decided to publicly leak
60 000 messages between the conty group and other people and these leaked messages showed that the russian government
Had been hacking into places that just seemed to be in poor taste, you know, like hacking medical researchers
So it's not a far fetch to think that conty may be working with the russian government
Or that the russian government would be attacking smaller countries
Sort of as a testing ground to practice their hacking skills
But I mean an infiltration at this level
Really can pose as a whole new type of ransomware
Like just hypothetically
Imagine a phone call from putin to the president of the dominican republic where putin could say

something like
Listen, we want you to support our war with ukraine. And if you don't we'll turn your whole country off
Because they can with their hand in so many agencies networks and critical infrastructure
They could just shut down the dominican republic
And that would be a form of ransomware wouldn't it be?
No, this was just a hypothetical. I have no idea if putin has any relations with the dominican republic
At some point does uh, do you contact the president and say hey, we've got a really big deal
It's not just your normal malware, but this is um, this is a geopolitical problem. Yes, we did
So we call a national meeting with there, you know, the big persons support the government
So we inform the president the intelligence
agencies that while we discover
Of course attribution is very hard when it comes to cyber attacks
It's incredibly easy to hide in the shadows on the internet
So even though there are some things that point to this being russia and dark caracal
How confident can you really be?
Especially when you're on the phone briefing the president
Maybe someone else just got a hold of the bandook malware or concy ransomware
Maybe someone wants you to think that it was those threat actors attacking you just to throw you off the scent
Because we've seen threat actors put in fake clues to do just that before for this situation
There were a lot more questions than there were answers
If dark caracal is lebanese based, why would they be working with russia or conty?
Was this financially motivated or politically motivated?
This attribution wasn't exactly clear and neither are the motives
Yeah, so there are no supposed support together
So that things went over our heads over and over we overthink it. So why why why?
Uh, does lebanon and dominican republic have any relations? We do so our
current president
His family is from lebanon
Oh, what hold on how can the president of dominican republic be from lebanon? Let me look this up
Okay, the his grandfather was born in lebanon and moved to the dominican republic in the 1800s
It was not clear to me at least if he's still tied to lebanon in any way shape or form
I mean, I couldn't even find out if he's can speak lebanese, you know
But it seems like only weeks after he was elected as president is when this attack happened
So maybe this has something to do with lebanon sending a message to the president
My mind is spinning here and I don't want to make any wild assumptions
At the very least i'm reminded of how costa rica's president declared war on conty
And now I can see that that's not so far fetched of an idea anymore
At this point or had a very good understanding of this campaign and malware and he even reversed engineered some of the malware
And inspected it for clues and looked at their command and control servers
And had a full map of where the infections were and how they were moving around the network
On top of that vendors started to improve their systems issuing patches and updates and better ways

to detect this
So he got together with all the teams inside the agencies that were infected and explained the remediation process
Step by step
He walked them through how to remove this and stop this from happening again
And he also called the isp to have them block certain domains and he was actively cleaning up the mess
Of course when you go to threat actors not going to go down without a fight
So while they'd block a domain or a command and control server
A new one would just spin up and they had to keep blocking and updating their detection methods
And you know the goal for security isn't always to stop all the threats permanently
But instead just to make it as hard as you can for the bad guys to get in
Because it takes work to spin up new domains
It takes work to pull out a new zero day to infect more systems and it takes work to regain access once you get kicked out
So having this coordinated effort to shut them out
Started to exhaust the attackers resources
And do they really want to put a lot more work and effort into getting back in?
Or just move on to the next target
There's a concept called the pyramid of pain when defending a network
And it's basically the more painful you can make it for the attackers to get in the less likely they'll actually do it
You never will become fully secure, but at least you can make them work for it
So after a massive coordinated effort to clean up the government agencies and a big bank and critical infrastructure
They were able to successfully clear everything off and keep it off
In fact, they seemed to have stopped the conty ransomware attack before it actually triggered ransomware on any systems
It was only staging the ransom, but never actually executed it
Omar also looked to see if any data got exiled traded from the network
But it didn't so it doesn't seem like rush hour dark care calls stole any information out of the government
Did they did they disrupt uh critical infrastructure?
and they they tried to but they
Could not that you know
And the critical infrastructure works and what we call the ot which is operational technology
Oh, yeah to control a dam or a water pump or electrical transformer
It doesn't use like a typical windows computer or something
It's a different system called ot which is operational technology
Which is opposed to it information technology and ot takes a completely different skill set
And sounds like whoever got into these systems didn't quite have the skill set to control ot systems
Which was good that they didn't get disrupted
What a whirlwind story this was, huh
To have a government completely cracked open like that with no way to stop the attackers in my

opinion at least
But then to gain back control of it and lock them out
Omar likes sharing this story with others so that they could be aware that this kind of stuff goes on in the world
And in fact as i'm looking things up here. It seems like venezuela also got targeted with the same group or groups
So in 2022 latin american countries were hit hard with these huge coordinated attack campaigns
That may have been unstoppable due to the sophistication and breadth of the attack
And i wonder if haydie got hit, you know
The president of haydie has been assassinated in the place as a barely functioning government
And it's kind of been taken over by gangs
Would you expect their cyber security posture to be strong or lacking?
I mean if russia infiltrated haydie's networks
Is there anyone there to even notice it and clean it up?
And i just wonder about haydie because they share the same island as the dominican republic
I don't know in some ways. I hate that our world is so vulnerable digitally still that our most critical systems are still susceptible to attack
My knee jerk reaction is to say something like take your systems offline if you can't secure them properly
But that's the opposite of technological progress. So that kind of attitude or strategy just isn't going to fly today
I just feel like when our systems get too complicated
They become insecure and we certainly live in a very complicated network of computers now, don't we?
But the thing is even in my dreams
I still can't find a safe place to hide
A huge thank you to omar aviles for coming on the show and sharing this story with us
The easiest way to find omar to connect with him is by looking him up on linkedin
I'll have a link to his linkedin in the show notes
In this episode we talked about the threat actor dark care call and I actually did a full episode on them a while back
And that's episode 38. It's a really fascinating group. So go check out that episode
Just as a reminder this show is now on a monthly release schedule
So look for new episodes on the first tuesday of every month
I also have a store where you can buy cool shirts to support the show
It's not all branded with dark net diaries logos. They are some there
But there are a ton of shirts that I just know you'll absolutely love the design and want to wear these shirts
So please go visit shop dot dark net diaries dot com and thanks for supporting the show
The show is made by me the bullfighter jack reciter editing helped this episode by the bipedal tristan ledger
Mixing done by proximity sound and our theme music was created by the mysterious breakmaster cylinder who just released a new album
And I'll have a link in the show notes if you want to take a listen

Now even though when I see people rate this show a 10
I always assume it's in binary and they're really giving it a 2
This is dark net diaries
You