# #180 - There's room for everybody in your router (with Giorgio Perticone)

[00:00:00]

Hello and welcome back to the, Security Break podcast, but this time for a very special episode, since we're, doing a joint episode together for, with, G Mark here from the CISO Tradecraft, podcast. I'm so excited to do this. let's say I'm a newcomer to this, podcast industry, let's say.

so the, opportunity is to do something like this. it's, it's very, exciting. And, let me, let me think that, maybe I'm starting to do something interesting, to do something useful, out there. And, yeah, thank you. Thank you, Mark, for accepting, I was going to thank you very much and to everybody out there, [00:01:00] hello, and welcome to another episode of CISO Tradecraft, the podcast that provides you with the information, knowledge, and wisdom to be a more effective cybersecurity leader.

And we're pleased to have our first joint podcast here after 170 episodes. It finally took us some time to get together with somebody. Who wants to go ahead and also reflect cybersecurity and helping out. as you had said, you're on the right track. There's a lot of good information out there that we can get to people.

In fact, there's so much information out there that is difficult to filter what you should care about. What you don't care about, what is true, what is maybe not so true. And so hopefully today we'll cover a number of issues that I think we will find quite fascinating and perhaps give us a model for how we might want to do podcasts going forward.

Yeah, absolutely. And just to, add something to that, it's not only the fact that there's definitely too much information out there. There's also the fact that [00:02:00] even when you, find out just some interesting information, you still need some, elaboration of that information, right?

Because I discovered during this podcast that, depending on the people reading the same news and depending on the background and skill set and the knowledge of that person, you can. came up with a lot of different, consequences and, different thoughts and different, elaborations that you can do from the same piece of information.

This is the reason why I really want to, share this moment, share this, this kind of, study, basically, reading out some news and elaborating on those. I think that you're actually studying those and the fact that I can share those thoughts with some other people, especially with a lot of more, knowledge and different background than mine, can, and will, definitely help me out, but also all the people that are going to listen to this.

Gentle reminder, [00:03:00] this is currently live on YouTube, will be remain available on YouTube, will be also re uploaded on the other various platforms for podcasts, so Spotify, Apple Podcasts or whatever, and also, eventually on the, on all the, platforms of the CISO Tradecraft, podcast.

that said, the plan is, the plan is pretty simple. We collected a bunch of news from the last week, and we're going to introduce them and to talk about them in a few seconds. So let me share my screen here with the first one of those. Here we are. yeah, I'm going to just introduce the article itself.

once again, I've taken something from the Crabs on Security blog, which I personally think it's very usable. if you want, just go in there and check out the other, posts and articles there. [00:04:00] So do your own research, just not, limit yourself with what we are providing.

let's say this specific article from April 29th. it's talking about, yeah, once again, something happening in the U. S. specifically, but I think it's very, relatable with other countries and other companies and situations as well. we're talking about the, Federal Communication Commission or FCC, which basically find the biggest, wireless providers in the US, namely AT& T, Sprint, T Mobile and Verizon for a very specific thing that I, as an European, really remember me of, GDPR because they are finding those, those companies because they are sharing, without, users consent.

geolocation information about their users that, from the biggest wireless providers, I [00:05:00] would expect that's most, if not all of the, US population possibly, with the third party, data aggregator, which are on their own, also reselling those data, technically making anyone, with not really a lot of money being able to purchase those, those information, those data about anyone else, which is a pretty big issue, I will say, right?

We are talking about really geolocation. It's not just about information that sometimes is, could be difficult to make people understand that these, in fact, a threat, to, to themselves. But when it comes to actual physical location, I think it's a really, really understandable.

now I think that's really the core of the article, right? We are talking about, privacy, about data protection. We are talking about what the companies can or cannot do with the data they are collecting as [00:06:00] part of the, their work, because, if you don't know, when you are using a cell phone, you are basically, as part of the service, the antennas that are, providing you the service of, your fork connection can also somewhat geolocate you.

It's not as, precise as, GPS or something, but can still be used by anyone to find out where are you placed at that specific moment. Now, I want to stop there and see what are your first thoughts when you read this article, Mark, what do you think? it shows you a good insight.

I think for everybody to listen, there's a couple different fundamentals going on. You'd mentioned GDPR, and the General Data Protection Regulation for the European Union specifies 99 different requirements. It's good reading if you can't get to sleep at night, it'll help you get to sleep. But one of the things it does provide is to allow the citizen, the person to have some [00:07:00] control over the use of their data.

Now in the United States, we started with a whole bunch of breach notification laws, starting with California Senate bill 1386, a number of years ago. And these had been copied in some form or another by pretty much all of the states, but notice that this is not breach notification. It's just more along the lines of the California Consumer Privacy Act, the CCPA, which was written in 2018.

And we view that as breach notification. the Americanized version of GDPR. As it's takes place, other states have coming out in the United States, unlike the European union has not really built a harmonized program for how to do these things until about two weeks ago, when there's a bill proposed in the U S house that says, Hey, maybe we should actually try to normalize what these things are and have some sort of a national regulation, because think about it, if you're a corporation, And you do business in one state in the United States or one nation over in, EU, okay, you read the rules, you comply, but what if you have [00:08:00] to comply with 27 or 28 or 50 or different more, all of a sudden, that web of complication becomes very difficult.

So on one side, you have regulation and government trying to go ahead and respond to the needs of their citizenry. People say, Hey, I'm tired of this. I want you to fix it. Other times there are lobbyists who say, Hey, you know what, Mr. Politician, how would you like a nice big contribution to your reelection campaign?

Please just go ahead and push this bill through the legislature and we'll be happy. And as the American satirist and humorist Mark Twain wrote years ago, America has the best Congress money can buy. Now, on the other side of that represents the businesses who are given an opportunity to have a lot of information and a lot of other resources.

And quite honestly, one of the imperatives that you have there when you start a business is we take a look at it, and this would be MBA [00:09:00] 101, is what? Is that you're going to go ahead and you've got customers, employees, shareholders, and stakeholders and things like that. And quite honestly, the purpose of a business is going to do what?

Attract and retain customers, but then you're going to optimize your profitability. You do your profitability optimization by either increasing your sales More customers, increasing the price that you charge your existing customers, more margin, or decreasing waste, at which point you become more efficient.

But when you decrease waste, it's not just a matter of saying, Hey, I'm going to get rid of inefficiencies. I might say that. Hey, in doing this manufacturing process, I have all these leftover scraps of wood. I'm a lumber mill and I make boards. What do I do with all this sawdust? It's good for nothing but throwing away.

And then someone says, Hey, if you put some glue in it and some high pressure, you can make press board. And now all of a sudden we can use that for [00:10:00] construction material. And pretty much any house you buy today is not going to be made of solid pieces of lumber, but it's going to be all the sawdust glued together.

They said, Hey, this is waste. We've made it into a product. We've made money. Now let's come and take a look at what we're talking about here. The four major wireless providers, in fact, they are the four wireless providers in the United States, AT& T and Verizon and Sprint and T Mobile, the latter two having merged recently.

Oh, okay. And then there are, yeah. And which is interesting because when you look at, Hey, I got a 4G network and I got a GSM network, how am I going to, and that's the CDMA versus it don't work too well. But, anyway, the thought is what other resellers, smaller companies, you can say, Hey, I have this mobile, they're really all just renting some piece of, this larger company.

The sawdust, if you will, is the customer data. The customer data could [00:11:00] consume things such as name, address. Perhaps national identifier, social security number to get the credit history in there, the record of payments and things such as that. A credit reporting company would like to know that because if I'm going to grant credit to somebody, I want to know if they're paying their bills on time.

So the credit information has some value. I could market, I could sell that and I could make some money off of that. That's some sawdust. What's some more sawdust? how about the call records? Who calls what number? that's getting rather private. And so maybe we get concerned about that.

But what we're finding here and discussing about this particular episode is location information. Now, location information, you said as well, very personal. And you could have multiple phones. Here's an iPhone. Here's a Android phone. And I've got a burner phone over here that I use for places like DEF CON and other fun places where it doesn't get turned on very often.

It gets turned on, I use it, so they're tracking that [00:12:00] burner phone, they must think I live in Las Vegas. The point is what? Is that we create a tremendous amount of information about ourselves. Anytime we're interacting with a system or a network, just from your laptop or your PC, your IP address, although it's given to you, it's assigned, because most IP addresses are going to be ephemeral, the IP address that you have to your residence may be locked in by your ISP.

So if I know that IP address, I could probably figure out where you live. If I know, if someone says, Oh, I'm 192. 168. 1. 1. No, I'm sorry. That's your local address. And it reminds me of a meme where they say, what's your address? it's 104. No, what's your local address? Oh, 127. 0. 0. 1. No, what's your physical address?

One, one colon, 22, the Mac address, and of course, Mac address only goes layer two. [00:13:00] It only is gonna go one step. And so typically, you're not gonna have the MAC address of your device talking to the ISP, unless you're going ahead and you are duplicating that on your router. You can say, go ahead and mirror that, but by and large.

That information is protected, but what's not protected then necessarily is a content. Prior to Ed Snowden and the revelations that there is a lot of information gathering of unencrypted traffic, most people do it HTTP and most websites offered HTTP. And we're good with that. We went to DEF CON years ago, a friend of mine named Riverside, that's his handle, came up with something called the wall of sheep and the wall of sheep was, they monitored the wifi network.

At any time somebody logged in with an ID and a password and an unencrypted link, it would say, here's where you went, Facebook, here's your full email address. And here's the first few characters of your password with asterisks toward the end. And the wall of sheep would just scroll [00:14:00] like crazy. Now this is 18, 20 years ago.

15 years ago. now it got to the point where everybody's HTTPS and like, all right, Hey, there's 30, 000 people here. Bink. All right. Another one. So what are we seeing? We have been able to protect the content of our information from sniffing, from snooping, from et cetera, by encapsulating it into a security protocol, HTTPS.

But the location information, although I could send you a message saying, Hey, Google Maps, HTTPS. But where I'm located has to be determined by the cellular company. And that triangulation is going to be potentially because you've got cell towers and your phone's going to pick the strongest signal usually.

And as you're traveling and moving, it's going to jump from tower to tower. You have to track that. You need to be able to keep that communications going. Nobody wants to have to hang up their cell phone and redial every half a kilometer as you go along, The Autostrada or something like that, because it's just not working.

And [00:15:00] as a result, that information is required. It's in the logs. if it's in the logs, it's available. And therefore it appears that this whole issue was these companies are collecting a tremendous amount of location data, but since nobody had specifically said, don't do it. Some smart MBA said, let's go make us some money on this.

And they were doing it. However, it turned out that after the rules came out to say that. You're not allowed to do it. They kept going. FCC will typically issue a warning, Federal Communications Commission that's in our, of the United States government. And if you go, Oh my goodness, we were so sorry. We will stop it immediately.

And you stop it immediately and you fix it. They're like, But in this particular case, if you take a look at the article, you find out that AT& T and Verizon took over 320 days, it's at the bottom of the article, T Mobile, 275 days and Sprint for another 386 days. Yeah, we're number one. [00:16:00] Now, what happens is that we look at this as this is the one of many examples of when organizations are going to face a crisis.

Issues with regard to regulation. Here's the question you have as a business owner. How much is the fine? How much money are you making? And if you look at the paragraph above the one you've highlighted, it said, still these fines represent a tiny fraction of each company carrier's annual revenues. Now, sometimes you get to a jury trial in the United States and most places ask for trial by jury.

That's.

I don't know about you, but when you look at the people that are probably, out there, how many of those do you think are your technical peers, your intellectual peers, your ethical peers, but they're just crap, six or 12 people and say, here you go, we're going to explain a highly technical case and try to convince you that you should give billions, probably [00:17:00] not billions, but millions of dollars to the plaintiff because they were so badly injured and oh, by the way, we, the attorneys get 40% plus expenses.

It's not a bad deal as you . Yeah. I really think that, that's really the difference between the, current, regulations in Europe, versus, what the you have in the us. The fact that I think we are a little, just a little. more aggressive in the fees regarding those, kind of, data breaches, involving, user personal data.

I think, I'm not an expert, but I think the last time I read about it was up to 4 percent of the, annual, revenue. Mobile turnover is the word, which is in the United States. We would say gross revenue. And then some of these proposed fines are 10%. And I'm saying like, wait a minute, time out, let's get this right.

What if I do one, one hundredth of my business in the EU [00:18:00] or only of all the revenue I collected, This much as a person and you want all this? It's no, you can't balance your own federal budgets because you're spending too much on, the wrong programs or whatever. Don't come looking to some company that has run a fashion effectively and lean in a few years and say, we're going to go take your money because we can't figure out how to make it legitimately ourselves.

So that's the American view. It's come on. Give me a break. I can see if you said 4 percent of the profits you made in our nation. All right. That's a, pretty good slap. But do you say 4 percent of the entire galactic income that you have earned throughout all the planetary systems?

Yeah, right, now at one, but you can see the, precedence there. So there are some folks who say There's no probably correct way to do it. There are just, extremes that, that are not good, even in my opinion, still, it's, interesting to see how, especially a global company, which is affected, as you said before, by multiple regulations from different countries.

The fact [00:19:00] that, you as a, company owner, you have to consider all of those. Maybe. a regulation from this country is not, let's say that important because the fee potential is not that high, but in another country, it could be a little less, let's say, interesting to, to consider, when, it comes to, such, kind of activities.

And I want just to compare very quickly the kind of fee that, you know, and the kind of money the company is doing by selling those data. And. here in the, article, it's also, mentioned that, as an experiment, they tried to, challenge, let's say a hacker, basically just, consulted to find out, geolocation about a specific person.

And, they just went out to one of those data aggregator and, tried to, to try and actually did, buy the information directly from, there for [00:20:00] just, 300, which I think, it's not that, it's not that high considering what you're really buying, That's why I got my pocket right now, but I could, I'm sure I could get it together, but excellent point.

But think about the government saying, so sorry to interrupt, but you're on the right track here. So if you said, okay, we find Sprint and T Mobile 12 million, 80 million, 47. If you want to say what is reasonable, What I would think is that if I'm the regulator, I'm going to go to one of these companies and say, how much money did you make selling this piece of sawdust?

You sold this information. Now, if you sold this information for 1 million and you incurred a 57 million fine, that's steep. But if they said you sold it for one and we're going to fine you one, that just makes it even. So typically they'll do what they call treble damages. Okay. You sold it for one, we're going to fine you three.

You're not going to disable your cut, but you're probably not going to do [00:21:00] that again. That's not going to help you make your bonus this year. If you, every time that you collect one, you cost you three, that doesn't scale, but that's enough in a way to dissuade someone now, multiple offenders. Same thing.

You go ahead and, you break the law first time. Okay. There's a fine second, third, fourth, and go on like that. But what you also see is a dynamics of corporations and governments. So let me take a similarity. It's not communications companies, but transportation. Lyft and Uber are two major ride share companies here in the United States.

And the city of Minneapolis city council said, we're going to pass a regulation. We need to look out for these Uber drivers and these Lyft drivers. So you have to pay them this much as a wage and this much, and. So they figured, Hey, wow, this is be great. All these people are making a living wage.

They'll be happy. They'll spend, you know what both companies did. We're out of here. Bye. We can't make money. We have no obligation to lose money in your city. [00:22:00] And if you in a corporate environment are faced with a regulatory environment, and the regulators have never even managed a lemonade stand when they were eight years old, let alone try to manage a profit and loss in a competitive environment.

They're just writing regulations. Hey, you want to write a regulation like that? You've got to be an experienced CEO, retire as a CEO, then go work for the government and write some regs. You'll think about it differently. In this particular case, the companies voted with their feet. Imagine if you say, Hey, Google, we want to fine you a hundred billion euros.

And they go, fine, we'll shut down Google in Europe. It's forbidden. You're not allowed to do it. In fact, when GDPR first came out, I had several clients that came to me and said, how do I do a geolocation IP block? I am so afraid of these crazy Europeans trying to take all my hard earned money. I don't want a European customer.

They're not enough of my business to matter. I'd rather lose that 1 percent than risk this huge fine. And so there was actually a company saying, we just [00:23:00] don't want to do business with Europe anymore. not necessarily a direction that your regulators want to go. Not only that, We we actually had, a lot of companies that completely, shut down because, their entire business was not really, sustainable anymore, if they had to, to comply with GDPR and similar regulations in Europe.

So when it came out for the first time, it really affected. heavily on a lot of different corporate environments, definitely. All right. let's see, we've got some more articles we want to talk about. Let's make sure we get to them. Absolutely. this was very interesting, especially because I really want to, provide.

different views, security is not only about hacking stuff. It's also about, compliance regulations, and even if that's not maybe your job or what you want to do as a job, [00:24:00] still, it's very important, I think that you are aware of such kind of, regulation that, that are there.

And also maybe just as a citizen, you want to be aware of the fact that you have some kind of, protections regarding your personal data that companies are correcting from yourself. Yeah. that said, we changed completely topic with the, with the next news. This time we are switching, to something that we already discussed in previous episodes of the Security Break podcast, especially, re relating to back bounties.

So when we talk about bug bounties, those are basically programs. run by companies which are allowing in, with some limits, people from outside the company. So no someone where you are hiring to do but just, random researchers out there that wants to spend their time like this, to try and, hack into your [00:25:00] products, services in order to find vulnerabilities.

And if you provide, the information relating to those vulnerabilities, the, company can also, give you some kind of, bonuses regarding money, for, the, for your work that you did. And the news here is talking especially about, about Google, who, just recently raised, by, basically a lot, their, their prices for vulnerabilities regarding, especially Android apps and those Google Android apps, specifically, we are talking about 10 times the prices that the way they were offering before.

So from 30, 000 to 300, 000, and this is. I will say a very big jump into the money. Someone could say that this is still not, comparable to a third party, say organizations that are asking for the same kind of [00:26:00] information regarding, Android vulnerabilities. But still, the fact that we see legitimate companies rising their prices, I think it's a, very good, indication.

And just to be, 100 percent clear here, they are also adding some bonuses if you, as a researcher, provide not only information about the vulnerability itself, like the existence of the vulnerability, but also if you can provide information about how to fix the vulnerability, let's say, a demonstration of how the vulnerability works and you, how you can exploit that, and possibly a way to remediate the vulnerabilities, right?

So maybe you have to fix this library or whatever, or you, you want to upgrade. some parts of the, software and application and so on and so forth. I think this is also a very important. let's say, input to give out to those researchers. Because once again, I really think you as a, pen tester, red teamer, or, [00:27:00] in that kind of, basically a job role, you want to not only find vulnerabilities, let's say, think about, think an attacker, but also, try to expand your, knowledge and your, professionality, in, how to defend from the things that you, that you find out.

I think that's a very, important, let's say, incentive. regarding how, researchers should do their work, right? you don't want only to simulate the attacker, but also actually help the, company itself. Now, what's your side? So a couple of thoughts on this article. First of all, it says, hey, if you can find a bug, you can find a bug going against what we would call a black box, which means I don't know what's inside it, but I found out that if I could do this type of input, I get that type of output.

Okay, great. I've got, I've found a bug. All right, I could reproduce that bug. I can give you a proof of concept. How in the [00:28:00] world am I going to show you how to fix it unless I've stolen all your source code and re engineered your source code? At that point, if somebody gives me a fix, I'm calling the FBI.

It's hey, it's a lot bigger than that. Secondly, if you scroll down a little bit to the, just before the second, or actually the last sentence in this article, keep going. All right, stop right there for a minute. Now look at the chart. And you see the chart, we got everything up to 300, 000 for code execution.

And if you scroll over to the right a little bit, you'll find out that attacker on the same network for other Vaughns that are not data theft, they're not code execution, 2, 400. It's a little bit out of the screen right now. You have to slide if your monitor lets you do that. Look at the last sentence.

More importantly, you received over 40 valid security bug reports nearing 100, 000 in rewards paid to security researchers. Do the basic math, kids. What's 100 grand divided by 40? 2, 500. What's the lowest possible payout? 2, [00:29:00] 400. Guess what? This is like a lottery ticket. Oh, yeah, you could win 10 million. You know what the odds are?

You're going to lose your money. You know what your second best odds are? You're going to get a free ticket. All right. So here's where I think life gets interesting. I'm going to put a little link here in the chat. If you can go ahead and pull that page up on your computer, this is called Zerodium and Zerodium.

If you open up that link and scroll down a little bit, they have what looks like a periodic table of the elements and There we go. And scroll down a little bit further. Keep going. And where's that picture? There it is. And so this is a little bit hard to see, but you can look at it yourself. xerodium.

com slant program dot html. And what this does is each of these different rows represents a different bounty. Up to a million dollars at the top for a Windows remote code execution with zero click up to 500, 250, 210. [00:30:00] And what happens is the Zerodium access sort of a third party negotiator and I'm pitching them one thing.

I'm just using them as an example, but you mentioned about the market and that's a very good point. And so if I as a security researcher, it used to be before this became legitimized. If you found a bug with some company and you called them up and said, there's a problem, they would say, we're calling the cops.

Your evil hacker says, no, I'm a security researcher. I'm working on a program. We found a problem. Now we're going to call the cops. And so what happened was there's no incentive to report. And as a result, bugs went for a long way. There's been finally some understanding that they'll go ahead and say, let's carve out some exemptions in the law for somebody who's doing legitimate security research.

Now you've got to be careful because you can misuse that. If we take a look at the case of Uber, where their chief information security officer ended up facing Significant penalties, and I'm not going to get into the details. You can read up on them if you're not familiar with the case, but essentially somebody broke into their system, stole information.

He said, Hey, let's reclassify. This is the bug bounty program. And then you found the bug and we [00:31:00] paid off the ransomware, but that was actually a bug bounty. And, yep, we're good. And we don't have to report a breach. That's how you go to follow the rules. When I take a look at all this and we put it together, what do we find out?

The buyers. If you find a legitimate exploit, you can A, exploit it yourself, assuming that you're not going to be doing any, you don't care about the consequences, or you might be operating in a country out of the jurisdiction of law enforcement that cares about it, at which point off you go. You could sell it to the company itself if they have a bug bounty program, and that's what's significant here, is they're saying, hey, we will offer more.

And if you take a look at some of the bug bounty programs that are out there, for example, Apple has A bug bounty that could exceed a million. Microsoft up to about 250, 000. Amazon has their own, Intel, Facebook. Some of them just give you an attaboy and some people only wanted an attaboy. It used to be in Microsoft.

You look at a patch and you used to go ahead and you see this latest thing that comes in here with this particular, Microsoft release. And it [00:32:00] says special note to purple unicorn and all the handles and things like that of people who found it. That's cool. Use it yourself, take it to the vendor and maybe they'll give you bug bounty, maybe they'll just give you an added weight, but they're not going to call the cops anymore.

Third one is to go ahead to something like a Zerodium and a third party says, Hey, we've already pre negotiated stuff. Yeah, we'll take a percentage. That's how we make our money. We've, we'll work it out for you. So you give us your best case, we'll clean it up and we'll see if we can't sell it for more.

We'll take a percentage. I don't know what it is. I don't know their business model and you go get what's left. Okay, fine. Then you could go on to say, who's left? there's the military and there's the intelligence agencies. And I can say, I happen to one particular country over another that's in a current conflict, or if it's not a nation state, it's one particular party over another, maybe they'll pay for it.

They pay pretty well. Organized crime may pay pretty well. And what you'll find out then is there are the dark web. [00:33:00] purchases of that. And we've seen bounties come out as a result of the Russian Ukraine conflict, where certain targeted things where they just can't get in, but they know that these officials from the other nation were using particular devices.

They say, Hey, we will up it. We will outbid anybody else. If you can give me a zero click remote code execution on a Whatever the platform is. So that tells you a little bit about what the targeting requirements are for foreign intelligence services when they start bidding up the prices of something and you're onto something, but not so much that your exploit is better than somebody else's, there just happens to be a security requirement for it.

So how do we interpret all that and come up with something that's actionable? If you're a security. researcher. You can make some pretty good money and doing this. I work with a fellow SANS instructor. I won't mention his name because he, mentions this to other people, but it's not my business to say who he is, but he's really, smart.

He's one of the. [00:34:00] Senior folks at SANS, author of 700 series courses, which is as high as they go. And his hobby is not fixing a car or playing video games. So it's finding exploits, finding bugs and reporting them. And he makes good six figures on a sideline. if you're going to have a hobby, all things being equal, and if it's going to pay enough to buy a new house, every couple of years, why not?

that's a great way to do it. Plus you're improving. The ecosystem, because he is one of the quote unquote good guys, and he's not going to be selling it over to the dark side. So ultimately what we find then is there is some accountability going on. The manufacturers say, Hey, we could face a significant fine.

If we don't patch this thing, there could be a significant exploit and there'd be lawsuits by our customers, by holders of data, by government entities. So let's go ahead. And again, economic decision is your MBA is at work. I'd rather pay. 200, 000. To get this thing [00:35:00] fixed, then pay 20 million in fines or breaches or bad publicity on the other end.

So ultimately it's not, they're giving you money because they like to give you money. they're giving you money because they believe that this is going to go ahead and save them money in the long run. And therefore they're going to a low ball your bid, most likely. Because it saves the money. And that's where a third party might be able to say, yeah, we, could probably, this is important, but the second thing is, that if it really doesn't affect their bottom line, if it's changing happy to glad you found a spelling error on their app.

Nobody cares. You're not gonna get paid for that. Yeah, it does. It has to be at least, somewhat important so that, it is actually affecting their data, their systems and their users, right? Because we are talking about, the Android, operating system. And so it's going to be, their customers, devices that are actually affected.[00:36:00]

now I think this is a very important topic that we discussed multiple times, but still it's very, very helpful and very interesting to, take this kind of news because, anyone can do this potentially, right? Anyone with the, of course, right skills and everything can think, Oh, I'm going to do as a hobby, as my, job or whatever.

do some bug bounty, but the impact of each person doing that, And the impact of the decision to, what you said before to who I'm going to sell this kind of information. Once I find out it, it's going to have a very, big impact on a lot of people all around the world, potentially, right?

So the thing for me, once again, my personal opinion, a kid who learned how to find out about basic vulnerabilities that potentially can, I don't know, be changed, chained with the other [00:37:00] vulnerabilities and eventually. Exfiltrate that and so on and so forth. The thing that they just want easy money and find out the, the, the guy who is going to, provide more money for it.

Of course, it's an easy choice, but if you are not aware of all the consequences of your decision in that case. it can definitely, and it should change your mind on, who you're going to sell that information to. So I think this is worth to, be repeated, a lot of times. And I thank you very much, very much, Mark, for, your, let's say summary of this market, because it's, a market on itself.

And as we say, as we said, there's a lot of money at stake, with a lot of different also actors are involved. Bad actors, good actors, legit actors and, less legit ones, of course. so it's very, an interesting one. [00:38:00] Let's say that, of course this is something, what we're, the news itself, it's limited to those Android application, owned by Google.

So I am, I'm not really aware of if there's anything else regarding the operating system itself or third party application on the Android, probably that's going to be related only to the, applications, developers. themselves. you want also, if you want to do this, you want to be aware of what you're really targeting, right?

There is a scope, there is a scope, whatever if you are doing this as a, freelancer researcher, or if you're actually hired by a company, when you're trying to simulate an attack, you also want to understand whether in order to make that money, understand when, whether what you are really, replicating it's expected and it's allowed by the company itself.

Because if you're [00:39:00] going to go to, Google and say, Oh, I actually find a vulnerability in the, another third party application that is not even owned by Google. you're doing something a little different. Maybe you're providing Google with information that you should not.

Provide two. so it's very complex, right? It's not something that of course we can discuss entirely in just, our limited time, but I really encourage everyone to do, your own research if you are, considering this, kind of work. Yeah. And possibly even consider getting some legal counsel.

We now have enough attorneys that understand what some of the implications are. And I'm not saying you need a lawyer up because you're, you found something that's of value to the ecosystem. but I would certainly support your Conclusion to say, think carefully to whom you're going to sell it. The highest bidder, isn't necessarily the best bidder, at least in terms of the whole world ecosystem and maybe even for your own and your family's [00:40:00] health and safety too, because you might find out that all of a sudden you've got yourself involved in something you really didn't expect to.

But for the most part, if you go ahead and you go through a bug bounty program, particularly directly with the vendor, you're not going to see some sort of, Dark sedan with the smoked out windows parked outside of your house, waiting for your kids to go to school in the morning. So just leave it at that.

Absolutely. so once again, one, very interesting news here. very interesting topic. I think, it's true what you said before, we still have a huge gap between, third parties and the actual, the big tech companies out there in, in what they are offering as, and, as awards and prizes, but still, I personally think that a little rise, it's going the right direction, let's say.

hopefully it can be, get better, in the following years. That said, we have a third and final news for today. Unfortunately, final [00:41:00] one, still we have limited time and hopefully we can do this again at some point. if if you think it's a good idea, let us know in the comments, or, write to me or to Mark, provide message, so that, any feedback will be appreciated also to, to improve this.

And, just before we continue. If you're liking this, please consider subscribing to both of the channels, because that's, that's really helpful for us, and, I'll be really thankful. That said, final news for today, and I like to reiterate on the fact that the final news I select, gives the name to the epset.

it's, let's say, the, most important one in my opinion, just because it's, let's say, a tricky one. in regards to the consequences and the thoughts that maybe you, you didn't think about before reading this kind of news, even though it can be [00:42:00] straightforward after you read it, right?

So the thing is, this news, is taken from a research. I think I forgot what is the company doing the research. it's, Yeah, I will find out very soon. Trend Micro had mentioned about, they were referenced in here. And yeah, Trend Micro is here. anyway, I, always say, do not limit, to what you, we, we are saying.

I will write down the articles in the description. So do your own research. Let's say the thing is that these, this research by, Trend Micro is basically evidencing how some, Edge devices, how they call it right now. So basically, most of the time, routers or VPN concentrators, and those devices that are basically exposed, at least, a part of it is exposed to the internet.

And, which are most commonly used to create the botnets, basically, [00:43:00] Army of device, of compromised devices used for, vast, amount of, different kinds of attacks, DDoS, or just spam to sell some, not so legit products and so on and so forth, are very commonly compromised by different kinds of actors.

Also at the same time. Now I want to, slow down and reiterate on this thing right here, because that's really the core of the news. Even though the news is the article is pretty long and encourage you to read through, it all, I think this is the, topic that I want to focus on, right?

The thing that when you know, you as, once again a person, so your. Home Network, or you as a corporate in a company with, your huge network of thousands or even more, devices, each one of those can be compromised, right? And, can still be compromised right now. And in the meantime, [00:44:00] a second group of actors, maybe with a totally different objective, right?

We can have, cyber criminals that are, let's say driven by just, money, And monetization. And you can have some maybe state sponsored doctors, which I want to do maybe, to hide their tracks when doing, some, let's say spycraft or something like that. Espionage, let's say, the thing that they can use the same devices to run their operations.

And this is actually help helping both the. Different actors, right? Because the thing that you see different kind of activities with different kind of objectives, it makes even more difficult to attribute and to find out who is really behind the kind of attack. And, very interesting thing is that.

it's, once again, it's specified in the article, but I want to highlight this. the fact that the first actor compromised a router, for example, [00:45:00] right? And it's installing some malware, right? Let's remember, everyone, that malware is just another kind of code. It's just another kind of software.

And even malware can be vulnerable, right? And the thing is that they are basically, extending the attack, surface of that And, at least in one case, it's, it was the malware itself that was exploited to, get access to the second actor. So it's a, a chain of, of events that it just, gets worse basically.

and once again, I want to hear your thoughts about this, this factor right here, because I don't think everyone is really considering this kind of, this kind of thing, when you fix a device, Maybe you kicked out some attackers and maybe someone else is [00:46:00] still in there, with a different backdoor and a different malware, right?

Yeah. And if we think of a virology analogy where you go ahead, for example, you go to the doctor, you say, I have some medical condition and he gives you perhaps something to treat that. they say, Feed a cold, starve a fever. The idea is, that it's okay if you get a cold because you'll recover from that, but the flu you might not recover from.

And so as a result, you say, all right, fine. Maybe you've got help get rid of this, but we're going to weaken your system and come over here. Let's look at a little bit of background and history about some of these things. So back in 2016, we might remember the Mirai botnet. The Mirai botnet went after things that are running on ARC processors, mostly internet of things.

More precisely, things like cameras and the like, and that was able to create a gigantic distributed denial of service attack that took out even an internet, register, [00:47:00] domain registration provider. Now, what was interesting is that when we figured out, or, whomever figured out who are the creators of it?

A couple of guys, 20 and 21 years old, Padishah and Josiah wife. And what they did is they created Protraff Solutions, a company offering mitigations. to DDoS attacks. We basically are racketeering is what it's called, where you create a problem and then you charge someone to fix the problem.

it got people thinking, Hey, this is, this works and off it goes. And so in a situation like that, you go, apparently somebody could get into something and it could spread out and it could be. Pretty massive. Now, let's go ahead a couple more years and look at 2018 when we found a situation where there were a number of routers and systems that were hacked and from, a company called micro teak.

And the gray hat hackers, we'll call it someone like, not quite all the way to the white I like, but Gray hat's a fun place to be. said, Hey, you know what? I found a whole bunch of vulnerabilities. [00:48:00] There's a hundred thousand systems out there. So Alexa went ahead and. Patch them. How did he patch them?

By breaking into them and then slamming the door behind him. So basically nobody else can break into this thing, including me. out of a hundred thousand people, I think maybe 50 people expressed their gratitude. A whole lot less than the lepers in the Bible where you got one out of ten. Here you're like 50 out of a hundred thousand.

So don't expect people to appreciate you doing favors like that. But apparently what he had done, he just added firewall rules that blocked So now let's go ahead and with that from someone who says, I'm going to exploit this thing and oh, by the way, form a business around it and charge money for it till you get arrested for racketeering.

And on the other end, I found a vulnerability and the company's not fixing it. So I just went ahead and did a vigilante and I fixed it and I drove down the risk. Now what's left? Now we have situations where whether it's a home system Or a corporate system is that these are going to be desirable for a couple of reasons.

One is you had mentioned things such as a [00:49:00] botnet, but botnets pretty much all you need is bandwidth. The bots themselves aren't doing a lot of thinking per se. And that was one of the things that made Mirai work is all these little machines. These little chips had a stripped down Linux variant, but it had a full TCP IP stack at which point.

You're in business, but it could also be used for intelligence gathering, sniffing the traffic that's coming through, keeping track of that information, as well as being able to provide a launch point. Now let's think about it from a suggestion of cyber. So I've been accepted into a talk in. October at a conference called COSAC, C O S A C dot net.

And at COSAC, this will be my third year talking about cyber war as it pertains to the Russia Ukraine conflict. And this particular time would cause me to want to write another talk on what I called network warfare, the end of civilization as we know it, is the, now the attacks, the intrusions are not going after military targets.

They're not kinetic going ahead [00:50:00] and trying to blow up a tank. Okay. That's a legitimate weapon in a. But now they're going after civilian infrastructure. And the thought is this, is that it doesn't take a full blown national war to create a low level of conflict. In fact, cyber is great because it's usually below the level of conflict that would represent all out hostilities.

And it provides some bit of plausible deniability, if you will, to the nation state that's doing it. So now, if you think about that and you say, think of the adversaries of whatever your nation is, whether it's Italy, whether it's EU, the United States or whomever, and there's, are going to be nation states or non government organizations who will have adversarial purposes.

And they say, Hey, if we can get into your water supply, if we can get into your electrical supply, your air traffic control, the banking system, look at the United States has described 16 countries. critical infrastructures, and different nations, different places have different counts. [00:51:00] what a great way to pre position for an attack.

You could go ahead and go after some portion of the civilian population. So Clausewitz, who is the primary military theoretician for the West as compared to Sun Tzu for the East, his, in his book Von Kriege and War talked about the trinity of war, where you have the military, the government, and the will of the people.

And you find out if you can win on any one of these three, you win. If you defeat the military on the battlefield, you win. If you can send in the CIA and overthrow the government, you win. If you could go ahead, for example, North Vietnam in the 1970s and convince the people that they don't want to be in a war, you win.

Even though you couldn't win on one or two. So all three of those represent valid targets, if you will, from the perspective of warfare. the world's not seeming to get a friendlier place these days. We're seeing a lot more conflicts breaking out in the last few years. I don't think that's going to be the end of it.

And so we need to ask ourselves as cybersecurity professionals, [00:52:00] as CISOs, if we're in charge of platform, or even just people who work in this industry, what are our vulnerabilities? Could our systems be a value to an opponent? Now it may not be because your information is of value. Because they don't care, but we think about, for example, the geolocation information that came from that first article, we're talking about the company.

What if I could track the executives? What if I could track government officials? What if I could track generals? What if I could track all of these fill in the blank of potential military targets? Or just even knowing what they're up to should tell you that, all these people came together in this building.

Or they all came to this area, then all the cell phones went dark, and then two hours later they came back on again. something's happening. Second one is with regard to your contribution to the fabric of the infrastructure of your society. If you're a critical infrastructure, your water processor, and somebody can go ahead and remotely come in there and start adding extra chlorine or change or the bromine or whatever you're using for sanitation or changing that chemical mix or allowing sewage to back up into the drinking water, you can [00:53:00] make a real mess.

And although that's not technically a legitimate military target, you The people doing it might technically not be military professionals. And so as a result, they don't feel any need to adhere to any particular code of ethics. So we have to operate from a different perspective. And the one is this is to say, let's assume that.

Our systems are already compromised. Now, if you really believe that you would run away from podcasts right now, and you would log in and you would start doing threat hunting, but to a large extent, different threat actors have different approaches as we look at. And this is just a generalization, but actors from people's Republic of China tend to be low and slow, like a ninja in a way, those that are classified with the.

Coding Bear, often come from the Russian Federation. They tend to be a little bit more break and grab and smash and grab a little bit faster. They get their stuff. They're not gonna get caught anyway. So on that, get as much as you can instead of risk getting [00:54:00] caught while you're still tiptoeing around in the dark and different other groups, different advanced persistent threats or APTs, as we call them, will have their own.

Modus Operandi, their own MO. if we know what their tactics and techniques are, and we know who our threat actors are based upon a threat analysis, I can go take a MITRE attack framework, put them all in there and see where I've got these three threat actors, Oh, by the way, they all use the same thing.

So maybe I need to defend against that. That's where they're coming in. I don't have to go ahead and look at absolutely everything in my system, but that's probably a good place to start. How do you know if somebody is in your system? you have to go look for it. one of the things that some organizations do, if you're an extreme, you're going to rip and replace every so often.

wait a minute. There's nothing wrong with that system. You know what? I'm going to get a new one anyway. And so from a extremely high, important system, for example, I get a new cell phone [00:55:00] about once every four or five years, like clockwork. I'm not a big, Consumer. I don't wear them. In fact, my old cell phone is sitting over there.

It's a Google Pixel 3a. This is a Google Pixel 7a. And eventually I'll probably be upgrading to the Google Pixel 11 when it comes out because I get a nice outer box. It doesn't break and I don't take it swimming. And as a result, they last a long time. Why do I mention that? Because in this particular case, they have a very cost effective solution.

Okay, my amortized, my cost of my cell phone is just a very small amount on any given day. But if I were really, concerned about my cell phone being infected, having malware in it, being tracked, the, people being able to know that this particular EMEI, code is associated with that phone, I'll get a new phone every week.

If we look at, for example, the difficulty faced in tracking, for example, non government military leaders, all right, and then the question [00:56:00] is, hey, we want to go ahead and find so and so is a, an actor, they're smart, they have good operation security, OPSEC, use something once, throw it away, use something once, throw it away, use something once, throw it away.

That's expensive. But it's a lot more expensive to get arrested or to get a warhead on your forehead and get blown up. Therefore, what do we do? If you're in a critical infrastructure, if you're in a line of business where the work that you do is going to be of significant importance to your community, Or to your nation or to the people you care about.

Maybe you need to go ahead and replace things sooner rather than later. What do You can keep a Cisco switch that's 10 years out of date, still running, although vulnerabilities will accumulate. They might patch them. But they're not going to patch them for the older version. I can still run Windows 95.

See, this is, they say art is anything you can get away with. So these are my old Windows XP machines, alright? And I can fire them up about once every year or two to [00:57:00] keep the hard drive moving. they stopped providing updates for Windows XP in 2014. Yet, it still runs. And I can put Office 2003, On Windows XP, put the plug in to help me read the XML files and I keep up with just about anybody for office work.

Doesn't mean it's a good idea because of all the existing threats that it has. So as long as this thing is sitting here powered off, it's secure because there's nothing to run. Think of the analogy here. Nation states, their intelligence services are going to do the best they can to pre position their assets at pre launch places.

Whether it's NATO saying, Hey, back in the days of the Soviet Union, we want to have somebody to prevent the Soviet army from coming through the folder gap, or take a look at something in South Korea saying, we're concerned about North Korea coming over in Japan, US forces being stationed over there for whomever their enemy might be.

There's a lot of parallels for it in the kinetic world, but in the kinetic world where we have things and objects and people and [00:58:00] devices and tanks that requires a lot of physically transporting stuff, which is a bit of a tell. In the digital world, we don't have that. Somebody, you look at the traffic, particularly if you have someone who's low and slow and they get a compromise in there, they may just be sitting there and waiting.

They could be watching for days or weeks or months or potentially even years, just in case they get the order to go. And much like zero days, age like milk, not like wine, because although I discovered a zero day, There's seven plus billion people out there and someone else eventually will figure it out and it's not going to work anymore.

I either got to use it or lose it as compared to, Oh, this is getting better all the time. That Windows 95 thing I've been cultivating for almost 20 years is ripe right about now. It's going to be a nice, wine. Nah, it doesn't work that way. How do we fix this? assume that there's somebody in your network until you can prove it.

Otherwise, how do you prove it? Otherwise? if I go ahead and rip and replace, put new stuff in there, it's [00:59:00] chances I took somebody out. But the thing is that if you have pure devices, it's And you take one of them out, someone else comes in, just like an infection. It's going to spread laterally. So you have to do it all.

You risk disrupting the organization because of the fact that some of these attacks are sophisticated enough that can actually get in the firmware and things like that. You're not going to spot them by looking at the TCP IP traffic. You're not going to set up Wireshark and sniff it and say, Oh, it's a bad guy.

it's going to be invisible. So it is a very tough problem, but understand that nation state actors are invisible. Today, actively trying to pre position themselves and has successfully done so on both sides or all three sides, however you want to look at it. this is, this is actually a very interesting, approach, let's say, and, I think it's very depending on, the trade model of the, organization being that a company or, maybe, a state itself or any kind of organization, because it's something that.

It makes definitely sense from a security professional [01:00:00] perspective. It also makes, it becomes, even more difficult at scale. So the bigger is the company, the, the bigger is the network and, how many devices are in there. The more difficult and the more, of course, expensive it gets to do something like this.

And at the same time, if you're also a very, small company and, all of your money is already spent on those few devices that you have in your network, in your infrastructure, replacing them from, From time to time, it can be a very, prohibitive thing. So I will understand the difficulty in, let's say deploying this kind of approach, but at the same time is, as you said, there are some specific, let's say, contexts that really justify the reason why you want to do something like this, right?

Because as you said, assuming compromise is not the fact about that you detect something bad going on. But the fact that, [01:01:00] for, let's say statistics, at some point, after a certain amount of time, eventually you will have not one, but multiple vulnerabilities on the same device. And, If we consider all of the different actors that are, acting in the wild, and we already said that there are different ones with different objectives and, all of those can all, target the same device potentially, Your exposed devices will be, eventually filtered.

It's not about when it's about, it's not about if it's about when it will happen. And if you want to get a good mental model, go take some food, take a plate, whatever you made for lunch and go set it out in the backyard. And just wait to see what comes. Probably flies will be first.

Boom. Ants will come again. Maybe a little bit later some birds will come by. And they'll come like that. You get a stray dog or a fox or something. And what you notice is it's attracting all this attention. And they can all be in there at the same time. Although they might fight with each [01:02:00] other for the big pieces.

Think of our resources the same way. They're attractive. to other entities. And those other entities can coexist and quote unquote feed off of it. Some may take advantage of the fact that maybe something knocked down the fence in your backyard and then they're going to go through the opening. They didn't have to knock down the fence, something bigger did that for them.

And given the fact that we all have budgets and things like that, I would encourage people, know your equipment, know what you have, keep your patches and patch up to date. Your patch management program is going to be one of the most critical things that you can do to manage this and then reboot your systems from time to time.

And if you're really worried about the presence of persistent actors, go ahead and take a look at your logs. And here's a good question to ask. What is the longest? Standing existing connection you've got going out through your firewall. why would you be connected overnight? Everybody. Everybody goes home at 1700.

At 1800, there should be nothing connected. And yet you find some things have been persistent for weeks or for months. And sometimes it could used to find [01:03:00] insider threats. Somebody set up a PC anywhere and they're remoting in because maybe they're hard workers, they wanna work over the weekend. Or maybe somebody had set that up so they can surreptitiously act from inside the network and grab your stuff.

But what if you cleared out all your connections? What needs to stay connected to the outside world once everybody has gone home? That's another way. And then when you, then you go ahead and now you turn on your wire shark and you sit on the outside of that and you see what connections light up first before anybody comes in the office, there's your threat hunting right there.

And that's cheap. And that's, would be, I think, an interesting thing to do. Yeah, it could be definitely cheap at the same time. Also, involves a lot of efforts for in time from the people itself. So you also need to. Probably cultivate your own security team, which is not something that unfortunately, every organization is, is doing right now, even though if we compare probably to, 10 or 12, 15 years ago, it's, definitely much better.

Yeah. Threat actor like [01:04:00] Volt Typhoon, which is a Chinese group, has been pretty much very effective in getting into obsolete or unpatched equipment. And so to a large extent, what I tell people is, let's say, when I try and clean the kitchen, I said, my job is to make ants hungry. What do Okay, in Florida, there's always going to be ants.

They've been here for a long time. And if you make them hungry, if there's nothing to eat, if there's nothing around, they're not going to come. They're going to yeah, this is, no good. Make hackers hungry. They're going to come looking for stuff. Make them work for it. Make nation state attackers work for it.

Granted, it's not like a hacker is going to go ahead and say, Oh, this is too tough. I'm going to go move along. When you're up against a nation state in some of these groups, these people coming in, they punch a clock. They come in the morning, they sit there, they work their eight hour shift, and then they go home to their kids, and they help their daughter with their homework, and they go ahead and have a conversation, and, this is what they do for a living, and that's part of their job, so don't hate the people.

They're just doing, they're just trying to feed their family, but make their job incredibly, difficult. When they get something, they ought [01:05:00] to be doing a happy dance, because it took them months to get around you, where everybody else might have taken days. Which is really all we can do, honestly, right?

It's, security is not about ensuring that nothing can happen because that's just not, let's say, philosophically possible. but it's about, making it very, difficult, even more difficult every day for them to breach our network. I'm really, happy we did this, Mark.

I am so thankful, for, all of the, inputs and all the information you just, gave me personally, but also all the people that are going to listen to this. But unfortunately, our time, is, is finished for today. I thanks, I thank also all the people that were, watching this live, but just as a reminder, if you didn't watch all of this, the video will still be there.

on the, YouTube channel. And also if you prefer just to listen to it, you can search for it in all [01:06:00] of the podcast platforms. thanks everyone. Once again, Mark, is there anything else you want to mention before we close it up? for those of listeners who came in through CISO Tradecraft, thanks for being part of another show.

We've just broken a record. That's the longest show I've ever done. Richard Thieme had that record prior to it, and that was a fascinating one. But Giorgio, I think this was great. I really enjoyed the opportunity to discuss some of these current events and things like that. This episode will go out, I'll say tomorrow, it's Sunday morning here when we're recording this.

And as a result, for those who follow CISO Tradecraft, if you're not already subscribing to our YouTube channel, please do Follow us on LinkedIn. We put out good information almost every single day, and it goes far beyond a podcast. We try to give a high signal, low noise, information so that you can help you with your cybersecurity journey.

And until next time. Thank you, Giorgio. And to our listeners and our viewers, stay safe out there. Thank you, everyone. Bye