Managing Cybersecurity Threats in 2023 Episode 2

PLUS Staff: [00:00:00] Welcome to this PLUS Podcast, Managing Cybersecurity Threats in 2023. We would like to remind everyone that the information and opinions expressed by our speakers today are their own, and do not necessarily represent the views of their employers, or of PLUS. The contents of these materials may not be relied upon as legal advice.

And now I'd like to turn it over to David to get us started.

David Shannon: Thank you, Tyla. Good morning, everybody. Thanks for joining us again. This is our second episode here on data security and data breaches in 2023. For those that you who don't know me, my name's David Shannon. I'm a partner at uh, Marshall Dennehey in Philadelphia.

I chair our Data Security and Privacy group, and I have with me Ryan Chapman, who's with Unit 42 of Palo Alto Networks. I'll let Ryan introduce himself as.

Ryan Chapman: Hello, hello. Yes. Thank you for the intro and I'll continue that. My name is Ryan Chapman. I work with Palo Alto's, Unit 42, working Incident Response.

I work a number of ransomware cases, [00:01:00] and I also am the author of the New Sans Institute Course Forensics 528 Ransomware for Incident Responders. I basically spent a year and a half of my life kind of putting, pen to paper on how the incident responder does what we do. And so, I've been living and breathing ransomware.

I've been taking the cases purposely versus," Hey, do you want to take this case?" "Is that ransomware?" "No, I want ransomware." So, I've been just immersed in that world for a very long time and I'm very excited to be here to talk to you today.

David Shannon: All right, I appreciate it. Thanks Ryan. And I'm glad you're so energetic so early in the morning, here. So, we're going to talk ransomware real quickly. Three issues I thought we would touch on. There's so much to talk about with it, but if we're going to look at the current state, we're about three months into 2023, the new year. And so, we'll talk a little bit about what we're seeing the different threat groups, the different type of attacks just in the last three months.

We'll also talk a little bit about the ransoms we're seeing with no exfiltration or with exfiltration but no encryption. And then finally, the Biden [00:02:00] administration came out with a new national cyber strategy about three weeks ago, right at the beginning of the month. And there's a lot there, but we'll try and touch on just a few key points that Ryan and I have seen and what's being talked about in the media and in the data security and privacy realm here in the United States and really across the the world is cause it will affect everybody. So first, Ryan, let's talk a little bit about, I can tell you that, I've seen an uptake tick in ransomware attacks. In the cases we're getting, say in the last month, I've had different forensic groups tell me they've also seen an uptick in the number they're getting.

I had one forensic group tell me that they were at full capacity just two weeks ago and couldn't take a case that I called about. Which really means that there's something going on where there's more attacks, whether it be with encryption or without encryption, and they're just taking data.

That's what I've really seen just in the last three months, is that ransomware well, it slowed down a bit. In 2022, there was a lot of stats and articles about how it had gone down in the last couple quarters of [00:03:00] 2022. It seems to have really jumped back up a little bit now, and we're seeing a lot more, seeing higher demands to start.

At Unit 42, what are you guys seeing? How do you see the current status of this type of attack as we're heading into, almost into April now.

Ryan Chapman: Basically, exactly what you said. There was a bit of a lull towards the end of 2022. There were media reports all over the place talking about how ransomware is going away, and that was not the case at all as far as, what we're seeing and the data that I see on a personal basis there's a, a drop off, a very big drop off in payments to ransomware actors.

And if you're familiar with Coveware, they do a ton of negotiations and they recently posted a blog article, I don't remember the exact month. But if you just go to blog.coveware.com, there's been two different iterations over the past, I want to say six months-ish from this recording where it was like, "Hey, ransomware payments are way down, right?"

And a number of us were looking into, "Ooh, why is that occurring?" And a big part of that, the big belief there was the conflict in Ukraine and how so many of [00:04:00] these groups are backed by Russia. And there's so many then conflicting feelings of, "Ooh, wait a minute, if we give these people money, financial capabilities, like what, what are we doing here?" But at the same time, I personally did not, and our group did not really see ransomware drop off. It continued it, there was a lull, and then all of a sudden, we have this big uptick. We have groups like Vice Society who are going crazy after colleges, or I should say higher education institutions.

We're seeing cities basically being targeted. Some of these are being targeted, some of them are being more of a wide- net approach. And another thing that I'm seeing is that Allan Liska is a fella who I have a lot of [00:05:00] appreciation for. He has a book out Ransomware: Understand, Prevent, Recover.

It's a very high-level book. He does a lot of presentations. I love Allan. He did a talk recently at I think it was ResponderCon and talking about the de-razzing of ransomware. So, ransomware as a service is strong. It's still continuing strong. However, we're seeing these offshoots of individuals going out and basically doing their own thing.

And there's more cases that I've even personally worked where you're not really sure who the threat actor is. And that's very different from what we were seeing in 2022. And before, you were seeing this boisterous, "Hey, you've just been hit by so-and-so group." Whether it was the big player, currently Blockbit or BlackBite, or whoever it may have been.

But in these cases, we're seeing a lot of these, what look to be kind of splinter groups is they're just taking bits and pieces from other groups and doing the same things, but then avoiding, that big old pot sharing towards the end basically. So, we're, yeah, I [00:06:00] definitely see an uptick. There are too many and it's bothersome.

It's very bothersome. Too many groups who are quote unquote at capacity, there are many cons consulting firms out there just like us at Unit 42. And you start to see how busy we and they are, and it gets to be very bothersome, which makes sense as to why the Biden administration recently started pushing more and more policies and realizing this is not going away.

Like everyone thought in late 2022, "oh ransomware, that's going to be a thing of the past." No, not what we're seeing, right now.

David Shannon: Yeah, I would agree with that, Ryan. I know last week we were handling one where we had a real lull in getting a response from the threat actor. And it was surprising.

It I think it took well over 36 hours from our initial response and we were like, "are they so busy that they can't get back to us?" It even, it sounds sad, but the threat actor's, customer service is poor because they have so much work. Kind of going into that, I think we, obviously we're both saying and talking about everything [00:07:00] we've heard, that ransomware is definitely still very prominent, may even be increasing a little bit in the last month or so.

Touch on a little bit, Ryan. What I've seen also is and it's well known now, but the, the ransomware attack that occurs and they don't encrypt the data. They just take the data. Particularly, if it's like a professional services group, whether it's a law firm or if you get into some of the medical providers but they take the data and just say, "we have it, we're going to publish it."

They now know that's such a big threat to these companies and to these businesses, and it really does become an issue. And then, you're basically negotiating just so that you can get a video or a screenshot of them deleting the files. What that really means, have they copied them somewhere? Likely they have, but at least the client or the business has some kind of assurance that they can at least tell people that we saw them deleted, but definitely have seen that. Or where they're just exfiltrating data and then they're sending you a file tree and saying, “we have all this, and you better pay us.”

Are you seeing [00:08:00] that as well? And are people paying for that just as much as they would to get a de-encryption key like they did in the past?

Ryan Chapman: So, I can't comment directly on negotiations that we've done at Unit 42 because we do perform our own negotiations and at middlemen, some of the payment stuff, if that needs to occur.

So, with that caveat out there, I'm saying the big four and there might be some people saying, "wow, what about this group?" I'm like," this is what I'm seeing." First off, the Karakurt Extortion Group, which was essentially started after the downfall of the Conti brand. I'm going to call it a brand cause that's what it was.

Cause those people didn't go anywhere. They just stopped using that brand and then they splintered into other groups. They're still hard at work, making our lives miserable, basically. So Karakurt was one of the first ones to put out, "Hey, this is what we stand for. This is what we do. We are a data extortion group."

After them, you have groups like Ransom House who are doing that. They're not as well known, for example, as Karakurt, but they're getting there. And then more recently, we've had at least two very large [00:09:00] groups who are very well known for a while now, who have transitioned to this methodology. We're still seeing every once in a while there be an encryption via one of their attacks, but that could just be an affiliate, not getting the memo kind of thing perhaps. But Beyond Leon, and then also The Clop Group, which that name goes, back for a number of years now.

These two groups have recently joined that ideology of, yeah, let's just do the data extortion itself and not block down the entire environment. So, I have heard, let's just say not including cases we've worked at Unit 42, but I have heard that folks are paying in order to get that data quote unquote erased, which just like you referenced, what's really happening there, I can make a video of me deleting data, doesn't mean I'm deleting it, so there's always that big worry.

But what worries me, is that this is helping these groups get a quote, unquote get away with it, right? They're being detected far less. And for that matter, they may not be detected until they essentially announce, "Hey, this is what [00:10:00] happened." And so, when we see groups like Beyond Leon and Clop make the move to do this, to no longer encrypt, basically, then you start to wonder, Ooh, how many other groups are going to do this?

And is it an overall good or is it an overall bad? So, it helps them avoid certain detections. Now, you have files being encrypted in an environment and there may be, certain alarms and things like uh, multiple files being written or modified at one time, or certain extensions, especially when they're not randomized, that are showing up with an environment that look like, "Hey, that looks like ransomware."

There's a number of us in IT who trained ourselves for many years, starting back in 2012-ish. "Hey, detect ransomware when stuff is being encrypted." So first off, horrible. That's never when you want to actually detect them, but we still have a lot of those systems, which I call legacy at this point.

Like, sure it's good to have it. That's not where you want to detect them. We have those things, but you also have the issue [00:11:00] where the threat actors are able to avoid notifying you because your systems aren't going down and your services aren't going down. The real impact to encryption, aside from just, "oh, users can't use their systems," is the entire network essentially goes down all the time, right?

You have active directory just being completely inaccessible, and that runs the entire network environment. Your payroll system gets encrypted. You're not able to function as a business. So, it's, I see it as a dual-edged sword. The threat actors are looking and going "we're not going to have as much of an impact." But what they do to counteract that, what I'm finding is that they have the role of the chaser, and they have the role, which is usually signified by like a fist in their little documentation and stuff. We want to hire chasers cause you know, they have active recruiting campaigns and, and things like that In these groups, the chaser's job is to chase down the money, like you have to pay us because, and they'll be the ones who also place calls to, VIPs and board members and [00:12:00] media and all kinds of places.

And we're seeing that, by the way, also an uptick in that type of activity.

David Shannon: Yeah, I'm aware of one where, the CEO and five board members all got the email letting them know, "we've encrypted your data and here's the stuff coming right to you, and we're going to start sending it to everyone that we can see in your email box, because we're in it and we're sending you an email directly."

So, are you seeing that as well, where they're getting very smart in how they look through a company's data and figure out who are the key players and who do we want to really scare so that we can get paid?

Ryan Chapman: Yes, exactly. So, in addition to the chasers, they're quote unquote hiring more, training them better, whatever they're doing.

They're also the data archive specialists. Many people have different names for them, but there are roles of people whose job is just to go through the exfiltrated data, to categorize it, to tag it, and to market and, what's supposed to be confidential and what's intellectual property.

And then that's their job, their data [00:13:00] warehouse specialists for stolen data. Those people are doing a much better job, unfortunately, for all of us, as are the chasers, and they're working very closely together. And we're even seeing that it's such an uptick in the exact activity that you just described that we're seeing fraud groups.

Technically this is a type of fraud, right? But we're seeing external fraud groups. Trying to capitalize on that. So, there was one that I sent out a LinkedIn and a tweet and whatever the social media I'm on, and it was, "Hey, be aware of this incoming ploy from a group calling themselves The Midnight Group."

I thought it was a new ploy and I looked at it. Coveware actually had it documented back in 2019 on their blog, and it's basically an email that goes out and it looks, they actually borrowed from the Royal Ransomware Group, the way that their notes look, essentially. And it makes it look like, hey, we have taken, and they give a number of gigabytes of data that they've stolen.

They use individual's name directly in the email to make it a little more [00:14:00] personal. And it looks like, "oh goodness, a data extortion group hit us." Not if they're named, Midnight Group, no. No, they didn't. They're just trying to get you to pay them for nothing. But that type of email where you don't have encryption and you just get notified, "Hey the following is really going to not be fun for you to read. Here's what happened. Give us money."

That is becoming more and more common. And it's, I see it over time as becoming very pointed in terms of what they actually have. And there's, they comment on, "we know exactly what insurance you have. We know how much money you have, this number that we're throwing your way in terms of what you have to pay us it's not arbitrary."

And they're becoming really good at that. And that's scary.

David Shannon: Yeah, it is a shame. I had one where they were quoting the coverages for a company's policies. Unfortunately, it was the one that they had about four years ago. I should say fortunately, cause they saw that, the coverage wasn't as robust as they then had.

So, I think Ryan, yeah. The two kind of key takeaways, just for the last three months for 2023 are ransomware is as strong as ever. There are still numerous [00:15:00] companies out there or companies, entities, threat actors who are conducting these attacks, and there's both encryption and non-encryption where they're just taking the data.

So just the final thing we wanted to talk about was, what's the response? The government response. So, I think it came out on March 2nd or 3rd, was the the National Cyber Strategy, which was a document and a policy document that was put out by President Biden's administration. It's not an executive order.

For those that you are aware, that means it's not an order that's has the effect of law. It's more of a policy document that's come out. And I know the two key points I saw and have read and heard about Ryan, and you can comment on 'em, are one. They want to kind of go after, so to speak software companies and say, you've got to do a better job of building in security into your systems before you put 'em out in the market.

That you can't just develop this great software program and then sell it. And then everybody finds out later on that you have all these vulnerabilities. So, they want to try and in some way, and there's talk about getting rid of limitation of [00:16:00] liability clauses or making these companies more responsible for these incidents.

So that would be one thing they're talking about. And secondly, is they want to become much more proactive in responding to these groups as opposed to reactive as we've been for say, the last, almost 10 years now since this kind of exploded. And by proactive, I mean they're talking about having the FBI and the Department of Defense really go after the threat actor groups.

We saw that, it came out in January. That one of the threat active groups had been infiltrated and for about six months, the government, the FBI was letting companies know, "yes, you've been attacked. Here's the de-encryption key, because we know they finally became public with that." So, it sounds like that's another area that the government thinks that we really need to change is instead of just reacting to these threats, actually trying, getting out there and stopping them beforehand.

So just what's your thought? I know you're well aware of this document and what the government's at least talking about or proposing. What do you think about it or how do you think it's going to end up as we go forward after they've [00:17:00] outlined all these issues?

Ryan Chapman: I think most of what they outlined is fantastic, and I just hope hope, hope it's not lip service and it's a real thing that's going to happen.

So, touching on the first thing you mentioned, a better job of building in security. When I first read what they had listed in I guess it was just the very, very top, of the the March 2nd publication was Rebalance the Responsibility to Defend Cyberspace. And that's in bold. By shifting the burden for cybersecurity away from individuals, small businesses and local governments.

And right there I started to worry. I said hold on. We still need them extremely familiar with what's happening, and we still need them plugged in. Let's not just, move away from those entities cause they're the true victims in all this. However, there's a big push to do things like, security enhancements of products.

And one of the ways that they're doing that, and I, I believe it mentions it in the full document. And there's some discussions, in the environment, my cohorts and myself and such like that of uh, bill of materials for [00:18:00] software. And it's something that we, The Royal we is that do a horrible job of.

So, these days it is very uncommon to produce software that doesn't heavily rely on third party software. On third party libraries. And so, a lot of those may be open source. You might be able to find 'em on Github.com, a the world's biggest code repository, basically. But what groups are not doing is they're not warehousing and cataloging and maintaining and following up on what software are they using in their software.

And the problem with that is then when all of a sudden one of those libraries that they're using, when one of those has a vulnerability, now your software potentially becomes vulnerable. And if you're not aware of that, because you're not tracking, that's a huge, huge problem. And a prime example of that would be the Log4J, or as some people call it the "Log Forge".

The Log4J vulnerability from Apache, the Apache Logger Log4J module. So many entities around the world were using that in [00:19:00] their software, and many of them weren't really even paying attention to that fact. So, when Log4J had this massive vulnerability, it started affecting big, expensive, this is the stuff that runs our infrastructure products.

And slowly over a period of about 30 days, these groups started announcing, "Hey remember that Log4J thing? Yeah. That greatly affects our product. In fact, if you have our product exposed to the internet, stop it now. Here's a fix." And the more that we have our eyes on what's actually embedded in all this commercial software, the better.

And for that matter, the more we have our eyes on who's not using commercial software, who's using open source and what those libraries are and what the security status of those are, the better. So, for that part, I love it. I think it's fantastic. We really need that. It's important.

David Shannon: And what about that second part there, Ryan?

Just cause I know we only have a few minutes left, what do you think about the government saying they're going to be more proactive? Some people have been a little skeptical about that. They don't move as nimbly and as quickly as the [00:20:00] private sector in some respects. What's your take on that?

Ryan Chapman: I'd absolutely love to see it.

What it's going to truly require, I guess I should back up a second here. Many people view ransomware entities and groups as ghosts, as these in invisible individual. No, not at all. Many of these highly, like high profile ransomware actors are very well known. Like they're actual human entities, like the people, like they have names and they drive certain types of cars.

And they're spouses like to post on Instagram. Like there's a lot of things that are well known about these actors. But based on where they're located, it's very difficult to quote unquote, do much about it. And so what I, from reading this whole like strategy and thinking about how this is going to really become a reality, it's going to require pressure, it's going to require a lot of pressure by the USG, by the United States government to try to, as best as they can, get action taken on these individuals.

And many times, many rants of our [00:21:00] actors are Russian speaking, right? They don't all necessarily live in Russia, but they primarily communicate in Russian on the dark net forums and things of that nature. Many of them live in quote unquote non-friendly countries. They're not, you not, there's no extradition law in place.

You're just say, "Hey, we need-- okay!" It doesn't work that way. So, what is going to be the thing that our government is able to do that says, "Hey, that person, we really need them to stop what they're doing. Like how are we going to make that happen?" And so, what I read in the document, it all sounds great, but they're going to have to leverage things and I don't know what those things are going to be.

And those are often the non-public things, right? So, what are they going to leverage and how much pressure are they going to put? And what true priority are they going to put there? Because our government has a lot of leverage. But where are they going to specifically place it and how important are these ransomware actors?

Truly, I believe they're becoming more and more and more and more important in the government's eyes. And that I think is actually fantastic.

David Shannon: That's true, Ryan. And I think that's what we're [00:22:00] going to probably watch for the next eight to nine months this year. And probably at this time next year we'll be looking back and saying, okay, this policy came out.

What actually has been done and what still needs to be do as opposed to just being talked about? But but that's for our next episode, probably in 2024. So, Ryan, I appreciate you joining me here on this one, and I appreciate everybody out there who's listening to the blog on the PLUS website and their LinkedIn page, and I believe they also have it up on Twitter too.

So, if you have any questions, feel free to reach out to Ryan or myself. And with that, we will turn it over to PLUS. Thank you.

PLUS Staff: Thank you David and Ryan for sharing your insights with PLUS and thank you to our listeners for listening to this PLUS Podcast. If you have ideas for a future PLUS Podcast, you can share those by completing the content idea form on the PLUS website.