Managing Cybersecurity Threats in 2025 Episode 1

PLUS Staff: [00:00:00] Thank you for listening to this PLUS podcast. Before we get started, 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.

With the housekeeping announcements out of the way, I'm pleased to turn it over to David Shannon.

David Shannon: Thanks, Tyla. And good afternoon, everybody. Thanks for listening again. This is another installment of our Cybersecurity and Data Breach podcast midway through 2025. Got an excellent guest today and we're going to talk about some of the kind of cyber trends and review what we've seen so far in this year.

As everyone knows--hopefully knows, I'm a privacy attorney at Marshall Dennehey. I've been working on these matters for probably about over 10, 12 years now. And we try and just look at some of the issues that we see periodically throughout the year in these PLUS podcasts. I'm joined by Evgueni Erchov, who's with Cypfer, which is a [00:01:00] forensic firm that I work with and probably a lot of insurance professionals, whether the underwriters, claims professionals, or even brokers are familiar with. I'll let him introduce himself. Just give a little soundbite on what they do and where they are right now. And then we'll talk about some of the things that we've both seen over the last six months.

Evgueni Erchov: Thank you, David. As David mentioned, my name is Evgueni Erchov. I'm Senior Research Director at Cypfer. So primarily, I focus on cyber threat intelligence that we get from our internal cases and doing analysis, a lot of analysis, on trends like with outside sources as well. And also conduct basically research and development on new service lines and technologies.

Quick background, I've been working in incident response field for about nine years. In former life, I served as US Army cyber operations officer, where my team supported one of the three letter agencies like in DC area. And I had a cool opportunity to actually work on state sponsored groups.

Based on my accent and my naming, probably can make an educated guess like which country was my [00:02:00] favorite. And also spent a few years working as a special agent chasing cyber criminals for living as well.

David Shannon: Oh, that's great. Thanks. I appreciate it. I'm glad you're here with us. So, as I was saying, yeah, we're about six months in now almost for 2025.

We always see some trends or some new things in the cyber field. Some of it remains the same and always will probably, but just wanted to kind of, we'll touch on a few issues there. Evgueni, and see what you think. I know ransomware wise and business email compromise, that's what we continue to see.

The numbers go up slightly, go down slightly. Depends on the month, depends on the threat actors. There were some large ones in the last few months. I know Yale New Haven Health had over 5 million records that were compromised, Hertz Car Rental, which I am a member of and usually use their app and their cars, they had over a million people.

Out in California, one of the Blue Shield healthcare providers was hit also, I think close to 5 million records. So not the 100 million, 200 million we see, but significant ones there. And then [00:03:00] of course, all of the smaller ones that we see on a daily basis.

But I think one of the things that I've seen, and we have a lot of problems with and issues is the third-party vendors is, you just see that so much now in a lot of these, where it's the third-party vendors that really, that's how they're either getting hit, which then leads to their clients or customers being hit as well, or, they're the vulnerability that, a threat actor will use to get into the larger client, which has all the data.

How about yourself? What are you seeing this year so far, and any particular trends you've seen in the ransomware field with some of the new threat actors or how they're getting into some of the businesses to get the records and to get the data?

Evgueni Erchov: Yeah, I guess somewhat good news is that we definitely see some kind of stabilization because ever since the Ukraine-Russia war started, we've seen a lot of restructuring, rebranding, going on. And closer to the end of the last year, like the number of groups that we've been tracking was like, it's around like 250 groups on and off [00:04:00] conduct ransomware, reparations.

And so far this year, like we don't really see that the bulk number changing that much. So, we may see like couple groups disappear, couple groups show up. But it appears that, in some sense, operations of those ransom groups stabilized, they probably a lot of them much smaller now because like with all the law enforcement operations and joint international collaborations between incident response and cybersecurity companies it is almost too dangerous to be a large, very successful group.

So, because of that, like a lot of them probably tapered down, got like smaller and I don't expect that trend to change going forward. But based on numbers, nothing really unusual that we observe month to month this year, because usually January starts pretty slow. Like my theory about that is in Russia, actually the first 10 days of the year are holidays.

So, I would assume that some of the cyber criminals that operate out of there have families and they will take them on vacation for the whole month, and that's why it's fairly slow. [00:05:00] Then we see like rapid growth in number of cases, like all the way through July, then July, like a slower month as well.

So far from January through May it followed the same pattern. So, like May was extremely busy for us as well and was more busy than the previous month.

David Shannon: Gotcha. Are you seeing any new groups that are doing anything different, this year or even at the end of last year or, you were talking about how it's stabilized somewhat.

Do you think it's stabilized as to how they actually do their work? So, it's a set program, set plan as how they walk through, get access and then, they handled the whole incident. Anything new or slightly different in the last six months?

Evgueni Erchov: I think the most concerning trend is that like with the whole restructure and assumption that the majority of those groups got smaller, I would expect them to be less sophisticated.

But unfortunately, we've seen some of the groups I think like Skatespire and I believe Luna Moth was the second one that still use fairly sophisticated techniques when it comes [00:06:00] like to initial exploitation of the network. So, like in, I think with Luna Moth they exploited a vulnerability that wasn't even announced a month later.

So, either they somehow were able to purchase it or they had guys smart enough to figure it out. Like through red teaming. It's like BlackCat teaming, from their

side to figure out and find that vulnerability and exploit it. So that piece is somewhat concerning. But at the same time the trend, like for the bulk of the groups is pretty much the same.

So, like they try to use the same type of like botnets, malware, open remote desktop connections, compromised VPN credentials. So, for the bulk of the group sophistication of an initial intrusion definitely got lower. And I guess that part is really good news.

David Shannon: Yeah, I think one of the things I was thinking about was, it seemed to me in the last, and it might be longer than six months, but even the ransomware notes that you see are written much clearer or in better English.

It used to be, obviously you would look at these [00:07:00] things and just kind of laugh at them, as to the poor English and the broken English, et cetera. But it seems as you said, they've kind of gotten more sophisticated and it's more standardized that yeah, I think that they have people who are fully conversant in English now, and the notes are just written better, much more professional, almost--you hate to say it.

And one of the other things that I've noticed, maybe you say in the last six months, to a little longer, is that the threat actors are staying, I think I would, I guess I would use the word patient. It used to be they were really on you to try and get their money immediately.

You know? They made it so that it was this huge threat that everything had to be done in 48 hours, you know, within one week. Now I've seen a number of ones where, they just you know, mosey along, so to speak, you know, and you can go a month negotiating. You can string them along even if you're not going to pay just because you want to try and string them along while you're trying to get the backups up.

Are you seeing that now more too, that some of these threat actors will just, they'll keep at it? It's not an emergency to them that they have to get this done in seven days to 10 days?

Evgueni Erchov: We [00:08:00] definitely see the same trend. And I think like part of the reason for that is that those groups got restructured.

They don't have pressure from upper management, they got smaller. And on the language piece, not necessarily that those guys took some classes in English. I think like artificial intelligence has something to do with that because I wouldn't

be surprised if some of the groups are using AI even to like conduct negotiations based on the responses that we get because they like, they have proper grammar, they're trying to be polite.

And the same goes for the ransom notes as well. We definitely see an improvement ransom notes and initial efficient emails. Because it, like, I completely agree with you. Like before if you would look at the email and you definitely can spot some of the grammar mistakes, it would be pretty easy to spot a phishing email.

Now they can even like with, especially like with use of AI, they can mimic your writing style. It will be sufficient for them either to see some of your emails or even take a look at some of your articles or blog posts that you [00:09:00] published somewhere like on internet and mimic the language in the phishing emails and communications the same way.

David Shannon: Yeah, I think that's a good point. We've talked about that a lot, both internally here and then in some of the conferences I've been at, is that the AI is really just going to improve, the procedures, for lack of a better term, that the threat actors use is that they just get better and better at drafting those phishing emails, and all the other communications that they have, and will make it harder and harder for people to set up the security for it because it's just fooling people to click on those links.

But yeah, so that's, I think, really ransomware, as you said, I think it, we looked at the last six months. It's somewhat stabilized. There are more people that are backing up in better ways, so you're not paying as often. But we're still seeing it, so it hasn't changed in that effect. It's just too lucrative for them to go away or to move on to something else. How about we switch gears a little bi?

How about the wire transfer frauds, the business email compromises? We've seen more and more of those [00:10:00] obviously in the last few years. Getting a lot of them this year as well. I looked at a couple of studies over the last month, which really saw, they were seeing increases in them, during the months, the first quarter of 2025.

And really seeing that everybody's getting hit. I read one study that was interesting. It said, if it's a large business, you're going to get a hundred percent of the time they've been hit by somebody. If it's a business with a thousand plus people, probably 80% of the time.

And then, in the surprising number, the businesses that have less than a thousand people, they're still getting hit with, wire transfer phishing emails and all that, probably up to 70% of the time. So, it seems like those are maybe AI generated as well. And it's just going out to so many different computers, so many different businesses that they're hitting on all different companies and different industries. What are you guys seeing in that field, in that section over the last six to eight months?

Evgueni Erchov: Unfortunately, just like ransomware business email compromise as a cybercriminal business will not go anywhere [00:11:00] anytime soon. And you mentioned artificial intelligence helps, significantly to reduce the barrier of entry into that field for cyber criminals because of a better English, or more sophisticated phishing emails more that you would trust.

We also seen combined techniques where they would try, for example, would leave you a voicemail pretending to be one of your partners from another company is saying, “Hey I'll be about to send you this document. Please take a look and respond to us as quickly as possible.” And in some cases, even using artificial intelligence to generate that voice email. So, you would not be able to spell the next something there.

And obviously, like if you expecting something, like you most likely will either open the document or click on the link and potentially would compromise access to your email environment. And the same thing goes for the actual multifactor authentication because seam swapping has been around for a while already.

There are also some new techniques to bypass the other forms of multifactor authentication as well. And [00:12:00] once they get access to your email environment. they can sit on it for weeks and monitor communication to figure out who's responsible for what, who's responsible for proven wires or any type of potential financial transactions, or even like HR records, your direct deposit accounts, et cetera.

We only had one case recently where a client was expecting a refund from his country club. So, he canceled a subscription with the country club and they owed him, it's was over a hundred thousand dollars.

David Shannon: That's a nice country club.

Evgueni Erchov: I'm sure the client is doing really well otherwise. But like the threat actor was able to basically intercept that, interject themselves into that

communication, start talking to the country club directly on behalf of that client, and updated the direct deposit information for the refund.

So, the guys are absolutely creative. They will continue to come up with new methods and techniques on how to gain funds. And yeah, unfortunately business email compromise is not going [00:13:00] anywhere.

David Shannon: Yeah, and I think it's a variety of things too. I think if you asked me one industry that we would say see more than others, it would certainly still be the real estate industry, just because there's so much money that's being wired, between the title agents and the real estate brokers and the banks and everyone else.

But, I had one recently where it was a wine importer, a small business that was importing wine from Italy, and they got into his system. And it's a small business, does well, but was shocked that they were able to get in and do all these things.

But it was the same as all the others. One of his employees clicked on a link and we were able to determine that they monitored their email system for about two months. Until they made a couple of changes and, some, I think it was two different, emails that had money being wired separately, not a huge amount of money, which was always interesting.

But enough that if they're doing it to so many different companies, it all adds up. We've seen some really large ones where you get into the six, seven figures. And then seeing these smaller ones where it can get down to, $40,000. It's almost like [00:14:00] if they get into somebody, they'll look around for a while, I think, and then if there's nothing large there, then they'll just do one or two smaller actions just to make it worthwhile.

Do you see more every day where it's say, five figures, six figures, as opposed to multimillion dollar wire transfers?

Evgueni Erchov: On business and compromise, like it usually small amounts, like we're not talking about the millions of dollars because millions of dollars are easier to spot.

Most likely they have to follow like additional approval procedures on the company side. So, like it's probably easier to spot, but even if you are able to, interject yourself into the process and get out like 10, even 10-20,000 like few

times over the course of the several months. It's still pretty significant, like once you multiply it by number of victims that they compromise.

David Shannon: Yeah, I think that's what it is, is that if either, if they're sending out all of these phishing emails and they're, it's just a matter of how many clicks do they get and then you get in and look and sooner or later they're going to find some [00:15:00] weakness and then take the money they can. And if they're getting 50 or a hundred thousand dollars from each one it all adds up.

And unfortunately, the client asks us, "what can we really do to protect ourselves?" And because it's employees mainly just clicking on phishing emails, you got to tell them, it's all just education. And the more education they do and the more training they have, it just gets more people to think before they're clicking on all these things.

Because I think these smaller businesses, they just don't have the robust, security and firewalls and everything else that you're going to see at larger companies. So unfortunately, when someone does click on some malicious link, they're getting in there with that. The threat actors are getting in there without the security, being able to figure out what's going on until it's too late when the money's already been sent out and gone.

But I think we'll see that continue, don't you? I mean, they're getting that money directly. It's sent right to them. So, it's another one where it's too lucrative for, you know, these threat actors and hackers to walk away from it, or move on to something else until somehow they see a decline in the [00:16:00] amount of money they make on these wire transfer frauds.

There's no reason for them to go into another field, unless they wanted to join you on the good side.

Evgueni Erchov: No, absolutely. And like to chime in on your point about the employee training like un unfortunately, like cybersecurity is not just like technology, like challenge technology issue.

It's also like a human issue. Because it, it doesn't really matter how many times you train your employees. And partially because of the most sophisticated types of attacks, like it still be a certain percentage of people that I would click on the link.

And just in another like quick segue, another example is like one of the trends we currently see is called spam bombing. So essentially like what the cyber

criminal's doing, they would automatically subscribe a victim to I don't know, like thousands of different newsletters.

And all of a sudden you start to get like hundreds and hundreds of emails, like from all the different countries. And it's almost impossible, especially if you're a small company, it's almost impossible to keep up with your spam [00:17:00] blocking. And later on, they would basically pretend to be your IT help desk and call you and say, "Hey, like we having an issue with your email environment without email environment. We, we can assist. If you want help. If you want help we'll help you."

And they literally like walk the victim through the process on how to install remote access tool. It could be like Team U or it could be some other solution. And the shortest time, like from the call to the actual exfiltration of data that we saw was like five minutes.

So, in five minutes, like from the start of the call, the artist would steal like a lot of sensitive data from your hard drives. And then they like would circle back and all try to extort payments to make sure that sensitive data is not being published. And the same thing can be done for just like typical ransomware attack where they would use that access to get back and install ransomware in your environment later on.

David Shannon: Yeah, they get in there and they do things so quickly. And the phone calls are really [00:18:00] tough and I have one, it's a real estate agent title company matter, which is in litigation now. And same thing where a call was made, but it was a phony phone number on the email, and the person they talked to sounded totally legit.

So it's, that individual is, "yes, it's a fraudulent email, but I did make a call, unfortunately, the phone number that was on that email was fake too." It's, you can't win. You tell everyone to make a phone call and then they look at the email and they see the phone number and they make, unless they're really hovering over that email address they're not seeing that it's a fraudulent email.

So, as we educate people better, the threat actors get educated too, and they change what they're doing, unfortunately.

Evgueni Erchov: Yeah, I have a funny story on that topic. Back in my former life when I was special agent, I was working on a case where I had to notify 15 US banks and some federal credit unions.

So, they have an issue, and they basically would need to work with us to resolve the issue. So, try to imagine like somebody on a call, like with my Russian accent, like trying to convince [00:19:00] you that you've been hacked and you have an issue. After like couple attempts I just give up. I say, “okay, like just Google my agency, like the hotline, call them, this is my name. Ask them to connect them to me. And then we'll continue the conversation.” Because otherwise it wouldn't be, it was not working.

David Shannon: I could see that. I could see how that might be a problem when you're calling the bank, but hopefully they were all able to get it resolved, one way or the other.

But alright, I think we've hit our time limit there. I appreciate it, Evgueni. It's always good to look at everything every six months or so. And unfortunately, I think the word that you kind of used that it's stabilized, is somewhat of a problem.

It's not getting better. You certainly don't want it getting worse, but it's become more of an everyday event and people are just almost numb to it now. Unfortunately for all the businesses out there there's only so much security that they can buy, they can pay for. Only so much education they can do. And for the threat actors, the better they get it, obviously the more money they're going to make. So, we'll see where we are at the end of the year if [00:20:00] anything else has changed. But I appreciate you getting on here with us and Tyla, we will talk to everybody in another three or four months.

Evgueni Erchov: Thank you very much for having me.

David Shannon: Absolutely. Thanks.

PLUS Staff: Thanks for listening to this PLUS podcast. If you have ideas for a Future PLUS podcast, please complete the Content Idea form on the PLUS website.