Eye on Security

The Cyber Landscape in Latin America

Transcript

Luke McNamara:

Welcome to another episode of the Eye on Security podcast. I am your host, Luke McNamara. Joining me today for a discussion around the threat landscape in Latin America and how organizations are facing it I have Ryan Goss, VP of Latin America and the Caribbean and Juan Carlos Garcia Caparros, director of Mandiant Consulting for Latin American in the Caribbean. Welcome folks, how are you?

Ryan Goss:

Very well. How are you?

Luke McNamara:

So maybe we can throw it off with tell me a little bit about your team's function and organization and what you're focused on solving or addressing for customers. Ryan, let's start with you,

Ryan Goss:

Like you mentioned, I'm the vice president for Latin America. So in charge of all sales and operations for the region and focused on really growing the company at this point, we have a relatively small footprint in the region. So really focused on building out our channel infrastructure, really going after the top industries where we play the best and I know we'll get into that a little bit later and just the overall sales and strategy marketing of what we do in Latin America, which are also is very important for the part of Mandiant and services.

Juan Carlos Garcia Caparros:

Hello, I'm Juan Carlos. I'm the director for Mandiant Consulting services in Latin America and Caribbean. And my focus principally is to offer solutions that could be in the consulting and implementation or even in the managed services side to resolve all these questions that customers have today in cybersecurity.

Luke McNamara:

So we have done, I guess, a few of these and it's been a bit of an informal series where we've looked at different regions and the threat landscape there and how organizations are focused on responding to those threats. And so maybe that's where we can first start this discussion here. Juan Carlos I'll start with you. Historically, what are the sorts of threats that we've seen face customers in Latin America? I'm sure there's been a lot that are very similar to what we see in different regions, the different types of adversary motivations, cyber espionage, cyber crime hacktivism, but give us a flavor for what that's looked like historically in Latin America.

Juan Carlos Garcia Caparros:

Oh, Latin America is not too much different from the rest of the world. Cyber criminals are focusing in monetarizing their vulnerabilities that they found in the customer's infrastructure. And also of course there are other kinds of attacks where they want to steal some information in order to use it or to sell it or even for espionage purpose.

The other thing that has come in the last year is the kind of criminals that are responsible for the states, countries that are interested in make a major changes in other countries. Now it's not just the monetary or the financial purpose, but it's over that now. So they can be involved in elections or immoral political stuff. So the landscape that we can see is very wide. And the idea is in our case is to be in the frontline, first to identify what are the motivations, what are the techniques and how we can help the customers in order to go about that kind of attack.

Luke McNamara:

Are there certain aspects of adversary activity or maybe the nature of how organizations are structured or other aspects of the business and the society there, where there're particular types of threats that maybe we see more of in Latin America than in other places or certain nuances to that threat?

Juan Carlos Garcia Caparros:

Yeah, one of the reality that we come in Latin America is that the security culture is probably lower than in other countries. Probably if we compare our security culture, our risk culture is less developed than we can see in the United States or in Europe. That's a big problem because many of the companies and the people are willing to take some risks and they are not really prepared to come from the criminals. I think that is a big difference from the rest of the other parts of the world. And the criminals are really wise and they're using that and taking advantage of things like the pandemic, the COVID. And the people are weaker than in other times because they're thinking in different things. They're not taking the enough care in order to avoid that.

So what we can see today is a big increment of malware, of course, but also direct attacks

through phishing that they're converted in ransomware and things like that. So that's the scene that we see. Almost every week we have a customer asking for help in order to resolve that kind of situations. And the situation here is that customers really they don't even know how well prepare in order to confront that kind of attacks. They don't know if there is some presence, if they're really prepared to respond. And of course, the maturity of the organization probably is not ready to confront this kind of very prepared cyber criminals. I think that's the main thing.

Ryan Goss:

Juan Carlos mentioned the COVID, one thing that we're seeing as well. And I think it's around the world. Obviously, the rapid digital transformation, but in Latin America in particular because their teams are so limited in terms of resources, they've really had to convert to doing just basic IT tasks in a lot of ways to facilitate this transformation, going all remote. And it's just taking away from their day-to-day. They already have limited cycles to be able to do their job and not become just a firefighters and putting out fires everywhere. It's gotten even harder now with this. So I've seen a greater increase in the need to automate, the need to really assess and really to have the information at their fingertips when they need it so.

Juan Carlos Garcia Caparros:

Yeah, and besides that increment in the attacks we face, that is [inaudible 00:06:33] mainly because it would require many companies to have more people connected with not really following all the best practices in order to be protected. They have to react very fast in order to have our business continuity. If you add that, the complexity of the cyber criminals, they collaborate. They work together in order to be more efficient and more effective in their attacks.

Also, there is another problem. The lack of skills in cybersecurity in Latin America is another problem. You'll see too many professionals that can be [inaudible 00:07:11] the companies. So the companies are requesting more and more services like the ones that we provide in order to resolve in a better way their problems.

Luke McNamara:

Yeah, so that's a point I'm curious of hearing more on. Because I think it's interesting to see in different regions where the skillset comes from. In some places like the United States, we see a lot that particularly on the cyber threat intel side, for example, that may come from government or the military. And so the skill sets that have built up over there in organizations like that, or the financial sector where they do have a lot of resources, then eventually transfer to other sectors and regions, maybe that's different for different skillsets and components. But historically, where do you typically see folks coming from? What sectors do folks typically come from that have very strong backgrounds in some of the core cybersecurity capabilities?

Ryan Goss:

Yeah, I would say it's probably not unlike any many things we see, even in the US it's mostly from the financial sector, government primarily. There's big industries and companies that take like a Coca-Cola or something like that. They're going to have a strong team and that's specific industry verticals where we see pockets of strength. And again, we focus primarily on those kind of customers, but where the most sophistication and the biggest budgets are by far is banking, finance and government.

Juan Carlos Garcia Caparros:

The other area where we can find that kind of skills or professionals probably, and this is more related to regulatory stuff, require for some companies that are on the regulatory requirements is for example, it's finance for sure. So we can get professionals from that. And also, there is some universities are trying to develop that kind of skills, but it still is limited. So, in one side we have the finance area, we have the of course, the consulting companies that they're developing their own skills. But still I think there is a big gap we do what is required and what we really have in the market.

Luke McNamara:

So with those threats, which again are not uncommon to what we see in the different regions with this background and expertise, kind of where that sits in different industries across the region. What are the problems that we typically see customers coming to us with? And maybe Ryan I'll start with you on this, what are they typically looking for when they're approaching us?

Ryan Goss:

Well, yeah. And that's a great question. I think there's been iterations of FireEye obviously. So, it's a very interesting dynamic of where we are right now, because we still have the loyal customer from way back that we had bought the original inline sandbox and stayed with us through all of our evolution. And we do have some customers that have nearly the entire suite and they've really taken advantage of services, but those are few and far between. So now as we go through our transformation and we have increased portfolio, not only on the solution side, but also within the consulting side. The reputation of FireEye in the past is always that we are very elite and expensive company both on our solutions as well as our services. And I think that perception has changed a little bit with the move to subscription and ARR.

So I think really the intelligence piece is really taking form, in my opinion. Our intel offer being one thing, but really the Helix Platform being that source of intelligence and really the differentiator for us. Inevitably, we find ourselves in, I would say, knife fights with one provider if it's an end point deal, then we're fighting all the end point providers. So we are trying to differentiate ourselves from the rest in terms of providing that intel as well. So I think that's taking form and that's the type of solutions that they're looking for.

Ryan Goss:

I'll let Juan Carlos talk more about the services, but from my perception on the services and that it hasn't necessarily changed in the time that I've been here. That CA's or the compromise assessments, it really one of our strengths, of course, and they really recognize us as a leader within that. So they come to us for that a lot. We're doing much better now with, for example, the IRR retainers. That we really understanding the value of that, and being able to have us on speed dial if you will. So there's a lot of just the... Back to what Juan Carlos said in terms of with the limited resources that customers have. Let's just take it if it's a Swift or something like that. They say, "Well, we need to make sure that we're okay within this protocol and this platform. Let's call Mandiant, because they're the best. So we're getting a lot of those as well. So I'll hand it over to Juan Carlos and he'll talk more about the services.

Juan Carlos Garcia Caparros:

The other thing that I think that the service that are going to feel better a customer, it will depend on what is the moment that is happening. And what I'm trying to say with that, if you're already compromised and you're being attacked or you have breach, the kind of services that are going to be required totally reactive. And we are calling here the services like the incident response services that we have. That is something that we can do it really well, we are probably one of the best in the world doing that. And the approaches get there, bring that team, understand the environment and try to help the customer in order to avoid further damage. Identify who is the attacker and be sure that the attacker is going to be out of their systems and their persistency is going to be something gone.

So that's probably the main service that we're recognized in the world. In the other hand, when there is not an attack, that there is a possibility that the organization is compromised or not. We have a certain kind of evaluation that we do in order to review first if the customer is compromised, if the customer is prepared to respond to that kind of attacks and try to define with them what is going to be their security posture. I think this is more in proactive side in order to help the customer to define what is the current state, what should be the future state and why they need to do in order to close that gap.

And we have other kinds of services in order to help the organization to transform, or to train or to create security culture in the organization. And also area of delivering or doing managed services. We have many other different services in order to manage their defense capabilities of the customer. Not just the monitoring, but also the detection, response and even the recovery in order to cover, they call it spectrum of recording that is required to get into cyber cybersecurity.

Luke McNamara:

One thing that I think we've seen a lot of this year with, in particular driven by the speed of ransomware attacks and the nature of how those have transformed really in 2020 is a lot of

organizations elevating the security discussion up into the C-suite into the boardroom in ways maybe they hadn't in the past.

I'm curious, in your description of organizations that are looking for that reactive response, and maybe weren't thinking as much about investing in security or that maybe being more constrained to the IT and security function rather than the larger discussion within the business and for the organizations that are thinking about this more proactively, have you seen a shift or a change where that conversation around security is being elevated more into the boardroom and how they're approaching it and how they want to think about it in the future?

Ryan Goss:

It's getting there. It has a very long way to go. And a lot of the discussions I have with everybody on the team is exactly around that. Back to my analogy, the knife fight, especially as we get into other solutions like intel and validation. If we're still at that operator level, it's going to be very difficult. So, I think that's one of the benefits of FireEye, Mandiant and the frontline intel that we have in the messaging that we are continuing to deliver at it really helps us get there. And a lot of the discussions we have, we don't initially don't get into bits and bytes and speeds and feeds and all that stuff that eventually you have to get to, but if you start getting there right away, it's going to be very tough. So as we talk about this transformation stuff, and really a good example, Juan Carlos has mentioned the regulation.

So in Brazil, the equivalent of the GDPR is LGPD and it's just as rigid. That regulation is driving investment that wasn't there before and the people that are on the line are the executive. So that's one clear cut example of it getting elevated. But again, the unique differentiator that we have, not only on the Mandiant side but on the intel side, when we can really provide that insight into that and not put it in the technical terms, just what is your risk? Are you exposed to risk or not? And can you prove what your risk level is? Can you show the board of directors and your bosses and the executives that the investments that have been made are in fact doing what they should be doing? That's not happening overnight.

Obviously, we are gaining much more traction along those lines in terms of getting not only to the CSO but above, but it's definitely a process and it all goes back to the level of maturity as well. And the maturity level of the companies where they think, "Okay well, security is just an after thought. You just have to be there to check the box without getting into too many details." It can even come down from a government, Juan Carlos is in Mexico. And unfortunately right now, the tendency from high above is to austerity plan and do everything as efficient as possible, as cheap as possible. And that obviously impacts security as well. And you're not going to have any level of high-level discussion necessarily when that's on the table.

So every country is different. Some are much more in tune like a Brazil because of LGPD versus what's going on in Mexico right now, but that obviously will change in a couple of years when things are fluid. But from our level, on a practitioner level, there's definitely much more interest on that executive level and above.

Luke McNamara:

We've talked about intel a couple of times here and sitting on the intel side, I would be remiss if I didn't ask a further question around that, which is, I think in my mind, one of the notable examples that we've historically seen of a set of threat actors doing activity in a particular region of a particular kind that maybe historically you wouldn't expect, would be some of the activity we saw from North Korean threat actors targeting financials throughout Latin America.

Ryan Goss:

Correct.

Luke McNamara:

And again, there's always a tendency for organizations, especially with limited resources, focus on the threat actors that are currently hitting my sector, currently active in my region. But I think that scenario goes to the point of if you're trying to think through potential risk, at least having some awareness of what the other threat actors out there are, who are carrying out global campaigns, what their capabilities look like and where there are those early warning signs of a threat and targeting.

When we think about how organizations in Latin America are approaching threat intelligence, situations like that, are those wake up calls to the value of threat intelligence, kind of an early warning system, or there's still much this focus on IOCs, tactical indicators and using those and the SOC use case contact.

Ryan Goss:

Yeah, I would say it's still a very tactical way to use it, unfortunately. There are the exceptions. We have customers that are very mature and they've invested not only in one intel solution, but maybe several. The challenge continues to be, it's still on the tactical side, how to make that intel much more actionable in real time with this level of employee that doesn't necessarily have all the knowledge like Juan Carlos was pointing to. And they're just very focused. They want to see, okay, are these, like you said, IOCs or if it's a bank, bins and is it that binary? Is it there or not? If it's not, then this solution is not valuable to me.

I think we've come a long way. It's not so cut and dry now. And they are understanding the value of understanding tendencies from other parts of the world and TTPs and all that type of stuff that can really give them early warning sign of, "Hey, we need to make some adjustments here because of what's going on." Connecting the dots. That is an ongoing process. I think the more that the other intel providers continue to enter into the market and they can see the differentiation, then that's when we become a much more interesting.

But it's frustrating because we can show beyond a reasonable doubt that we are very good intel solution, but with very limited budgets and very limited scope and how we're going to use

that intel, it's sometimes become difficult. But it's ongoing discussion and I would say every single year, more and more projects, there's more and more of the RFPs are much more in depth and the requirements are there. So I like where we are, but it's a huge growth area I should say for us. I don't know if you want to add anything Juan Carlos?

Juan Carlos Garcia Caparros:

Yeah, I will say that some intelligence for sure is one way to have a proactive approach in order to be ready to respond. But there is a situation that may complexes this because many of the organizations, they receive tons of information, tons of cyber intelligence. The problem and Ryan already mentioned is that it's not actionable. And that is because there is no context in that information. So is required to cover some additional filter in order to create a specific context for the organizations. Otherwise, it's too many information that is not easy to take decisions based on that.

The other thing is that the collaboration between the different organization doesn't occur. The banks, they don't speak each other, they don't share information. They're still in their islands of information. And it does one of the things that is required to happen as well as in the cybersecurity companies that we should share more information in order to collaborate. Of course, there're business situations that it doesn't allow that to happen very easily, but it's the only way because the criminals, the cyber criminals, they really collaborate between them. And for that reason, they're sometimes even more prepared than the good guys in order to response better. So contextual cyber intelligence is, for me, is the next step to follow.

Luke McNamara:

Two areas that come to mind in our discussion here with some of the things that you brought up. And I'm curious what you've seen to be the response level and interest from organizations in Latin America, training and validation, particularly maybe for some organizations that haven't historically invested as much in security. And so maybe there's a lot less security debts when it comes to figuring out what stuff they want to throw out and going through that process of looking at controls, what's working right? The whole validation context, but then also training, right? To address maybe some of those workforce shortages, where there is maybe a lack of expertise in certain areas. How are organizations thinking about those things?

Ryan Goss:

Yeah, I guess starting on the validation point. It's similar to what we talked about with the intel. If we go all the way back to the Verodin acquisition and then starting to talk about that and really starting to learn about what a bass is versus what legit differentiation in Verodin et cetera, and being able to evangelize that. And that's the word, it's a lot of evangelization at this point, because unfortunately those bass players arrive first. And so they set the table and this is what this looks like. And we just get bolt into that and it takes time. And we've been going through that process. We do have, again, going back to the level of maturity, those customers

that are truly in tune with what a true validation and all the use cases that we can provide and really just the level of granularity and detail that they can have is really impressive.

Now, it goes back sometimes to just checking the box and having a minimum like, "Hey, do you guys have some tool to check in the bass," providers are using the term validation as well, "Oh yeah, we got it." And so it becomes immediately a price exercise. And it's just that process of getting them to a point where, okay, they see the difference and now they have to budget for it.

And then to your second point, the training piece. That is an ongoing problem for them, because it happens a lot. They've invest all this time in training their people, getting them from a very low level, but smart people. When we say maturity level, not because of any level of intelligence or anything, it's just that the experience that they've had. So then they go and they bring them up, they get them ready to be solid contributor. And then

And so I think that's back to one thing is the education and the training piece, but the other is having a company like FireEye and Mandiant behind them to help them get their program level and the maturity level that Juan Carlos was talking about earlier is really important, but that training is definitely difficult. And there's also a lot of local companies that offer trending. So I wouldn't say that training is necessarily a big part of our portfolio, where we do have training is when it's part of a bigger deal and obviously, training specifically on our tuff, unless it's an engagement specifically to really lift the maturity level of the whole security program, including the employees and their skillset.

Juan Carlos Garcia Caparros:

Yeah, I would like to add that training is okay but if there is not objective that really matters is really we're objective of create cybersecurity culture based on risk. The training is something that it won't work because is going to only to pass a requirement or to pass a regulatory requirement. Training has to be focused on creating that cybersecurity culture and it has many different phases. And one of the faces that many companies forgot at the end is to pass that training. If that training it really make a difference, it really create that culture, that they can have a simulations of attacks and test how the people is going to react in and test if the recovery plan is really something that is going to work. So this has to do with service with the enterprise resiliency of the company.

So, because the question is not if you are going to be attack, the question is when is this is going to happen and the companies have to be ready to resolve that. Ready in the controls, ready in the processes, ready in the technology, but even most ready in the way that the people is going to react in order to be recovered from that attack. I think that's the main point of the training, not just to pass a regulatory requirement or a corporate requirement.

Luke McNamara:

That is an excellent point, having that divorced from a larger strategy around risk mitigation and the processes and controls and the expertise, and then the people component of what an organization has in the way to stand up against cyber threats, I think it's very important.

Wrapping up here. I'm curious what things that you would leave the audience with, things to look for as we go into 2021. Ryan you've mentioned for example, regulation and how that's had an impact or shaped how organizations are thinking about security. Obviously COVID-19, as hopefully we come out of that in 2021, knock on wood. There may be aspects of that where though Juan Carlos pointed early on, organizations have had to change ways that they've conducted business. And there may be continued evolutions around that that have security implications and that may drive certain security controls or processes. And there may be evolution that don't threat landscape. We may see new threat actors emerge from Latin America or target Latin America. So I'm curious what your thoughts and predictions are for 2021.

Ryan Goss:

Yeah, you mentioned actually a couple of them and it all ties into what we've been talking about throughout this as it relates to COVID and rapid acceleration of the digital transformation towards cloud. We've seen it in this COVID period within 2020 and it'll only get more and more as we go into 2021 as budgeting has focused on that transformation. So we'll see a lot of that and yeah, more and more regulations coming online. And I'd say just the model as we continue to talk about lack of resources.

So the MSSP requirements, our need to have strong MSSP partners, not only for us, but for the end users and how they buy in and really be able to outsource a lot of that stuff is really important for them. And I think for us as a company with our transformation, there's a lot on opportunity now and us going down market a little bit and really focusing more on that small to medium business where before it just wasn't viable for us, but now it is. And I think we're going to see a lot more action out of that small and medium to business. And of course, continuing on the top of the pyramid as well. So Juan Carlos?

Juan Carlos Garcia Caparros:

I will add that one thing that we can expect is to see more attacks. This is not going to finish very soon. The cyber criminals, they do the things with all the time. They can be preparing an attack for days, months even years in, and nobody can notice what is happening. They have all the time in the world in order to attack an organization. And for sure the COVID-19 pandemic helped the criminals in order to have more time without being noticed. So it is important that the company have the capabilities in order to detect, to response and recover at the same time, at the same level, at the same level of maturity as Ryan mentioned.

And the other thing is security is not a technical matter, is a business decision matter. The companies need to understand that is not just a technical thing, or is a matter of be careful about the data or things like that, but it goes beyond that. It can destroy completely. A company can destroy their reputation. It can take an organization out of business very easily, and that's why the security is not the responsibility of the SOC or the guy in IT, is a responsibility of every single person, every single executive with the organization. And the security should be in their DNA for sure, in order to not just to report, respond in what is required in the organization, but even in their own life. So I think that's the way that we need to see cybersecurity these days.

Luke McNamara:

Wise words to end this on. Gentlemen, thank you for your time. It's been a fantastic conversation, thank you both.

Ryan Goss:

Thank you.

Juan Carlos Garcia Caparros:

Thank you.