ATTACKIQ

Think Bad, Do Good Podcast
Episode 4: NEW FIN6 MITRE Emulation Plan

Jonathan (00:05): Jose Barajas, it's good to see you. Freshly haircut. You got your quarantine haircut, man.

Jose (00:15): I tried to cut it myself and I realized why I went to the barber.

Jonathan (00:25): You're lucky you got a good shaped head, man.

Jose (00:25): Yeah.

Jonathan (00:26): It's really good.

Jose (00:27): Yeah, if it was a little oblong it might not work out. But I think I pulled it off.

Jonathan (00:33): So my mom and I have a square head and the advice I've been given is not to shave my head. Yeah. You look good, man. You look good. It's good. You're very fortunate to be able to do a cut like that.

Okay. So this is not in fact, the quarantine barbershop podcast, as much as we maybe would want this to be. And it looks like I'm in a basement. So let me try and fix the lighting. Now I look like a CIA agent, but today, we're going to talk about... It's a very exciting day for AttackIQ. So for how long have you been working on this with the center for Threat-Informed Defense, Jose? How long has it been?

Jose (01:12): Well, since its inception. Since AttackIQ joined the CTID as a founding member, we've been involved every step of the way with them. So whenever that was, I guess. End of last year, beginning of this year? I don't even know since I've been locked at home this whole time.

Jonathan (01:31): Yes. Actually. We're in a time warp situation.

Jose (01:32): Yeah.

Jonathan (01:33): That's awesome.

Jose (01:35): I think it was earlier, I think earlier this year or maybe late last year, I forget the exact timing. So that's a little over six months. And as we're going to talk about today, right, quite a few projects are coming to fruition as part of that partnership. And well, that's what we're here for today. Right? So we'll talk that.

Jonathan (01:51): Yeah, yeah. Let me offer. So today, MITRE's Center for Threat-Informed Defense, MITRE is a nonprofit that operates in the public interest, a federally funded research and development center with whom AttackIQ is very closely partnered. And one of the organizations within MITRE that we work closely with is the Center for Threat-Informed Defense.

Jonathan (02:12): And today the exciting news is they've launched their first emulation plan focused on FIN6, which for those of you who don't trade in three letter acronyms followed by a number is a cybercriminal group that focuses on financial theft and a lot of ransomware, and more. So it's a big day just because of FIN6. FIN6 has been able to break into networks, steal data, conduct ransomware attacks quite a bit all over the world for the last few years. And this emulation plan will help security organizations put a stop to it.

Jonathan (02:48): So that's the one big defensive takeaway that we're going to talk about. But as Jose and I were indicating when we weren't talking about haircuts upfront, today's announcement is also a historic first. It's the first major research project that the Center for Threat-Informed Defense has put out around cybersecurity emulation plans. So for background on the center, it's a vital research organization that brings together some of the world's leading companies. And Jose will tell us more about that.

Jonathan (03:12): All concerned with cybersecurity. With MITRE's researchers, so you get some of the smartest national security, cyber security researchers in the United States, plus AttackIQ, and we're one of the founding members. And the goal is to crack hard security problems. And that's what the emulation plan does. And so we're super excited to have Jose here.

Jonathan (03:34): Jose was there for the first podcast that we did. And he affirmed for me how and why this is such a good idea, because he's so much fun to have on. He's a technical lead at AttackIQ. He's a malware researcher. He's just super smart. And he's been AttackIQ's rep to the Center for Threat-Informed Defense from the beginning. And he's also an amateur barber, obviously. So Jose tell us what is FIN6? Who are these guys and what are they about?

Jose (04:03): Yeah, so FIN6 is a group that has been followed by the industry. So obviously, MITRE's tracking them and others have been tracking them as well. And the reason why we have that three-letter acronym, FIN, is because they're known to actually target financial organizations. Some publicly have attributed to Russia. We go to MITRE that attribution that's steadily there.

Jose (04:27): But I think in general you can say that some of this behavior is being generated in that part of the world. And is definitely targeting, based on the threat reports that we analyzed, targeting financial organizations, target organizations with point of sales and web payment systems as well.

Jose (04:45): So what this really means is that if those types of systems are ones that you, as an organization, manage, or if you're a financial organization, this emulation plan and FIN6, I should say, is representative of things you should likely care about from a defense perspective.

Jonathan (05:04):
Yep. That's right. And in my research, Jose, it's, they're they're known as a criminal group, but they've not been attributed to any specific nation state. But they may be based in Russia.

Jose (05:13): Correct.

Jonathan (05:13): Exactly

Jose (05:13): Exactly. Yep. That is what I was hinting at.

Jonathan (05:15):
Right. Right, right. Right, right. Yeah. I learned this through open source research. There's not a lot of attribution around them, out there in the world.

Jose (05:22): Yeah. I think I've been hearing attribution since the beginning of my career and I mean, it's still a hard thing to do today. So I think at the end of the day, I mean, there's definitely some value in attribution, but at the end of the day, I think it's understanding these groups and what they typically do so that we can know where to focus on. I think is a more important part. At the end of the day, if it's Russia or some other country or part of the world, it really doesn't matter because if I'm a financial organization, these are the types of behaviors that should be focused on as my kinda feedback there.

Jonathan (06:01): Yeah. So let's get into that on the emulation plan. I think the interesting thing about attribution is that you tend to do it... Nation states tend to do it when they're trying to punish another nation state or when they're trying to punish a specific criminal group for a specific reason.

Jonathan (06:15): So for sanctions and building a case against them legally, that's part of the reason why. But if you're just trying to blunt their techniques and this is much more focused on techniques.

Jonathan (06:24): So Jose, tell us a little bit about the history of the CTID and who they are, who's in it?

Jose (06:30): Yeah. So along with AttackIQ as part of the founding members, we also have some nonprofits involved as well, such as the Center for Critical Security Controls. So CIS controls. Center for Internet Security, they're also involved as well. So it's really an initiative across the board, from industries, from technologies, to finance. Us being one of the few vendors that are involved to some even nonprofit organizations that help make the security industry better.

Jonathan (07:00):
Right. And then there's MITRE. Are the MITRE researchers actively involved as well?

Jose (07:02):
Oh absolutely. Yeah. MITRE is absolutely involved across the board in all projects. But yeah, these are some of the organizations that are working with us today on these projects.

Jonathan (07:15): So it's cool. It's major companies that should be concerned about cybersecurity for their own sake because they don't want to be attacked. And then people who research and think about threats. And then for us, a cybersecurity company that builds capability. So, it's a good mix.

Jose (07:28): Exactly.

Jonathan (07:28): Yeah.

Jose (07:30):
It makes across the board of, we talk about a little bit more about my involvement in the FIN6 emulation plans that are at the tactical level. I know we want to talk about that a little bit today.

Jonathan (07:39): Yeah. Let's do it.

Jose (07:41):
I can talk about how that played out in terms of areas of focus given what each and every one of us do.

Jonathan (07:50):
Yeah. What did you learn? What are some of your big takeaways from the process?

Jose (07:54): Yeah, so I think one of the big takeaways from the process is, first and foremost, is I think the way that the cybersecurity industry has matured has been amazing. And what I mean by that is, when I started my career maybe 14 years ago, no one wanted to share anything. Right. If I ask, "Hey, how'd you get hit by this or that? Or how did that work?" No one wanted to share anything. People thought, "Why am I going to tell you how the attacker is doing things?"

Jose (08:20): Because, now you can do them themselves. And I think we've reached this point where I mean, we should know what the attackers are doing. Let's just put it out there. They're going to figure it out anyways. They're sharing it amongst themselves. So it should be out there so that as defenders, we can understand things.

Jose (08:37): So I think first and foremost, the fact that this consortium MITRE group for the Center for Threat- Informed Defense put together, and even though it's technically a closed group, at least at the level of when we're directly doing the research. But I mean just the level of openness and sharing was one of the first pieces that to me was very striking. And I think just shows the degree of maturity that we have in the state of cybersecurity today. That in mind, we obviously have a long way to go, but I think initiatives such as this are going to help us get there.

Jonathan (9:09): That's awesome. That's really cool. I mean, when I first heard that AttackIQ was doing it, my eyes got wide and got really excited about it. So let's dig in a little bit into the emulation plan and on the website, we'll see some images and they'll be some links to the actual plan itself for the launch. But can you walk through a little bit of what is it intended to do and how does it help the cybersecurity community, overall?

Jose (9:33): Yeah. So, let me back up a little bit. So as part of the Center for the Threat-Informed Defense, one of the things that MITRE is doing is based on feedback from us and other organizations, they're sending out a set of research projects that we can subscribe to. So ourselves, and three others decided that FIN6 was an area of investment for us.

Jose (09:52): And we wanted to generate this emulation plan template. And that's still while we're talking today is, ourselves and three other organizations decided that creating an emulation plan around FIN6 was important, and that's really why we're here today.

Jose (10:09): Now for the FIN6 project, the objective was to create an emulation plan. That term emulation plan is going to be very, you've heard it before because MITRE actually did emulation plan for

APT3 and APT29.

Jose (10:39): So for those of you that are knowledgeable in that, the difference here is that this is something that we developed as part of our group and the objective of APT3 and APT29 was for MITRE to walk through, do the analysis and tell you, "This is what APT3 did. This is what APT29 did, and we've ran it against these vendors. Here are the results." Allowing you as a defender, as an informed defender, to take that context to make sure that you're same technology is doing, if not better at minimum, the same, that MITRE has done.

Jose (10:55): So now what we're doing is we're creating an emulation plan for FIN6. And while we're not going to run it against 12 different EDR vendors or however many MITRE selected as part of round one and round two. What we are going to produce is an analysis of what FIN6 has done based on publicly available threat intelligence.

Jose (11:14): So not some shadowy stuff that we can share and put out there in the world. Based on that information, we've distilled that down into the tactics, techniques, and procedures that FIN6 is known to execute and basically define these are the typical things that we observe when FIN6 is found within an organization.

Jose (11:32): So at a high level, what we've done is we've actually broken it down into phases. I won't get into this yet, but for FIN6, we did it in a phased approach where phase one was a collection and initial activity phase. And then phase two was a more pointed one. Right? Focus on targeting the POS, or maybe targeting a normal brick and mortar system. So, what that allows is that if I'm an analyst and I know I manage our POS systems, then I probably want to focus on that piece because it's probably going to target me as an example.

Jose (12:04): So that was an output. And the idea here is that as an analyst, I can go get this emulation plan from MITRE. I can read almost the cliff notes on what it means at a very detailed level, what attack techniques are involved? And how they actually play out over time assuming this bad actor was in my organization? As an analyst, I can now step-by-step recreate this behavior almost with a very simple cut and copy paste. Right. And recreate this behavior, so I can make sure that my environment is working effectively.

Jose (12:40): And just to finish, the objective here is not just to produce that, but this is going to be a template so that the entire MITRE community can use it as a basis to generate their own emulation plans and generate emulation plan for FIN7, FIN8, FIN9, FIN10. Those don't exist, by the way, I'm just joking. But right. The point is that the entire MITRE community can use this as a model to submit other emulation plans, so as a community, we can grow this knowledge base and get better together.

Jonathan (13:07):
That's interesting. I mean, is it kind of like the GitHub of emulation plans then?

Jose (13:11): Yeah, I think that's a good analogy to use. Right. I think it's going to become a library where you can go in and grab that emulation plan and what's great, it can either be ran step-by-step like I talked about, manually. One of the big pieces that was a requirement for this project is also to spit out a little JSON object, which means we can ingest that and do things in a programmatic fashion as well.

Jose (13:40): Obviously, here at AttackIQ, we're absolutely going to take advantage of that, given that we automate security testing with our platform today, but that also allows other organizations to pull that context into their process in a programmatic fashion as well. So it's not just a manual for doing an emulation plan, but it's also gives you those tools so that you can do things at that programmatic level, too.

Jonathan (14:04): Jose, you say JSON, but did you mean YAML?

Jose (14:07): I did mean YAML.

Jonathan (14:08): What's a YAML? What is a YAML?

Jose (14:11): A YAML is just a simple, human readable, a way of expressing data. So a lot of applications use the YAML format to transmit data amongst one another, might be one use case.

Jonathan (14:25): That's interesting. I mean, if I was to mention what a YAML is to my son, he would think it's an animal for a book or something. So this is the interface that the security operation, a security member would have when they're trying to use the emulation plan. Is that what that is?

Jose (14:40): Yeah. So if I wanted to take the emulation plant and put it into something like MITRE Caldera or and from our perspective, we want to grab that YAML file and have an AttackIQ generate and recreate this attacker behavior, that's exactly what it's there. Which is, provide all the context necessary to run the emulation finds.

Jonathan (14:48): Cool. And that will put something like that up on the website so that you can see it folks, so that you can actually have context for what Jose's talking about. Now what was it like? So MITRE would write one of these on the, would write an emulation plan on their own for APT3 or APT29. What was the experience like doing this as a group and what did you offer and what did you learn?

Jose (15:22): Yeah, so doing this as a group, I think was definitely a good experience for me personally. I definitely enjoyed getting into the weeds a little bit. And yeah, working with the MITRE team was amazing. The team there, you'll see the quality of the work, but the team there did an amazing job. And really from the objective of this project, we were able to... What was the question? Geez. Just lost my [crosstalk 00:15:22].

Jonathan (15:49): So funny. Jose shaves his head. We're not cutting this, they're keeping all this. He shaves his head and all of a sudden he can't think straight. So the longer my hair gets, the smarter I get, that should be the case. So we're talking about what it was like to work with the group. And I think the interesting thing is we built a cyber range. It was a virtual range in which folks could test the emulation plan. Is that right?

Jose (16:12): Yeah. So a big involvement, a big piece of involvement on our side. And what I did is we actually provided a cyber range for ourselves and other contributors to take the emulation plans and run through them. All right? So most of the organizations had taken the emulation plans and run them on their own environment, but this isn't just for us. This is for the entire community. So I was able to spin up a cyber range, which is basically made up of a simple recreation of a corporate environment.

Jose (16:42): Domain controller, we had a SIM and we also had a number of machines connected to that domain controller. So, that allowed us to have testing grounds. I was able to walk through it as a novice analyst trying to walk through these emulation plans. And it was just a space for myself and for the entire MITRE team involved in this project to really test on.

Jose (17:06): We use it to validate controls and configurations as part of our process internally. And it was something that we could share with the group, which was really cool. And I think they really appreciated that we were able to provide that and it really helped validate some of the pieces of the emulation plans that you see today.

Jonathan (17:21): That's awesome. And you're going to teach a class on how to do emulation planning going forward? Is that through AttackIQ Academy? Or how are you doing that?

Jose (17:29): I am. Yeah. So I think for, towards the end of this month, I'm going to finish this up. So we should see something up next month and I'm basically give a little Masterclass, which is going to walk you through how to develop your own emulation plans as well. So, from reading threat intel, converting that into MITRE TTPs, to actually generating the emulation plans, which is the outcome of this project.

Jonathan (17:54): That's awesome, man. That's really great. Well, here's an early advanced plug for Jose's emulation planning class. So sign up if you want to build an emulation plan and learn about that process because he's obviously, he's a researcher, but you've been doing this now with the CTID and it's pretty awesome. The one thing I want to make sure we talk about is the emulation plan for FIN6 was built out of the CTID process. But AttackIQ also has recently built counter ransomware capabilities into the security optimization platform in order to test.

Jonathan (18:29): If you're a hospital, if you're any organization in the world that's concerned about ransomware and we know hospitals are getting hit especially hard over the last few years, particularly under Coronavirus because they're more susceptible and more vulnerable, and doctors are more stressed, they just want to pay the ransomware. And we had Siobhan Gorman do a great webinar last week, which you can also see on our website about best practices for managing ransomware. But the security optimization platform has Ryuk. And what's the other one? Oh, I want to say Lady Gaga. That's not what it's called.

Jose (18:57): Yeah. Ryuk, most recently, WastedLocker. I mean, there's been so many just this year alone. But I think Ryuk and WastedLocker have been the bigger players, lately. We definitely have some earlier ransomware as well, but those are the ones that we've recently released in focus. And the objective there is the same as with the emulation plans to a certain degree.

Jose (19:18): Right? You have a ransomware strategy that we discussed last time on this podcast. Well, let's run that Ryuk, let's run that WastedLocker methodology. Let's make sure that that plan actually stands up as expected to this attacker behavior. So those are kind of things that we've put out there. Some of those do align with the same tactics that FIN6 did. But of course we cover some of the other areas, too.

Jonathan (19:47): Yeah. Yeah. That's great. Well, that's really cool, man. Congratulations for building this and working with the CTID on this. What are some of your hopes for the CTID going forward as we close out this podcast today?

Jose (20:01): Yeah. For the CTID going forward, I mean, I think there was a good amount of organizations that joined initially. I'm excited to see this grow and I expect other members to join, which means that other players in our industry can help contribute. And I mean, we have organizations, globally, contributing to this, so it's not just within the United States. So I think that's really exciting. I think what's also really exciting is we have a number of other projects that we've been involved in.

Jose (20:28): We'll talk about those at the appropriate time. But FIN6 is just a start and I can think of at least four other projects that we're involved in. Well, I should say just as a whole, we're involved in that, the next level of how those things are combined, put together, and help provide a joint set of capabilities.

Jose (20:51): I think I'm really excited for that as well. Right? These emulation plans are the first step towards that. But we're going to see a lot more output that, individually, is going to be very valuable for us. But when it's put together, it's going to have extreme value for us, not just at the analyst level, but organizationally. Right.

Jonathan (21:11): That's awesome. I mean, you can ultimately, as you can see on our solutions page on the website, www.attackiq.com, we've got all these different solutions that the security optimization platform provides as you deploy emulation plans and assessments against your security controls to reveal performance data about your technology and your teams and your processes.

Jonathan (21:33): And that obviously for a financial threat actor, for anyone who's trading financial information, point of sales, ransomware, anywhere there's money being transacted you want to pay attention to these kinds of groups that you know are going to come after you. But the ability to run emulations and do that is really a part of our process. And that's why we're building blueprints, which are step-by-step approaches for companies to figure out how to do this and how to get the most out of the security optimization platform.

Jonathan (22:08): Cool, Jose. Thank you, man. We got to do this more often. Yeah, [crosstalk 00:22:08] we got to do it more often.

Jose (22:09): This wasn't too hard. Yeah. We can definitely do this a little bit more.

Jonathan (22:15): To be clear. You're still being recorded. So this is your farewell to the community. As you lean back in your chair.

Jose (22:20): Oops. Bye community. This was great. I definitely enjoy these. We should definitely do it again. Yeah. Anytime, Jonathan. I'm here. Let me know.

Jonathan (22:31): Look at that face. How can you guys resist that face? We're going to come back for more Jose. Thanks, Jose. Really appreciate it, man. Yep, see you soon.

Jose (22:41): You're welcome. Take care.