Chris Salgado "On Streaming Services Hacking"

Leah Evert-Burks: This is Leah Evert-Burks with the Center for Anti-Counterfeiting and Product Protection @ Michigan State University and *this* is *Brand Protection Stories* - stories about the practice of brand protection by those who live it.

Leah Evert-Burks: This is Leah Evert-Burks with the Center for Anti-Counterfeiting and Product Protection @ Michigan State University and *this* is *Brand Protection Stories* - stories about the practice of brand protection by those who live it.

Leah Evert-Burks: In *Brand Protection Stories* we talk to those in the brand protection community about particular cases in their careers. Through some *stranger than fiction* real life scenarios we learn about the practice of brand protection and the challenges faced by brand-owners worldwide.

Chris Salgado: This guy was really good at what he did. He was an effective hacker and he ended up being, there's certain things I can't say about this - but he ended up being kind of a ring leader of a known group I'll say and so he knew what he was doing and I'd go so far as, say, he know hell of a lot more than I did, and we were just diligent with our efforts, and just in just looked over under every rock, you know, and just looked in every corner that we could in the Internet world, and just tried to uncover as much information as possible.

Leah Evert-Burks: Christopher Salgado is a security and investigations leader with more than 19 years in security, cyber and physical investigations. Throughout his career, he has assisted investigative and law firms, and several companies, including Fortune 500 companies, with the installation of numerous innovative and efficient processes in the topics of investigations, security, brand protection, threat management, business continuity, intelligence, operations, recruiting, customer service, employee morale and leadership. These companies cover the spectrum of industries, including social media, pharmaceutical, luxury brands, consumables, automotive, electronics, film production, streaming services, entertainment, and insurance. Chris also worked at Facebook as an investigator team lead. Situated on a global team, he assisted in managing investigations and operations and was instrumental in building the investigations division at Facebook. During this time, news about the notorious Cambridge Analytica scandal broke as did the allegations of Russians hacking the Facebook platform to intervene in 2016 US elections. As a global consultant Chris has presented to members of Europol, Interpol and the EU Commission on physical and cyber investigations. As an investigator, Chris has collectively conducted, managed and trained on tens of thousands of investigations, including: Cyber, Brand

Protection, Corporate, Criminal, Civil, and Surveillance. Chris graduated from Illinois Institute of Technology with a Bachelor of Science in Political Science and a minor in Psychology. In his spare time Chris is a contributing author to PI Magazine on cyber and social media investigations and a member of the London Speaker Bureau.

Leah Evert-Burks: Good morning Chris.

Chris Salgado: Good morning.

Leah Evert-Burks: How did we live before streaming? It's hard to quantify how important this form of at-home entertainment has become for us in particular in 2020, 21, 22, and beyond. With the pandemic came the shuttering of movie theaters and though now reopening consumption of media may have forever changed. Online streaming was the consumer's lifeline, also a financial lifeline for movie studios. So what happens when demand spikes for any goods or services - infringers move in. Such as the story, we will talk to Chris today about on the hacking of online streaming services. So, Chris, you have been an investigator for years, and have worked with numerous brands in a variety of industries, and as the audience has heard from your bio, you established the Facebook investigations division during an interesting time in that platform's history. Before we get into this case, regarding the hacking of a movie streaming service, can you touch a little bit on what your experience was at Facebook.

Chris Salgado: Yeah, yeah, thank you for having me. I appreciate it. So when I went to Facebook I was onboarded as a contractor, and I was tasked with helping the team. It wasn't just me though, I'm not a prodigy. It was a team of fantastic individuals, including my director and I was tasked with helping them stay their global investigations division and it was, I thought I knew social media and cyber investigations pre-Facebook. I didn't know social media or cyber investigations pre-Facebook. We learned a lot there. It was absolutely fantastic and I'm super grateful that they gave me the opportunity to do that and kind of spread my wings. They enjoyed what I had done for them, and they bought out my contracts, made me an FTE full-time employee at Facebook, itself. Gave me another roster of projects to help implement and oversee with them. And it was absolutely fantastic time and opportunity and time, because I was there when Cambridge Analytica broke. I was there when the the news really kind of fueled into the fire of the Russians hacking the platform for the US 2016 Presidential election. I was there post-election, but I was there when the fire really began on them, saying, hey or people saying, hey, what really happened here? So it's pretty critical time and help support a lot of different operations there, and, like, I said, staying-up new systems and implementing efficiencies in current ones. So we did uh, we cut our hands in a lot of different buckets. There's a lot that I can't say about what I did at Facebook but it was a absolutely fantastic time, and I'm absolutely humble that they give me the opportunity to do.

Leah Evert-Burks: Yeah, sounds fascinating.

Chris Salgado: It really was. It really was, both as the project itself and the opportunity itself. And again kind of multiplied by the timing of my entrance into Facebook, and the tenure that I had over there lots of stuff just kind of spiking up for us to engage upon.

Leah Evert-Burks: Right. Right. So, as I mentioned in my intro streaming really has become a lifeline for consumers. This case was an incident of hacking before the airing of a major film on a streaming platform. I think first it would be helpful if you could explain to the listeners what the world of hackers is like.

Chris Salgado: So it was, in regard to major content coming out I don't want to say film specifically, but it was major content. But yeah, I mean in a nutshell these days unfortunately, hacker has become hard and parcel with everyday life, right? Everything is onboarded into the digital media or digital life. And we as as individuals, even beyond consumers, just as persons.

We are forced upon the digital world if we weren't already engaged in that. Many of us,

I'll even go so far as say, most of us were. But even for those that have been engaging upon the digital world for years decades, even, you know, we find ourselves kind of being forced and doing more than we did before, plain and simple ordering groceries online. I remember when Pea Pod, you know, was around, and what the early 2000s something like that. And I thought no, that's I would never do that they had their flyers and stuff. I would never do that. But here we are today and I'm ordering groceries online.

Leah Evert-Burks: Right.

Chris Salgado: You know, beyond Amazon. It's hey, let me get some dragon fruit over here, you know. So yeah, we've been thrusted into a more regular version of us going online and engaging in whatever livelihood that we have with that and it was - so the hackers, the world has kind of developed a connotation of this underground murky area where it's just secret codes and secret passages, you know, knocks on special doors in an alley and then we open up into it like a cantina, and everyone's got a hacked laptop, or something like that, and I'm sure those exist across the globe. But it's become so popularized, popular, excuse me to really bring in everybody across the spectrum as far as demographics go. I mean you've got your white hat hackers, right? Those are the folks that hack for good reasons. You've got your black hat hackers, polar opposite, and then you've got your gray hat hackers those are the folks that really engage in hacking, and sometimes they do good, sometimes they don't do good, right, and they're kind of like, maybe even like bounty hunters. If you give me enough money, I'll help you out so. But again, the demographics on the hacker are really runs the gamut, I mean. There was the report that I was just reading, not too long ago issued by, I believe it was the - I apologize I can't remember what entity it was but it was a report that I was reading where one of them, very well-known hackers, hacking groups is led by a 16-year-old living with his mom. I mean, and this is a very effective hackers group so again you've got your and and we've come across with our cyber investigations for our

clients. We've come across instances where we've uncovered literally supposed white hat hackers enveloped with a really well-known cybersecurity firms, and they're honeymooning as black hat hackers. We've uncovered that in several episodes that we have engaged upon for our clients. So again, it really spans the spectrum as far as demographics. Regionally speaking, a lot of people think all the all the hackers are in Russia or China, and we do have some over there, but they're all over the place here in the US. And they're all over the place if you remember when Twitter got hacked. It was 2 years ago now, the head of that hacking group, and it was a very, very small group was a 17-year-old, actually here out of Florida. I'm in Florida. So you know it really runs the spectrum of regions, of demographics, of even skill set.

Leah Evert-Burks: So the hacker case that you were called upon Chris. You were retained to find this hacker where other investigators had failed to locate the perpetrator. What were some of the obstacles that you faced?

Chris Salgado: There were plenty, as you said we weren't the first firm engaging in the into, onto the situation. It was a pretty rough case, and I can't fault the other investigators, for really not being able to uncover what we ultimately did, because what it was was this this hacker, this person was tapping into the content database of one of our clients, and he would download the content, and he would release the content on his own private servers underground. But it was so much, even though we're talking underground it was so much that it was significantly impacting the bottom line of our client, because you kind of think underground, how much a percentage of those people kind of engaged kind of go that pathway. You do the cost analysis, as the client say - Okay, do we really need to engage this person or can we absorb that as a loss? Every company, does it. And the answer to that was absolutely. They need to engage on that person because of the large infiltration that he was developing on a routine basis. So we, in partnership with our client, we start off with very little information on the subject. You're talking like IP addresses, or IP address, username with a sanitized account. I mean very nothing to go on there. So, continuing to partnership with our client, we were able to identify the individual. But, that's I mean that's a great summary and watered-down version of what happened because we, this guy was really good at what he did. He was an effective hacker and he ended up being - there's certain things I can't say about this, but he ended up being kind of a ring leader of a known group I'll say and so he knew what he was doing and I'd go so far as, say, he know hell of a lot more than I did, and we were just diligent with our efforts, and just in just looked over under every rock, you know, and just looked in every corner that we could in the Internet world, and just tried to uncover as much information as possible. And this this individual just let loose on numerous red herrings in case anybody was trying to identify who he was. He knew he was, he was doing something that wasn't really on the up and up. So you dropped a lot of red herrings, a lot of dead ends. He put up a lot of different obstacles and it wasn't just him. He was involved,

like, I said, in a group and he got his kind of cronies, and that group to really support him, IN various ways, and they multiplied his effect. They dropped red herrings. They dropped dead ends as well. They even turn the corners and kind of set up their enemy hacker groups to take the fall. So you thought you were chasing one person, and you turn on you say oh, it's actually not, Mr. John, it's Mr. Jake and it's not Mr. Jake, Mr. John wants you think that.

Leah Evert-Burks: So it led you to false leads. And it's it's interesting what you were saying just a few minutes ago about the range of hackers out there. So you know, typically in in criminal investigations, you could maybe profile the criminal. But here it's such a variety of society, that that's sounds like that is pretty difficult to do. Then what you just said that the hackers are supportive of each other. And then led you down paths to point to enemies of theirs. That's a lot to figure out.

Chris Salgado: It is, it was, it was not an easy case. I'm very grateful at the clients for having one, come to us and say hey we think you can do this because I looking at I was like I'm not sure if we can but we'll give it a shot right and and we did, and again in strong partnership with our client, we were able to develop a slew of information and then we had to carve out what information is misinformation - very popular topic these days, right, and then what information is legit information, and some folks don't really realize that misinformation is still information so it's still helpful to you even if it's to say hey, well, let's negate that attitude or that pathway because it's misinformation, even that's helpful. And you have to investigate the misinformation to kind of identify if it's plain misinformation and again that's still a telltale sign that, hey, that information is null and void to what you're trying to seek, it's still information. However, if you chase down that misinformation you might develop who you're author is because usually misinformation is published by an anonymous author, or even if says you know, John Doe online through a Reddit group, or something like that. You possibly can learn why they're doing it like I said you can identify. Oh, it seems that this author of this misinformation post is an enemy of my subject, right? So then you can understand, okay, what other nexus points can I develop from this? And again, misinformation is still information. It still can become key, or at least helpful, to your investigation.

Leah Evert-Burks: Yeah, I think that's a really important point to to talk about to really bring to light, because I think many times when people run into misinformation, they dismiss it. But it really is a way of figuring out what, what path you need to go on. Interesting that, Chris, that you mentioned, that this hacker threw up a number of red herrings. Can you outline what some of those were, or mentioned what some of those were?

Chris Salgado: Absolutely, so quite a few of them. Like I said this guy was really good at what he did he would use multiple usernames. So let's say, for instance, this is just an example, well, let's say that he had a Reddit account. Well, he would multiply that by 10 he would have 10 different Reddit accounts.

He′d cross genders, so he would say his Reddit account was John Doe. He would cross genders and say I′m also Jane Smith. He would also deploy multiple shared usernames. So in that same hypothetical and this is a hypothetical, in that same hypothetical of 10 usernames – I'm just saying Reddit is the popular forum out there. He would have his cronies in his hacker group use those same usernames. So you'd go ahead and you′d identify this context and you would develop an understanding what wording this person uses, your subject. You would develop an understanding of what their perspective is on a couple of things because this you gotta keep in mind this is a pretty lengthy investigation and then all of a sudden it would do a 180 an absolute 180 in context. So you still have the same username, Jane Doe or, Jane Smith, whatever it was, the same username pumping out, most of it very different ideology, very different wording from what it did and you′re like, doesn't sound like the same person. And sure enough, you dig even more and you identify that multiple individuals using the same username that too, is specifically set up to throw off investigators to throw off anybody that′s on the chase, because you either walk away at best confused, or you realize, Okay, you know what that might not be our guy or our gal right and you throw it off the the perspective investigation, which is very dangerous because you give off that information that otherwise could be pertinent to your investigation. And he would even have this, this actually did happen. He would even have his cronies set up different username accounts to bash him. Then you would think, okay, well, that person′s against them that′s part of the enemy. Oh, it′s the same person it′s all an amalgamation of misinformation, and it′s not easy to uncover, you have to really delve into it′s a lengthy investigation, but when you′ve got a client as we did, suffering the losses as they were - you really have to pull out all the tools and resources that you have to really dig into the situation. I can′t, this was a very challenging case but I′m very happy with the results of it. But those are the types of red herrings that he put up. The other misinformation, red herrings he put up, he had fake LinkedIn accounts. We knew that this individual had 2 lives. This individual had a professional life, and this individual had a hacker life, and he did a really good job of keeping a one-arm's distance between the 2. Our job was to identify who this was. We knew a name. We knew a username, and then we developed the hacker name. This hacker name was pretty popular and we still didn′t know who that was. So we had to draw that nexus point between the username to their realize that the person′s real identity. Well, with having the latter, a real identity, as we all do in this world. No matter what you do online, you have a real identity. We have LinkedIn accounts, a lot of us do. He did as well, and he had several of them, though, several of them, and he one of them he had, it was his account but when you delve into further, he had a photo of I I can say he had a photo of an African-American male as the profile photo, our subject was not African American so it threw us off a little bit, but the content of that gave us more information. To continue to chase down our subject now, if we stopped there because of that red herring we wouldn′t

have picked up that additional information. So again, he just really used a lot of different resources to throw off investigators.

Leah Evert-Burks: So you mentioned that he lived a double life, and in his professional life. What was his profession?

Chris Salgado: So I can say that I can say that he's an engineer at a very well-known company in the United States. I apologize, I'm not trying to dodge it but part of this is still open.

Leah Evert-Burks: I understand, I understand.

Chris Salgado: So I got a careful with that.

Leah Evert-Burks: Double lives. When you look at criminal networks, once uncovered, many times people are surprised by the individuals involved, a teenager living in their parents' basement, an engineer with a professional life in a legitimate company, but yet they are involved in criminal activity - activity where they believe they can stay hidden and undetected. The web provides that cover, whether hacking and selling stolen streaming content or physical counterfeit goods online.

Leah Evert-Burks: And I think Chris, you have mentioned that in your investigations you used what's called spider maps. Can you explain what those are?

Chris Salgado: So I'm a visual guy. So in my reports I like to employ icons. I like to employ graphs, pictures because I absorb better when it comes to that and I frankly don't like to deliver report to my client, or an update to my client, that has them guessing - Chris I read what you said what you wrote, but when you mean I don't understand, right, I don't like to give them that guesswork. So because this issue was convoluted, we ended up unwrapping an entire operation of individuals, not just our individual, our subject that we were looking for immediately. We unwrapped operation of at least 10 people in the group, and all of them were very skilled.

So it was, and with all this misinformation is red herrings, I mean, if you can imagine I'm just giving you a brief, brief thumbnail sketch of this, if you can imagine it got pretty convoluted

pretty quickly. So what I deployed again being a visual guy trying to not have the client guess at what I'm trying to say and really understand the situation as best as possible was I deployed a spider map because I felt the number of bad actors that we were engaging in we had to really identify who they were, what their nexus points were, what their roles were inside the operation. What, alias, aliases, were attributed to this person. Person A, or 1 through 10 I'll say and how those nexus points developed between each one. It was, it was, I can't say enough it was a pretty confusing situation. So we drew out a spider map that would really detail everyone's nexus points, whether it was a social media connection or an address connection, or they went to the same school or they worked at the same place 5 years ago.

Leah Evert-Burks: So, finding nexus.

Chris Salgado: Absolutely a 100%, and while our mission first was to really carve out the identity of the one subject, it just blew up in our faces because we had to understand we got an entire operation before us. Sure, he was the person with his fingerprints on what he had done, but he had a whole team supporting him, so we then had to open up our aperture of the investigation and understand how these bad actors and some of them were very key players in the in the process and the operation how they all fit together very, very key. And then, obviously, the client would be able to kind of take a step back, assess the entire operation through a macro view of it and say, Okay, we want to engage this person civilly. We want to I engage in this person criminally, kind of really identify what ducks they want to, or you know what arsenal they want to kind of unleash on each individual.

Leah Evert-Burks: Okay, and ultimately this hacker made a mistake. Can you walk us through the mistake that they made that enabled you to identify the hacker and be able to report to your client and to the legal authorities who this was?

Chris Salgado: Sure yeah, he, I'm absolutely thrilled that he made a mistake because It doesn't matter what your role is at your work. It doesn't matter what you do as a hobby, it doesn't matter what you do as a you know in life, we're all boiled down to being human and humans make mistakes and we certainly capitalized on this one and he was, I can't say enough I've said a few times. I need to say it again. He was very good at what he did. It was very, he was...

He was very careful with what he put out there with his online breadcrumbs and intentional misleading breadcrumbs as well. But lo and behold, we were searching the deep web and this was weeks out into this investigation. We're searching the deep web and we came across a document. It was a PDF document that was uploads to a very hidden website. It was actually a membership form for this individual, the subject of ours to start up an online account for another streaming service, and he put his real information in there. He put his real credit card information there, and he tied his hacker name to his real name. That was the one document, almost literal, smoking gun in the cyber world. That said, Chris, this is your guy, and then we had the ancillary information to really strengthen that. But yeah, he made a mistake, and we're able to capitalize it, and I don't want to water it down saying that, hey? We found it right I mean it's a a hell of a lot of effort, a lengthy amount of time and a lot of fortitude to really be able to capitalize, one identify that and capitalize or really understand what we're looking at because I kind of summed it up that wasn't that it wasn't that pretty as far as PDF here's your subject here's his real identity, but nonetheless that's how really close the door on that chapter and we really confirm who that person was.

Leah Evert-Burks: Yeah, it's so interesting like you said that that even the most sophisticated criminals are human. And you had to just kind of wait for that human mistake to happen and be paying attention on you know, multiple levels to just wait it out because eventually we all make mistakes. It

sounds so surprising, though, when you outline it, because hearing how sophisticated this hacker was, how he used his hacker community to throw off all the trails. And then, for him to make this mistake is, is surprising.

Chris Salgado: It absolutely was, when when I came across the, the document and I decoded what it had say, because it wasn't that black and white where PDF says here's your guy - I kind of had to take step back from the terminal from my computer and say, is this legit? Is that more misinformation? This is done by his enemy hacker group, right?

Leah Evert-Burks: Right?

Chris Salgado: It's just to your point it seemed too good to believe but again you take a step back from that perspective, and you realize doesn't matter what you do, CEO of a company you're an it super specialist it doesn't matter we're all human. We all make mistakes and this was his mistake, and I was in awe of it. But I was also thrilled to have that in my lap. So very much was a client.

Leah Evert-Burks: So, Chris, how long from beginning of the assignment to discovering this mistake, and being able to identify the hacker, how much time passed?

Chris Salgado: So it was a pretty lengthy investigation, a cyber investigation, right? There's surveillances out there there's physical investigations that extend when we we have a case that's over 2 years ongoing right now so. But as far as a cybergist here's your directive chase this person down; it was pretty lengthy. We were involved with it for about 6 to 8 weeks. Might not sound like a lot, but when you're sitting in front of your computer chasing somebody down for hours and hours per day, 6 to 8 weeks is a stretch. And again, it was justified because of how good this guy was, and not only him but his team of individuals that supported him. And this guy, I might add, he was absolutely narcissistic. He was very full of himself and I, and you could see that you could gather that from his writings from his, the way he led his team as well. And then, from the way that other people talked about him, both his peers and his enemies. And I like to think that this guy, maybe with this misstep of his. Maybe he dropped his guard because he figured he didn't have to have it up all the time. Just a speculation on my part. But this guy we had a evidence, piece after evidence, piece detail, and this guy was very full of himself, very narcissistic.

Leah Evert-Burks: Yeah, yeah, ego gets in the way.

Chris Salgado: Yeah, yeah, exactly. And it can put it can bring you down.

Leah Evert-Burks: Yeah. yeah, absolutely. Well, very interesting, and a world that I that I'm sure many of the listeners have not heard a lot about so very interesting investigation. So in thinking about this hacker case, Chris, if you could select one word to describe the case or the experience, what would that one word be?

Chris Salgado: Well to me, I guess the obvious word would be to to me challenging. But I also want to kind of bring in the word exciting too, because chasing somebody down, I apologize,

I've said this so many times, but chasing somebody down of this magnitude, with his skill set, with his stature in the hacker community, was exciting, certainly in my mind dangerous. But it was exciting, because we were trying to keep up with this guy and his cyber fortitude, skill set, know we had to match that as best as we could, and that was, in my opinion, very exciting.
It was absolutely challenging so I'll stick with challenging at first and drop in exciting if you asked me the same question twice.

Leah Evert-Burks: All right. That sounds good. Well, again, thank you, Chris, for walking us through this case, and thank you for doing the hard work.

Chris Salgado: Yeah, I appreciate it. Thank you for having me I definitely appreciate it and it's good to kind of talk about these instances to give the education out there of what can be done even when it's somebody that's pretty rough to chase down. You just gotta make sure that you deploy the right resources and have the patience to get from point A to point B.

Leah Evert-Burks: And don't stop and wait for that mistake.

Chris Salgado: Right, right exactly.

Leah Evert-Burks: Yeah OK, great, thank you Chris.

Chris Salgado: You're welcome, thank you Leah.

Leah Evert-Burks: I'm not sure if it should cause comfort or distress to hear about the human mistake the hacker made, because we are all human, and we all make mistakes. But also a human trait, persistence and good ol' fashioned grit and determination helped find this criminal and in that, I find much comfort. Chris displayed those attributes in tracking down this hacker and preserving the value and rightful ownership of creative content.

Leah Evert-Burks: If you're interested in sponsoring episodes of Brand Protection Stories, please contact A-CAPP Assistant Director Kari Kammel at kkammel@msu.edu.

Leah Evert-Burks: I first met my next guest, attorney Deborah Greaves when she was working to protect the iconic True Religion Jeans brand. Maybe more than any other product group, fashion brands can shoot to the top in meteoric speed, and within a short period of time one become the most coveted of items; requiring that brand protection teams match protection to the brand's acceleration. As you will hear, not only was the True Religion brand counterfeited widely, it was also the target of cargo theft, hijacking and even internal theft schemes to divert product. All in a brand protection professionals days' work. Join us.

Leah Evert-Burks: Thanks for joining us today for this edition of *Brand Protection Stories*, produced by the Center for Anti-Counterfeiting and Product Protection (or A-CAPP) @ Michigan State University in East Lansing, MI. Please visit us @ a-capp.msu.edu. A-CAPP is a non-profit organization founded in 2009. It is the first and only academic body focusing upon the complex global issues of anti-

counterfeiting and product protection of all products, across all industries, in all markets. In addition to this series, we offer certificate courses in brand protection, applied education and academic courses, executive education, student internships, live summits and virtual events, ground-breaking research, and publish the quarterly digital industry journal, *The Brand Protection Professional*.

Leah Evert-Burks: This is Leah Evert-Burks with A-CAPP. Until our next session, keep protecting your brands, and the world's consumers. Keep it real.