UNAUTHORIZED ACCESS
DARK WEB MONITORING
KAMRAN SALOUR, SADIA MIRZA
GUEST: KEITH WOJCIESZEK, KROLL
JUNE 3, 2022

[KAMRAN SALOUR]

Hello and welcome to Unauthorized Access: An Inside Look At Incident Response. My name is Kamran Salour and I'm joined by my co-host, Sadia Mirza, and today we are in our Philadelphia office, we have just completed a three-day stint at the Net Diligence Conference and we are very excited and fortunate to be joined by our good friend and all-around fantastic individual Keith Wojcieszek and today we are delighted to have Keith with us. And Keith is gonna talk to us about what he does at Kroll and he's gonna talk to us about dark web monitoring and some misconceptions about dark web monitoring and some instances where dark web monitoring will be important. And I think these are gonna be instances where you may not consider using dark web monitoring. Keith, thank you so much for coming today and joining us on our podcast.

[KEITH WOJCIESZAK]

Well, Kamran and Sadia, thanks so much for having me. It's really an honor to be here. Show number 001, following Net Diligence 2022. You know coming back from COVID it's been really nice to actually meet in person and have these meetings with everybody to really discover what's going on in cyber because it's just not easy doing over Zoom or Teams or Webex anymore. It's really nice to be in person. So, thank you for having me today.

[SADIA MIRZA]

Okay, so now you can tell us, you can tell us about what you do and we'll take it and then there's like a thousand different ways we can go from there. I know we have like, we're keeping 20-25 minutes, but let's see, I know there's a lot to unpack.

[KEITH]

I started Kroll about 5 years ago when I founded the cyber threat intelligence program. And really the overall goal for something, a program like that is to provide intel not only to internal Kroll but other partners, such as Troutman, and just, anyone that works alongside us because threat intelligence really leads investigations. And if you're in a silo, you're not sharing, you're not learning. So, it's really about sharing and getting in and becoming a group and understanding what is going on and throughout the threat landscape. So, Kroll and the cyber threat intelligence team, we are really expert at dark web investigations and strategic collections, ready to identify any type of malicious activity. Again, been here about 5 years at Kroll. Prior to that, I had a pretty fortunate career. I started off with the U.S. Secret Service where, honestly it's funny because I never really wanted to get too much involved in cyber security. You know, you join the Service you think, you are a protection guy, you're gonna

protect the President of the United States. And lo and behold, one of my bosses said to me, "Hey what do you think about cyber forensics?" I'm like, sure why not. I'm always up for a challenge. So, you know, I had some background in it, but I did some forensics and just went through my career and, lots of people don't know this, but the Secret Service started because in 1865 they were combatting one-third of the country's currency was counterfeit. So they were creating a financial infrastructure. Keep it safe, keep the currency safe and so with that, with those responsibilities, the Service devolved this really good cyber program and a forensics program in alliance with the other agencies. So I got involved with that and I did a lot of forensics when it came to case work. Did a lot of child exploitation, which again is weird, Secret Service we really get involved with that, trying to protect children. And then I really found a niche when it comes to intelligence and while, you know, doing my time in the Service, I did all types of different things. But, one of the main things I really enjoyed doing was looking up bad guys that would effectively hurt the financial infrastructure of the U.S. I'm a servant of the public, I want to do good, I want to make sure everything is good for the people to come in and feel comfortable with their finances, with credit cards, using credit cards, so I did what I could. And my concentration during this time on the cyber threat intel team was looking at Eastern European block. Primarily Russia, Moldova, Ukraine. I'm really getting familiar with those attackers and the culture itself. Because you really, you really need to know who your adversaries are and, not just know, but intimately know, because I think, again, Kamran you said this earlier, a misconception of dark web monitoring. I think there's a misconception overall about these attackers.

[KAMRAN]

Keith, could you talk even at a, just at a very high level when we're talking about threat intelligence. I think a lot of people just think of the quintessential you know hacker in the hooded sweatshirt in the dark room plugging away on a screen with green numbers going vertically and that's sort of the attacker and that's who you're targeting. But obviously there's much more to it than that. And you talked a little bit about, know they enemy as a tenant. Could you talk more broadly about threat intelligence in general and then we can focus in more on what it is you do and how you can utilize threat intelligence in the IR world.

[KEITH]

You know, you made a really good point there. They're not. These attackers we're dealing with every day, they're not the hooded sweatshirt, I mean they may have a hooded sweatshirt, who knows. But the last guy I arrested was a rocket scientist. And you know, opportunity is what they're looking for. And threat intelligence, like I said earlier, threat intelligence leads investigations, it really helps investigations bolster to find out what happened? How do we avoid these gaps in the future? Are there challenges that we weren't aware of? And whether it's a technical intelligence, a strategic intelligence, whatever approach you take to this, any information that turns into intelligence and actionable can really bolster one's security. As we see, today's threat landscape is constantly changing. Now what we're seeing is a lot of these phishing, and I know a lot of people say, "Oh well I'm protected by phishing, I have x, y and z in place; it's gonna help me." It may. It really may slow them down, but it only helps if you're username or password aren't being sold on the internet. Multifactor authentication. Great, it's awesome. It's very, very good. There are

good things about it, but there's vulnerabilities in multifactor authentication as well. So, although you have multifactor authentication, there's also a separate process to make sure it's actually a good way to ward off actors. There's certain types of multifactor, whether it's being a code being sent, you know those push notification used to get, have you ever, like your Apple phones. Right. How many times do you say, sign in to a new device and I get a push notification. Do you authorize this, yes. If you got those, like you got ten of those in one minute, at some point you're like I'm just sick of this and I'm just gonna push yes. There's, the threat landscape it's always changing and it's because, there's several reasons for it. Cyber insurance. That's changing the threat landscape. Because now the policies are requiring such a robust approach to really keeping their infrastructure safe and their protocols safe. And their safety features safe and everything they have. Because of that, the threat actors have to get better or they have to figure a way, okay, if insurance is really requiring all these security features or all these protocols, how am I gonna get by it. So they have to regroup and figure out how they're gonna attack. So everything's changing, it's all different angles that are really adding value to where kinda it's response is going. Where these threat actors are going.

[SADIA]

So, Keith can I ask you a question because this comes up in a lot of IR calls right. And I'm just gonna be talking generally and it might seem like a ridiculous question to people in the industry, but when people say the dark web, what is it that we're actually referring to? Can I get on the dark web? Should I get on the dark web? What am I gonna see there? Like, can you break it down for us, just for anyone who doesn't really know.

[KEITH]

The dark web is coined phrase really just from industry. There's access and there's levels of access that you need to obtain in order to get to certain locations. It could be a website that's encrypted by an encryption key that you need in order to get in. There's forums, there's different things. Now, a lot of these threat actors have gone away from the forum just because, I mean, the U.S. government and, actually, governments worldwide have done amazing job in taking down some of these high-level forums. But yeah, it's just the location on the internet and you just need to know how to get to. There's a prime example. Just happened. Raid Farms. Raid Farms just taken down and that's not necessarily considered a dark web, it was a forum that was open to everyone. You could get on it on your regular computer. But there's other areas that take levels of security in order to get on it, you have to have certain keys, you have to have certain VPN clients. And you have to get on through that way. So it's access to different locations that are not governed per se, by any type of regulation.

[SADIA]

Why do we want to look at them? What's happening on there? Like, whoa, what do we see if we get there?

[KEITH]

Well, so there's marketplaces that you can really just buy anything you want. Literally, anything. The one's that you know, concentrating on that I have in the past, know a lot of the financial data. You can buy healthcare information, you can buy personal identifiable information, credit card data. Anything that is monetizing. So, we're looking at, when we do dark web and we're looking at monitoring, we're looking at incidence of where we can benefit a company, we're looking for data being sold, information being sold. So it's any information that's of value and it changes. It really does. 2010 was very heavy with having credit cards. Can you still buy them, of course you can buy credit cards now. But there's different things, I mean, you see Bitcoin Wallets being sold. And they're just all different things that you can pretty much buy, you just need where to go and how to buy. And you can navigate there at some point.

[SADIA]

Okay, so taking us back to IR, like what type of attacks did the dark, like the real benefit. Like when does an insured or client need to engage for dark web monitoring? Or even if, is it sounds like it's more than monitoring, but when's the right time and what's the benefit we're gonna get out of it.

[KEITH]

It should be part of the basic investigation. Is it monitoring? It could be. Right, it could be looking for data. But it also could be utilized as this tool to tell the story. You know, understanding those five things in an investigation. When did they gain access? How did they gain access? What did they do while they were in there? Did they remove anything, was anything extracted? Is the threat contained? So as you're looking at those five pillars, are you answering those, are you doing everything you can to make sure those questions are answered correctly and, you know, that's the approach. That's the approach Kroll does. That's the approach our team does. And we'll do everything we can to make sure we answer those questions for the client.

[SADIA]

Honestly, that's great. Because I think a lot, I think most people thing about dark web monitoring just in the sense of seeing what data was leaked. But in terms of like notification obligations, right. Like seeing if there is, if any of your data has been leaked out on the dark web. It seems like there's so much more to that. But you know, I wanted to ask you, cause from the legal side of things, you know, this comes up a lot. And I think you guys have a solution to this too, and so maybe you can talk a little bit about the approach, like the keys, the search terms that you use because, I know Keith, you and me have worked matters, right, where consumers are complaining that they're information has been exposed and trying to tie it back to a particular incident, and so we were just the search for like, if somebody went and searched for SADIA MIRZA and her social, right, you probably will find it somewhere I'm assuming. You know, I'm assuming it's out there somewhere. But, you're not, I'm never gonna know which incident it was leaked from. It's probably been compromised several

thousand, you know, hopefully not, but several times, right? And so from that point it opened up a can of worms. Like where, you can't point to a particular company or organization or a particular breach but I think that what you're talking about it's a little bit different. You're not trying, you know, it's not one particular consumer's information. Maybe you craft search terms specific to an organization and their domain and you search things along those lines, maybe that's a little bit more fruitful if you're adding it to a component of the investigation. Is that, is that, are you following my line of thinking here?

[KEITH]

Yeah, no I, right with you yeah. And you mentioned that how do you determine that this particular either fraud activity or something happened, and I see this on this marketplace, how do I determine. There are ways, but it's just not easy, right. So unless a threat actor said hey I got this from this hack I did. Are you gonna see that, you're not gonna see that. I mean you could potentially cross-reference the time frame, but it's so hard because looking at the real picture here, your email has been compromised. You have a Yahoo of email accounts. What people don't understand is, how much sensitive data you have in your email. Tax returns, health appointments, you know nowadays everything's online right. You're getting emails for everything. So all of this data that is just so rich in personal identifiable information. You know, you're all, everyone's worried about the file server. Oh, I have all my data here. It probably has everything plus more in your email account. And when the email breaches occur, how can you pinpoint one particular incident that your data is being exposed on the, on any kind of marketplace when you're victim of maybe ten different breaches that you utilized that email and password because, you know, it's easier for me to keep the same password for all my accounts. When I'm breached by one, you know, I'm exposing my email and next thing you know they're in my email account. I mean I may not know it, but they're taking data, so it's very difficult to say that this one breach occurred and this one time my identifiers were exposed were because of this one breach. I mean, unless the threat actor is specifically saying I took that, this is how I took it and I know Sadia that, that I took your stuff.

[SADIA]

They have to link it together for you essentially?

[KEITH]

Yeah. Yeah. There are possibilities and a lot of, I think more at a government level, undercover operations and doing like search warrants and other court ordered documents tasks that are provided that a little bit easier, but still, it's still very challenging.

[SADIA]

This whole conversation has been enlightening. We do incident response day in and day out and I think there's still a lot of, I mean, it was very helpful to me, because I think I've always thought about this in that context to of just, what's been leaked. So if you base it really when you don't have the logs, you don't have the information that you need to conduct a real

investigation, is that the right time or is there additional moments too where it just needs to be added as a component? What do you think?

[KEITH]

So, you know, it's tough. Because you're battling with not only, it's scary. I mean, like the dark web. People are scared, they're scared of what they're potentially going to find. We may find something that may not be good, but wouldn't it be better that we find it and fix it so it's not something down the road? But there's also risks with that too, right. So the timing is difficult. I think it should be a part of the investigation. And it's because I'm in it all the time, right. I think it could benefit every investigation, but there is definitely certain circumstances where it may not be the best choice. But again, it's something that you need to weigh in on where the investigation is going. BEC, are you doing a business email compromise? Do we need to know, I mean that would be good to find out credentials. Why not just pull, use that domain, is there any other credentials being sold or was this just a single affect. So there's all different types of scenarios that you can bring it in on. It's really kind of the maturity of the team that's doing the investigation as well as the risk tolerance of the clients.

[SADIA]

So what about outside of investigations. Like, I'm assuming, it must be very mature client, like you have to be pretty far along in your information security program to just add this as a component of your security programs. You have clients doing that?

[KEITH]

We do. We do. You know, it is. So, yeah, there is a maturity level for sure. But think about this. The status quo of those that are getting attacked. I'll say that again, the status quo are getting attacked. So, what are you doing to better yourself? Are you developing a plan, not only an incident response plan, but a plan that will grow your cyber security maturity as you grow as a business. Dark web monitoring is good. You have dark web monitoring, you're looking for key words, whatever. But I think there's a better component to that. Because you have, maybe do an internal pen test or a vulnerability asset. Again, that is key. I think those are the case you want to harden your environment. And when you want to add in dark web monitoring, it needs to be more than just monitoring. You need to take a look, step back, it's not just monitoring for terms, but it's, okay I have Citrix, I have Manage Engine, I have Exchange. I need to know from not only from a pen-testing standpoint or a proactive standpoint, I need to know from anyone, if anyone goes out there and sees what's going on, am I vulnerable. And that should be part of this dark web monitoring. Is not only testing your terms and your key words but understanding your network. Understanding your environment to provide intelligence back to you that if something does have a zero-day vulnerability or something does have something that's attacked, that your threat intelligence team, whether it's internal or you're leasing from somebody or you're in a partnership with somebody, is on it and they understand it. And they're not just monitoring for terms, but they're monitoring for your environment. I think that's the key component to a mature and understanding the risks of a business. That's gonna be key. That's gonna be how you're gonna defeat these bad guys.

[SADIA]

That makes a lot of sense to me and I know Keith we're running out of time, but one final last question. So last night when someone happens to lose their blazer with their wallet in it and I connected them with threat intelligence to track it down until the wee hours of the morning. Were you impressed, or no?

[KEITH]

So I was. I was extremely impressed both by you and Kamran. With the dedication and the way you approached it. You were a true investigator and had an unbelievable outcome.

[SADIA]

Well Keith, thank you, thank you so much. We had, it was a rough start I know. Thank you so much for bearing with us right now, for the last two days. It was, Net D was great because you were there with us. So we really appreciate you coming on this trip with us.

[KEITH]

Thank you. And really good luck with this, you guys are phenomenal and really gonna add some really good insight to cyber security here in the future. So, thank you so much for having me on today.

[KAMRAN]

Keith, thank you so much. I certainly learned a lot about dark web monitoring and how to incorporate it in more investigations and when it's gonna show a lot of value and once again Keith, any conversation I have with you, I come away feeling humbled, but you're so gracious and with your time and your information. And I always learn a lot from you and today's been no different. So thank you so much Keith. We're really delighted to have you as our first guest and hopefully this is the first of many sessions that we can have together because it's always gonna be wonderful. So thank you again, very much.

[KEITH]

Thank you, Kamran. I appreciate it.