STRENGTH IN NUMBERS

9/3/2019

Brian Contos: Welcome to the Cybersecurity Effectiveness podcast, sponsored by Verodin. The Verodin Security Instrumentation Platform is the only business platform for security that helps you manage, measure, improve, and communicate security effectiveness. I'm your host Brian Contos, and we've got a really special guest today. Joining me is Jon Inns. Welcome to the podcast, Jon.

Jon Inns: Hi, Brian. Thank you for having me.

Brian Contos: So, Jon, can we start off by just getting a little bit of background on who you are and what you do?

Jon Inns: Sure. My name is Jon Inns, and I am currently the CEO of a company in the UK called Threat Status, or Threat Status, I guess, depending on which side of the water you're from. I guess as a bit of background about me. So, I started getting into information security early-2000s, and I was actually working in the government in the UK at the time. The role just enabled me to kind of move into an InfoSec position. So, I did that for a number of years, about seven years, I think I worked for the UK government. Then, during my journey, I came across a piece of technology called ArcSight, which I know you have a bit of background in there too, Brian. I just really liked the technology at the time, and actually, the whole subject of data became very interesting to me and proactive monetary became very interesting to me.

Jon Inns: So, I joined ArcSight, had a number of roles with them doing consulting, sales engineering. I actually ended up looking after UK government. I know, Brian, you and I did more than one trip overseas to AMIR and the Middle East and had a couple of beers on the way, which was great. Then, when ArcSight was acquired by Hewlett Packard, I think that was in 2012, something like that, I set up a business on my own. So, we were focused on really SIEM. We were SIEM specialists trying to make SIEM systems work better for people.

Jon Inns: We did that for a number of years. That was subsequently acquired by an MSSP called Accumuli. So, I worked for those guys for a few years, running product development and sales engineering. That was subsequently acquired again by company called NCC Group where, again, I was director of product for those guys for a couple of years. Then, I decided really we wanted to get back to the grassroots and focus on a specific problem area. So that's kind of when we set up the Threat Status.

Brian Contos: Yeah. You know, the first time I met you, Jon, and knowing your background and what you did with the government, I got to tell you, I was a little disappointed because I had these visions in my head that you'd be picking me up in an Aston Martin. There was no Aston Martin. In fact, we spent most of the time on the tube, so a bit of a let down there. But besides that–

Jon Inns: The Black Hawk was in the shop as well.

Brian Contos: – I think our last project together, we were in Stockholm, Sweden, I believe, doing a project for the Swedish police. So, yeah, we've been all over together. Well, it's a pleasure to have you on this podcast, and I know you've got a lot of really interesting things to share. So, let's just jump in because I know a lot of your focus is on data breaches and your team over there in the UK, you guys spend a lot of time monitoring, analyzing data breaches as part of your day job. Can you give us a little bit of background on the landscape as you're seeing it at this moment, and what kind of volumes are we talking about?

Jon Inns: Exactly. I mean, we decided some time ago that, at 1,000 foot, there was just an interesting sort of development with the volume of data breaches that were going on on the internet. So, if we look back, I guess a year ago, 18 months ago, we would see a data breach of some significant size, I would say once every three or four weeks. People know about some of the big ones like Yahoo, who by the sounds of things, lost everything. There was TK... What do you call it? One of the big retailers out in the U.S. Anyway. So, there was a big breach once every three or four weeks that would make the news. The rampart of breaches is just getting worse and worse and worse. So literally in the last 30 days, we've probably seen double-digit major breaches.

Jon Inns: Again, you've seen on the news like Marriott, Dell, Quora. These are literally in the last 30 days. So, to give you an idea of volume, I mean, we're currently tracking well over 11,000 individual data breaches from across the internet. To kind of break that down a bit more, there's well in excess of 10 billion credential pairs in amongst those data sets. I should add, that's probably now well in excess of 11 billion credential pairs because it's probably gone up a billion in the last 30 days just from those breaches that I've just mentioned.

Jon Inns: So, the volumes of data are kind of mind-blowing. We think of those 11 billion credential pairs, at least 20% of them are from corporate domains. So, there'll be corporate emails and password pairs. You know, you are talking billions of corporate credentials. The interesting thing about this is actually as these compromises are going on, it's not just the site that's getting compromised that's suffering; they're leaking data into a data pool that's already massive and it's just getting bigger and bigger and bigger. So, this data pool, as it's kind of swelling from all these new breaches, it's just becoming more and more

material that somebody else can use to compromise a different organization or a different site.

Jon Inns: So, the trajectory is phenomenal. Really, I think it's kind of a big statement to make. But at the moment, it really feels like kind of the internet is broken at the moment, Brian. It's prolific, it's going on so frequently. As I say, the data that's being lost is just being weaponized against other organizations. So, every time somebody loses something, the problem just gets bigger for everybody else.

Brian Contos: Yeah. It's beginning to get to the point where it's almost easier to list organizations that haven't suffered a breach.

Jon Inns: That's right.

Brian Contos: Yeah. There's obviously a tremendous amount of data and you said potentially up to 11 billion credential pairs, which is staggering. But even so, where do you go about finding this data? Where's it being traded?

Jon Inns: We use a mix of techniques to kind of find this stuff. So, we use both technology and people. We can use technology to scrape this data, and we find it in all sorts of places. The paysites are rife. There's more and more paysites popping up every day, and there's kind of data turning up on those. But a lot of that data is just regurgitated data from somewhere else, so it just does the rounds over and over. So, we use people, predominantly, to get the best results really.

Jon Inns: They spend a lot of time on the forums and on the dark web. Actually, I know the dark web's kind of this ethereal thing, but it's actually quite a resource-intensive thing to stay on top of it. Because only about 20% of the sites on the dark web are kind of persistent, really. Most of them kind of disappear and then spin up again in a different form or a different factor. So, we spend a lot of time and we have a lot of people working on those sites, building up personas and things like that so we can kind of get that information from them. The paysites are probably the least interesting, I guess, of those data sources.

Brian Contos: You know, so here's a question I've always had about that type of data. You know, say I'm a nefarious individual and I want to get some credit card information, some Gold Card numbers, and expiration dates, and things like that to do some Christmas shopping, how do I know that the data that I'm looking at is legitimate given that the people that I'm getting it from are also nefarious individuals? How do I know it's not just fabricated? "Here. Here's 100 Gold Card numbers." But maybe those were already sold off a year ago, or maybe they're just completely false. How's that separation done?

Jon Inns: So, there's some really funny stuff about that. So, if we talk about, like, creds, for example. Creds are very frequently fabricated. So, there is no honor amongst

thieves. These guys will rip each other off every day if they get the opportunity. So, things like creds, they will just try and pass off old data as new data. Say that they've compromised the new site when they [haven't], it's just something that's been robbed from somewhere else. In those kinds of situations, we do a whole bunch of stuff on it. So, we try and fingerprint the file. We'll walk halfway down a file and then we'll look for a record and a known point, and then we'll do that on every other file that we ever see. So, we can kind of take fingerprints from the files to make sure that they look unique.

Jon Inns: Actually, there's some other information in there like, "Is the password unique on every single record, or actually are there some commonality?" There's lots of things in the data that we can kind of do to try and identify whether or not it looks legitimate. But actually, particularly on the credit card stuff, again, it would be funny if it wasn't sad. Because what we see is these guys will sell credit cards, but they'll actually give a warranty with them. So, they'll literally go, "Hey, Brian, do you want to buy this credit card? You can have a $15 for the number. It's good. And if it's not good, I'll actually give you your money back." So then you kind of get… Yeah. It's a good deal if you're a crook. But then what somebody will do is they'll buy that credit card, they'll use it, and then they'll publish the actual number on another forum, and say, "Hey, everybody, go smash this credit card." Then, they'll get all of their buddies to go buy stuff, get the credit card locked out, and then the guy that originally bought it will go back to the guy that sold it to him and say, "This is a dud, give me my money back." They're literally scamming each other while they're using these stolen cards and things like that. So, it is a dog-eat-dog world out there. Yeah.

Brian Contos: The scammers scamming the scammers. Who would have guessed? Maybe it's obvious, but can you explain a bit about the data, how is it typically used by the criminal? What are some of their more common use cases?

Jon Inns: Again, we're really honed in and fascinated by creds at the moment, so valid credentials that can be monetized in one way or another. The first obvious one is that they're just trying to brute force sites. So, if they can get thousands, or hundreds of thousands, or millions of creds, then they can either sweep the net. They just push them into every login page that they can possibly find. Or, they'll do a targeted attack, and they'll actually try and compromise a specific application. But we see a lot of these guys build things called combo lists, they're aggregated lists of breach data that have come from multiple different sites. Then they'll just try and actually push them through a single site. So, they'll pick a target on the internet, and then they'll take all of these creds...

Jon Inns: As I say, every time there's a breach, the material pool just gets topped up again. So there's more data that they can kind of go at to re-monetize. So, they'll create a big combo of valid or known usernames, passwords, and they'll pick a site on the internet and then they'll just try and push all of those creds into it.

The ones that validate, they'll then hide of those off and then they'll resell them again and say, "Hey, I've got 200 valid accounts for this particular company, who wants to buy them at $50 each?" Because I know that they're working, for example.

Jon Inns: So, they can kind of use it for both kind of scattergun approach and actually very targeted approach. Again, quite often, we'll see that if they can validate the creds, they won't use them themselves. They'll just sell them on again because they'll have more monetary value to somebody else than it does to them. We also see them using it for the classic fraud stuff. If they can get onto a site, they can buy some e-goods or something like that. Then, they can take those e-goods off, sell them off on eBay.

Jon Inns: One of the kind of the big things I think it just went worldwide, probably about two months ago now, is these email scams that you see which sort of say, "Hey, you've be looking at our material, and I know you have because I have your password and here I can prove it." We've seen that have kind of all sorts of different impacts on people actually. It's the most trivial kind of scam. But actually, we've seen some real consequences from that. So, we've seen people deleting years of photographs of their laptops and things like that of their children because they're terrified that people have actually got access to their laptop and things like that.

Jon Inns: I think those things have been moderately effective in monetizing that, but I think it's been incredibly effective at terrorizing an awful lot of people. But the big one that everyone wants is account takeover. So actually, if I can get valid creds into your Office 365, then frankly, I can do whatever I want at this point. So, I can pretend to be your finance director, and I can tell you to send money somewhere else. I can start emailing my suppliers and tell them to pay two different accounts. Now, this all sounds kind of unlikely, but we actually are seeing it time and time again. I think this kind of plays into Verodin space as well actually. If you have all of this great security technology, how do you know is going to do anything for you in certain situations? So, the account takeover is the main prize, I think.

Brian Contos: Yeah. I'm curious on price. So, let's say, again, I'm that nefarious user. I had already gotten my credit card, I did some holiday shopping, now I'm ready to get some work done. I'd like to get some credentials for company X. Could I just go out there and say, "Hey, guys, anybody have credentials for company X?" What would be my process, and about how much would I be looking to pay for something like that?

Jon Inns: Yeah. Both of that thing. So actually, in some cases, the lists will literally be put up for sale. So that someone will say, "Hey, I've got 200 known working accounts for this particular company, and you can buy the entire list off of me

for $500 or something like that." Or actually, if you wanted a targeted account, then you could sort of say, "Yeah. Has anyone got a valid set of creds for this particular organization?" Quite often, you'll see somebody offering to do that for... it varies between $500 and two and a half thousand dollars to get you a valid set of creds for that.

Jon Inns: The ones that kind of get the premiums... So, when they see working pairs of creds for something like payments@company.com or marketing@company.com, those more generic accounts or are more highly prized because they know that they're shared amongst multiple people and they're probably going to yield some pretty interesting access.

Brian Contos: That's a good point. Well, let's talk a little bit about encryption then. A lot of companies today, hopefully, most but I know it's not all, are encrypting their data. You're often seeing press releases going out saying, "Hey there. Yeah, we had a data breach, but the data is encrypted. So, your risk level isn't as high as if it wasn't." What's your take on that?

Jon Inns: Yeah. Again, this is a really interesting one because... So sometimes, the data is encrypted and that's great. Obviously, if they're hashing their passwords and things like that in the applications, you can kind of take some kind of solace from that. But there's multiple interesting things about this in that actually everybody knows that we use passwords on multiple sites. It's a terrible habit but everyone does it. Now, some of these small sites actually, you could be an important person who's just using a very small forum. So again, we see forums around engineering, forums around legal advice, those kinds of things. These are forums that are set up just to help people, their hobby sites, things like that.

Jon Inns: But then, people subscribed to these. Again, they're using their corporate email to subscribe to them, and these things have almost no security so they're running a real old WordPress, or they're running a vBulletin, or something like that. Invariably, they never have any encryption, or they're really poorly implemented, or they're very weak encryption. So, actually, those can get compromised, and it almost undermines everything else because actually if you're using the same creds on those weak ones as you are and some of the solid ones, then it kind of doesn't matter. You've been blown anyway.

Jon Inns: But on some of the more sophisticated ones, they will be employing hashing. If they're good, they'll be salting their hash and things like that. We can see that improving over time. But what we're also seeing, again, is that bad guys, they're pooling their resources. So, actually there are numerous sites now where if you are able to kind of get an extracted data dump and the data's encrypted or hashed, then you can upload that to a shared site and loads of people will work on the problem with you. So, they'll donate compute time, they'll effectively

become part of a cracking team that will just sit there and try and auto smash these encryptions or these hashes.

Jon Inns: So, while a company might get compromised and they may well go public, exactly like you said, and say, "You know what? We had a breach, but it was all encrypted." That's very much a statement in time. So that may have been true at the moment that they got compromised. But we're very often we're seeing that shortly after that, people are going to work on it and they're starting to decrypt the hashes or reverse the hashes. It's a very dangerous thing because people take assurances that if the data's been masked or is hashed, then there's nothing to worry about. But very often, we see people going to work on cracking that almost immediately.

Brian Contos: Yeah. Honestly, if you do any research on rainbow tables and people using these monster machines just stacked with video cards and just kind of going after these things, it's—

Jon Inns: And they even run competitions amongst themselves, who's got the best cracking rig? So, they all take the problem and see who can reverse them fastest. Again, it's a bit of a e-sport, almost.

Brian Contos: Encryption's one piece of it. The other piece you hear people touting as one of the mechanisms people should use as a single sign-on. You know, Facebook, and LinkedIn, and Google, and many, many others offer this. From your perspectives, does this lower that risk? Does this increase the risk? What's your view on single sign-on?

Jon Inns: Well, it really depends on your perspective. I mean, single sign-on is super convenient. So obviously, the less times I have to log in with my password, the better, right? That's a user's perspective on things. So, people will willingly use their Facebook creds to log into all sorts of different things. But again, if you kind of just step back and think about what you're doing for a couple of minutes... Again, we see this both on the corporate side and the personal side, people reuse their passwords. So, I can be ceo@companyx.com, I use my corporate email to join some little vBulletin forum that I just want to get a bit of legal advice on. So, I create an account. Are you going to use the same password as you use everywhere else? Because I have bad password practices. That little vBulletin site gets compromised. Invariably, that password is probably going to work on my personal email, my Facebook account, something like that.

Jon Inns: So actually, the minute that becomes true, then again, all of my Facebook security's gone. If I'm SSO-ing, if I'm single sign-on-ing through my Facebook creds to multiple other sites, then actually, again, the whole thing just splinters into pieces really. So, it's just fascinating that just the smallest failure in a little corner of the internet can have this kind of rippling effect that kind of comes

right the way back into my corporate life and some of the sites that I depend on to run my business.

Brian Contos: Yeah. I mean, that's a great perspective. There is no silver bullet, right?

Jon Inns: Right.

Brian Contos: People say, "Oh, we interact our data. We leverage single sign-on." Yes. All our good things, all best practices, but it doesn't stave off all risk, that's for sure. Well, what advice can you give people that are trying to avoid these types of issues?

Jon Inns: Yeah. Again, I go back to my first statement, I think, which is it really does feel like the Internet's broken right now. The biggest companies in the world are getting compromised and they're losing data. So I think whoever you are, whether you're a corporate user, or personal use, or whatever, you really have to kind of keep that in the back of your mind at all time and just assume, "That if I create an account anywhere..." Passwords are supposed to be secrets. Just assume that they're not going to be secrets. Because if an account gets compromised and I can see your password, I don't only get to see your password, I get to see your whole thought process.

Jon Inns: If you're starting to use football players and I can see two of your passwords and you're using two different football players from the same team, I then know about you. I know the way that you're thinking. If you turn around and say, "I'm using a unique password on every site." And you're using LinkedIn123 on your LinkedIn site, and I can see that. Then, obviously, eBay123 is on your eBay site. I can see that. I now know your thought process, and I now have every opportunity to try and compromise your accounts.

Jon Inns: So, you kind of really need to think about that every time you're creating accounts on any application on the internet now. Just assume that that data's going to be seen. If you've obviously got the option, then 2FA is the way to go or multi-factor authentication. You know, we're desperately trying to educate people all the time about using unique passwords on different applications and using password managers and things like that. But I think it's now important that you do proactively monitor these breaches and see if it's going to affect you in some way.

Jon Inns: Because, as I say, just because you have an account on a site, that's not the only place that it's going to have an impact. So, I think you really need to start kind of keeping an eye on these data spills and asking yourself whether you're a part of it. But ultimately, never use the same creds across different sites because they are going to hurt. They're going to cause you a problem.

Brian Contos: What I'm hearing is using my password Messi123 for everything is probably not a great idea. But it makes sense that you want to keep track of these sites that monitor these breaches, just like you have credit card monitoring services, just like you monitor other things. You want to monitor your creds and see if you've shown up anywhere. I know there's a lot of ways to address that. That's great advice, Jon. Hey, Jon, as we wrap up here, there's a question we like to ask everybody that we interview on the show. And that's, who is your favorite superhero or super villain, and why?

Jon Inns: That's a good one. Can I have two?

Brian Contos: Sure, go ahead.

Jon Inns: So, I think a number one is got to be Deadpool, I guess. I just think that dude is kind of funny. You know, nobody's perfect and you can't please everybody all the time. So, I just like his kind of carry on regardless approach. Clearly, I don't endorse his actions, but he tries to do the right things and he stays positive. So, I've got to applaud him for that. I guess the other one is Harley Quinn. You know, what's not to like?

Brian Contos: Very cool, very cool. Well, we've had Deadpool a couple times. We haven't had Harley Quinn, so I'm glad to hear that we have a new one on the show. You know, I always wondered why there wasn't some kind of British superhero that some radioactive experiment during WWII at Bletchley Park and now he lives in Leeds off of the remains of people's fish and chips meals. I don't know. There's a lot of room there for superheroes.

Jon Inns: James Bond seems to be getting more and more superpowers every time I watch a new movie.

Brian Contos: Awesome. Well, thanks so much, Jon. And thanks to our listeners for joining and be sure to check out other Cybersecurity Effectiveness podcasts sponsored by Verodin.