FEDERAL TECH PODCAST

Ep.28 Can Knowledge of the Criminal Underground help Protect Federal Agencies?

Tue, 9/20 8:31AM • 27:02

SUMMARY KEYWORDS

identity, joel, credentials, breach, password, criminal, identification, area, information, years, attribution, data, federal, security, behavior, trust, access, people, organizations, mission

00:03
Hear that Joel? Okay, testimony. So we're gonna do this toss back and forth than a pause than a regular opener. Okay.

Welcome to the federal Tech Talk. Welcome to the federal tech podcast. My name is John Gilroy and I'll be your moderator. Today, we're going to talk to a company called spy cloud based in Austin, Texas. And we're gonna get an individual by the name of Joel Bagnold. We're gonna talk about some ways that this company collects information to help increase security for the federal government. But before we begin, there are probably a lot of people who know your background, Joel, maybe you can tell us about your background and why you're so uniquely qualified to be in this position.

01:15
Thank you, John. It's a pleasure to be here today talking with you. I started my career in 1986 After I graduated from West Point as an infantry officer, then spent the next 20 years in the US Army and special mission units. And in some policy positions on 911. I was actually independent on when the plane hit the building. And I just completed a study of asymmetric warfare, which was curiously coincidental. I found myself about one month later over at the White House working on the new established Homeland Security Council, as a policy director working Incident Management and threats. From there, I stayed at the White House for the next seven and a half years, retired, my military commission took on a presidential commission and served in various positions during the Bush 43 presidential administration. Both sold him Homeland Security and Counterterrorism. And when I left during the transition from President Bush, President Obama, I moved to Austin, Texas, and I've been focused on cybersecurity, commercial and federal, for the past 14 years.

02:25
Why can summarize it pretty quickly? You know, you've seen it from the trenches to the White House, I mean, you have the range that very few of my guests have. That's an incredible range, isn't it?

02:34
It's been a wonderful experience. And I've had the opportunity to see how government operates at the state and the federal level, and also the cross section of state capabilities and commercial capabilities and the cybersecurity industry, which needs a lot more work in terms of cooperation and collaboration to make it more effective. But there is a growing sense of urgency in the United States to ensure that our very best that we have to offer as a nation is being used by critical infrastructure, federal government, state and local governments and commercial industry to create the best kinds of protection and security possible.

03:14
I'm going to state the obvious you have obviously worked with some three letter organizations, and you are privy to information that you're not gonna talk about. And it's kind of interesting that with your background, you have chosen to work with spycloud. And then when I see someone like you, constantly choosing spy code, I'm thinking well, it's gotta be a reason for it. Maybe this is bang for the buck, this is very good value. Everyone talks about value today ensure investment. And so what kind of value can spycloud Bring for the federal customer

03:48
Spycoud is a big data analytics company that operates in the dark web, the deepest parts of Dark Web where we acquire information very early, right after a breach is taking place. And we have early warning access to enormous amount of PII or personally identifiable information. And we operate at the intersection of human identity and IT infrastructure. So we're very effective about attribution, and helping to find the malicious actors that are operating in the criminal underground, whether it's nation state sponsored or whether it's strictly financially or criminal motivated for nefarious purposes. We have about a third of the world's population now in our database, and we have high efficacy of accuracy and identifying bad actors on the web. So we provide attribution information, we provide criminal behavior of information we provide, most importantly, a pattern of life or pattern of behavior analysis to federal agencies, so they can support their emissions with this with this data and achieve successful mission outcomes.

05:05
I went to your website this morning spy icloud.com wealth of information. I think if you're listening to this, and there's snow on the ground and you want to learn more, I downloaded the 2022 identity exposure report. And then my jaw hit the ground back up, and I said, I don't believe these numbers. I just, I mean, you know, just come on now. I mean, I mean, if you read the numbers in this report, 200 billion recaptured assets. I mean, Joel and his team, they are searching the dark web for assets and information that I don't think people I can't believe the amount of information it's It's shocking.

05:46
It is unbelievable that we've been able to amass 200 billion assets over the past six years. And what's really interesting now that we've established ourselves and as an expert in this identity, enriched identity, area of expertise, we are now acquiring about a billion new records a month. And it's just fascinating how well our engineering team has put together a rather complex collection mechanism, that then we can parse into

searchable fields, we curate the data in a way that makes it very easy for any user to understand. And then we analyze the information so that queries against our data lake achieve very strong results in the areas that you're interested and trying to support your mission to the federal customer. And then we further enrich the analysis by providing a feedback loop between the federal customer, their use cases, and how we can better and richer data to help them achieve successful mission outcomes quicker. So a lot of words there. But we have have a relationship now with the intelligence community and Department of Defense and several law enforcement agencies for a number of years that have given us the ability to put domain expertise, subject matter expertise into our algorithms and analytical products that help the government better achieve understanding who's doing the bad thing on the web.

07:21
When you are at West Point, I'm sure you studied wars through the centuries, maybe even wars in the Middle Ages, Middle Ages had these castles and these moats, and they can pretty much establish a perimeter pretty easily. Some people say today that identity is no perimeter, there is no moat, there's no wall, there's no firewall. And so if identity is the new perimeter, being accurate with identification seems to be a good first step towards the this whole this big concept of zero trust, isn't it?

07:52
It really is. Attribution has been one of the top three cybersecurity mission requirements. Since we stood up the cybersecurity organizations in the federal government over 15 years ago, so if you look at US Cyber Command, and then the intelligence community agencies that are focused on cyber and then the new agency at department, homeland security that's helped Osiris reconstruct screen analysis is unbelievable, where we're attribution and the identification of infrastructure associated with human identity has achieved an apex now, and it's one of the most important elements of, of mission requirements for Trudeau Government. And we are right in the sweet spot of that.

08:41
We know just a little bit about your background, but you've been involved in heavy high level areas of legislation and recommendation policy. And so I don't normally go into the policy area, but you're just a perfect person to talk about policy because he gets this practical background too. So if you look at the policy legislation coming up, we see initiatives we see this we see that, are there challenges or gaps, you see that maybe they aren't covering in some of these increased reports about, for example, data management and about identity management moved to zero trust are the gaps there, and there's reports coming

09:16
out. We have made so much progress in the past couple of years and the new executive order on cybersecurity. They came out of the White House about a year ago, some of the new standards that have been published through NIST and also through the Department of Defense's cnmc program, new changes in identity management, the whole zero trust framework that's that's been implemented, being implemented now by the federal government have all done a great job of ensuring that we're moving in a very positive direction more quickly with regard to security practices and also enduring policies that will make a difference and our ability to

prevent the bad thing from happening. We've been in recent osmand for quite some time and shoring up our protections, but now we're starting to transition from as a whole government really from responding effectively to preventing the bad things are happening in the first place. And so in that regard, some of these new policies are making a very positive impact, the notion of continuous monitoring, for example, and treating identity as a critical element of understanding the threat landscape, very, very important. Those have all done a great job of ensuring that we're doing a better job of securing our human as well as our digital and network assets. That's Dorsten remaining gaps, we still do not have security culture set so that every individual that's operating on network are just thinking about operational security in their own personal behavior associated with their mission organization. 24/7, this needs to be ingrained in the culture and, and that is an area where there's still a need for improvement. There are some things we can do automatically, though, to help with that challenge with that hygiene challenge. And then more spycloud focuses its time and effort is ensuring that password usage is strong. And that if a password is being used in an environment that we can quickly identify that that is a stolen or lost or missing credential associated with that person's identity that it needs to be changed immediately so that we can ensure that it's not being taken advantage of by malicious actors.

11:30
You mentioned zero trust. I'm sure if you went to Google Trends and typed in zero trust, you'd see, you know, big ramp up, it's being debated in many cybersecurity areas all over town. And one counter argument or one argument people say was zero trust is great, but what about the insider threat? And they've already identified themselves? And so So is this, this an end game for you? And what spycloud What can you do to help the insider threat who's who's already defeated zero trust.

12:01
Given the fact that we have so much identity information in our database, we have the ability to through breach records and medical records and, and all the identity assets that we have in our data. Right now, we have the ability to understand a person's behavior, not only inside their work environment, but also outside their work environment with respect to social media or other accounts that they may have, once an asset is breached. companies and government organizations will typically make sure that any endpoint devices associated with a network reach or are cleaned or re imaged and put back into operation as a as a new machine as a new device. And what we fail to recognize sometimes is that the Mauer did in the very state associated with that breach, even though you clean the hard drive and you reimage the machine, that malware ingratiate is out there. And so if there are session cookies and and PII and anomalous behaviors that we can attribute to individuals that still reside in those breach records, then we can follow that person's behavior, follow the path, understand their digital life. And in with that understanding, we can assign a risk score associated with that individual that helps us understand when that individual is in a corporate entity or a government organization, that they have a lot of information, their background that their bosses and their network administrators may be concerned about with respect to their behavior in their current job.

13:47
Magicians like to work by misdirection. And you look in one area and all of a sudden something goes different area. And so I see what can happen here is that people are worrying about identification. It's called The first pillar of zero trust and talking about human identification, and attribution patterns and, and authentication. And

all of a sudden, you get hit by, you know, OT, operational technology. It's like, wait a minute, we spent 40 hours a week making sure Joel is Joel. And then someone from a phone system gets in or someone from I don't know, there's so many remote points now accessing coming in. And so does your company address issues involved with ot as well?

14:27
It does. And one of the advantages of converging infrastructure, which we've seen over the past 10 years or so, where OT and it were largely separate and their functions have now been converged largely due to the requirements of more sensors and more efficiency and that convergence from a threat landscape has increased the surface area if you will. The end the ability for threat actors to access ot in ways they weren't able to before. But it also allows for greater understanding of behaviors and OT environments. And that's where we kind of so when a when a breach does affect operational technology, we have the ability to pull in all that unique data and understand access points and enumeration of the attack surface and how the criminal element was able to gain access to that information. There's still an identity associated with the bad actor accessing the data operational technology and so by caught again, can offer a lot of very useful information and understanding how breaches take place, understanding lateral movement, understanding the identities associated with with that bad behavior.

15:50
Your young man, Joel, I've been around a while I've seen all kinds of things. And I see these trends. And back when I had learned all the acronyms role based access, control access, but all those memorize those things years ago, the trend up until recently has been to role based access control. And what I see happening is switching more and more people talking about access based access control, as is really a way to eliminate a lot of questions with the axis. So do you see this trend too? Am I just maybe listening to the wrong technology people when it comes to access controls?

16:23
Now, there's definitely a trend in this area, and we're concerned about it as well. But again, behind every access point, there's an identity, there's an enumerated protocol that can be ascribed to an identity. And, and so we have to be more clever about how we're preventing behaviors through new access mechanisms. And there's a lot of good work being done right now and making sure that we have preventative capabilities and in identity access management systems that we're concerned about.

16:59
Well, it's September 2022, we have to talk about the elephant the room, and the offense, probably drive around a car and from your house, it's Uber. And I got gotcha on the line, I got to ask the question about Uber. Have you studied much about Uber? Was it identity problem? Was it just a simple 16 year old phishing attack or so what do you know about Uber you can share with us

17:21

in terms of the breach, you know, there's still quite a bit of studying this thing down right now to fully understand the attack, but it was substantial. And it definitely had to do with identity and credentials, this is how the attack the attack point was initiated. And then there are other capabilities that were used to Exercise lateral movement, and, and be able to withdraw or take data from, from over. But identity was was in the taking advantage of identity was, was the way it was done.

18:02
In the commercial world. spycloud got a strong presence. I mean, we talked about many of the large organizations use your services spycloud. And and the commercial, they talked about account takeover. And they talked about fraud prevention. And you may think that's just you know, someone using their computer in St. Louis, if somebody has their computer in Oregon or something. But I think both of these aspects apply to the federal government as well. I mean, maybe not account takeover as easily with an individual's account. But But fraud exists in many different levels, even in the federal government, doesn't it?

18:33
It does to be thinking about student loan fraud and Medicare, Medicaid fraud and the enormous amount of fraud that takes place with respect to IRS consumption services every year. That or to ministration is one of the leading organizations that has to combat fraud every year. So outside of the normal, you know, notions of fraudulent activity and, and criminal activity in the commercial sector, that it is rampant in the federal sector as well. And so Spikeball can be used to great effect to identify those that are perpetrating fraud.

19:14
When we opened up this podcast, I made kind of a whimsical reference to the criminal underground. But this isn't just went I mean, this is this is this is a heart attack, as they say. And so you gather a lot of your company gathers a lot of information on the dark web, and goes to the criminal underground and you gather in passwords, and you gather in email addresses. And so what happens is you can make one of your customers aware if someone has been compromised is that how would use this to be captured data? That's

19:45
exactly right. And so if we see stolen lost missing credentials, and any of the breach data in our database, then we highlight that to our customers and then it will then trigger an alert to confirm form that customer as well as the employee being affected, that password needs to be changed. And so that simple identification in order can help prevent an enormous amount of challenging activity in a network. It is clearly stated in a number of different reports to include our own every year password usage and in re usage of stolen or lost credentials is and basic hygiene are about to account for about 85% of all successful cyberattacks. Wow, yeah.

20:42
I live in the Washington DC area. And I always have interesting neighbors. One of my neighbor works for the Nuclear Regulatory Commission. He's the physicist, you know, big, big Brainiac type guy. And, I mean, he's real smart guy. And I looked at him, I said, Well, he's probably not going to fall prey to some of these phishing scams, or these fraudsters. However, if you look around, I think on your website, saw the figure that.gov

accounts are in that database that you have. There's something like 206 9000 credentials for.gov in there. I mean, really, yes, it's got nothing to do with your PhD in physics, I just think humans are humans, and they can be deceived. And all of a sudden, their credentials are out there.

21:25
It has nothing to do with intellects. And it certainly doesn't have anything to do with the morality of a person. It's interesting that, you know, criminals have just as bad password usage as good people do. And so that's one of the reasons why we're pretty effective at identifying a criminal behavior today, because not only of the enormous amount of PII we have in our database, but also our password cracking capability gives us the opportunity to see criminal passwords in plain text format. And, and understand their patterns that they're using to establish their false credentials that are false identity. And we have enough of that information now. And we can see trend lines and understand better inform ourselves how to how to pass crack passwords that criminals think are pretty clever, but they're not. So

22:18
so if you get you get a lot of speak invitations and know that let's say you're in downtown DC speaking to a group of CIOs, and I would think the basic information you would give them would be to worry about their credentials and, and maybe use multifactor authentication. But then I've been reading stories about multi factor authentication frequent relies on the public phone number, which can be compromised. And so it seems like it just everyone's one step ahead in this game.

22:46
That everything you just said is true. The, the MFA has certainly improved security, but it's not impenetrable. It's not perfect. And so there are ways around it. But still, the number one concern in terms of being able to socially engineer criminals or socially engineering their way into networks is really through that initial identity access point where somebody is not taking very good care of their own security, hygiene and has not changed their password.

23:22
So if you've looked at the five pillars, or four pillars of zero trust from NIST, the first pillar is identification. I guess you'd agree with them on Joel,

23:30
I would I agree, then the first pillar should be identification. That's exactly right.

23:35
Looking into the future, you have a storied past, you've been all different levels. So do you think there's going to be some kind of an incident that's going to really light the fire behind people and have much more interested in moving up their level of identification? Or where do you see this whole general field headed in the next four or five years?

23:55
technology perspective, we're starting to see organizations using not only MFA, multi factor authentication, but substituting passwords for other types of credentials and in biometrics and, and so that's, that's a trend that I think is going to continue. But the other thing that we're seeing is that there's a lot more discipline and awareness in the system right now, which is healthy and good. And so that's an area where I think we'll also see an increase in training and awareness and people not responding to an alert to change a password or credential but proactively changing it as just a normal pattern of behavior pattern of life is something along the lines of you wash your clothes once a week while you're washing your clothes and when you get the clothes to dry, you're changing your password on all your accounts, you know, things like that is as mundane as that may sound isn't something that somebody would have changed your password on a weekly basis, that's something people would have done a year or two ago. And if so we're starting to see that kind of type of behavior to which is very practical and very good. And then in terms of enterprise systems, there's an awful lot of very interesting work been done in tying biometrics and identity, to layer two systems and accessing, you know, early on in the initial handshake between systems, that there's an identity, and a credential check that's being done much earlier in the process. So all those things taken an aggregate are going to improve credential security going forward.

25:44
Software developers talk about shifting left, it may be the identity management people, that's what I hear, when you say L two, that's a shift to the left is that's the before the boom. That's why several steps before the boom.

25:57
No doubt about it. And that's where we need to be as, as we talked about just a little bit ago, the prevention mindset now is very, very important. And so getting ahead of this challenges is very, very important. And so yes, it is early on in the process as you can establish a security credential as possible. And maintaining that throughout the session is extremely important.

26:20
So I'm going to end with your website again. spycloud.com. And if I were you, I'd get the 2022 identity exposure report and then get stunned by the numbers and don't believe that many numbers of passwords are floating around the internet. I never thought the reverse of it. I never thought that companies like Joel's can actually take and get the passwords for the malicious actors, and maybe keep a step of everyone and then do the proverbial move to the laughter left of boom. Another phrase that I've seen news many, many times. You've been listening to federal tech podcast with John Gilroy. I'd like to thank my guest, Joel Bagnold, Director of federal for spycloud.

26:57
Thank you so much, John, for this time today. I appreciate it.