Eye on Security

Breaking Down Malicious Insider Threats

Transcript

Luke McNamara:

Welcome to another episode of the Eye on Security Podcast. I am your host Luke McNamara. Joining me today I have Jon Ford, managing director of Mandiant, and Johnny Collins, director of Mandiant, as well. So, one of the great things about working at a company like Mandiant, being able to access the people with areas of expertise and things you know very little about, that would probably most of the people that come on this podcast, but today it's both of you gentlemen here to talk about insider threat. So, great to have both of you here.

Jon Ford:

Thank you for having us.

Johnny Collins:

Thank you for having us

Luke McNamara:

Before we get into the discussion around insider threat, I'd be curious to hear a little bit about your backgrounds and particularly how they relate to this sort of threat factor.

Jon Ford:

So, this is John Ford. My background, I came in from law enforcement, about 27 years between local law enforcement, as well as 20 years with the FBI. While I was at the FBI, I worked primarily for the cyber division, but worked investigations of all types during that time. And we certainly, during that time, worked investigations involving insider threats, both domestically and abroad, and so it became a key passion of ours and how we can build out a better program and a good program for our clients.

Johnny Collins:

Hey. So, I'm Johnny Collins. I've been doing this for about 17 years. My focus has been largely

on the commercial sector for insider threat. I've actually got one of the largest cases settled out a quarter to half a billion dollars between two large casinos, based on our methodology of follow the data. So, pass it back to you, Luke.

Luke McNamara:

Yeah. Great. So, one area I think maybe we can start off with is just a definition of what insider threat is, or at least how we think about it here. And I guess some of where I've seen insider threat defined or used differently as I've seen its application both in a cybersecurity context, but this is also something that you see often used with respect to physical security and other types of threats by insiders, employees, et cetera. So, just for everyone who's listening to this, how do we define this within the context of what we're typically looking at and responding to?

Johnny Collins:

So, we have what we call the insider threat continuum, and it's a range of what we call insider threats. And that range begins at the lowest tier on the levels of what we would consider an insider, and that's the unintentional insider. Those are the folks that are clicking a link that didn't mean to, didn't patch a server. That's the unintentional side of things. If we go up another tier, we include third-party and supply chain type connections, where some entity maybe coming in as the print repair person, or maybe it's some MSP or MSSP type entity. And then, as we go up the levels beyond that, that's your more traditional insiders that everybody knows, the malicious types, in other words, for corporate espionage or for actual espionage for another nation. And then, at the very top is what we call close contact. That's where you avoid all electronic communications. If you think of the movies where somebody meets in a park, puts some chalk on a bench or on a mailbox, that's what we call close contact or human enabled technical operations.

Luke McNamara:

So, this somewhat preempts what my second question was going to be, which is it's not always necessarily malicious activity, it seems like how you're framing that.

Johnny Collins:

Correct. And in fact, the most common cyber threat is the unintentional. It's part of the education process we go through with our clients, is developing that program to make sure you don't fall victim to becoming an insider. And so, that's one thing that we carry forward, is it's not always about the malicious or the disgruntled employee or somebody who's been recruited by a nation state, it can be someone who's just an innocent victim.

Luke McNamara:

And maybe going back to, again, like how different types of organizations think about this, or

have thought about this, and I don't know if you see a big difference in the corporate sector versus governments, the IC, et cetera, but typically where do we find that the remit for insider threat prevention or the security function, is that something that exists within the cybersecurity function of organizations? Is that something that also you can see it exists in the physical security environment? Where does that typically reside?

Johnny Collins:

So, on the corporate side, it traditionally lives in three places, but we'll see it under what we call cyber threat intelligence, so any type of intelligence group within an organization. We also see it within corporate investigations. That group, the corporate investigation group is traditionally for where a lot of the employee actions will be assigned. And then the last one that we will see also is just under HR or what we call the privacy group. Those are the three areas that we tend to see where insider threat lives. The ones that are the most successful tend to be the cyber threat intelligence groups. We see renaming of like groups being called the Counter-intelligence Group or the Data Protection Group or something along those lines. So, it's not just an overtly saying, "Insider threat is what we do." I'll pass it to Jon for the government side of things.

Jon Ford:

On the government side, we either see it usually one of two places. Usually it's within the security office, or it can be its own, such as an internal investigations type of office. And they usually, though, are structured in such a way that they have a direct pipeline to the senior executives of that organization. They're a little different as you go from national organization to national organization, but primarily, that's how they live. But they, too, are working in conjunction with the intelligence offices of those offices, and usually as a consortium, quite frankly, as we see with the National Insider Threat Taskforce.

Luke McNamara:

So, moving into the discussion, I guess, around how organizations, they have some function may be set up to do this, or they're thinking about setting up this sort of function, but how they might think about this in terms of their overall security posture and maybe just investment in this as a particular resource. How do you typically see organizations approach threat modeling around this specific type of threat? I can imagine when you think about other types of threats in cybersecurity context, if you're in a particular industry or a sector, let's say you work in oil and gas, and you have operations in the Gulf region, you may be at higher risk for targeting by certain types of actors. Maybe a higher risk for certain types of activity or threats. But insider threat is something that can happen to, it seems like, virtually any sector, any region. So, how do you typically see organizations thinking about that as part of their overall posture, and where do they need to put and dedicate resources?

Johnny Collins:

On the commercial side of things, what we tend to see is a heavy focus that's either what we would say is reactive or proactive. On the reactive side of things it's, "Hey, we see this data that's been leaked on the dark web. We see this has been dumped to GitHub. We see that this particular individual that we just let go, we see their IP address getting back into the environment." So, it's very reactive. The proactive side is vastly, vastly different, as you can imagine. So, they're monitoring the dark web, they've engaged folks like us to provide services, they have a very mature program. And so, they do it in a very different way, though.

Traditionally in the years past, you've heard profiling and things like that. That's not something that we see in organizations that are very mature. We see what we call monitoring activity. So, bucketizing your insider threat into different types of activity, for example, fraud might be one, or sabotage might be another, or corporate espionage versus nation state espionage, that those tend to get bucketized and get tracked into different systems. And those are systems that have case files, because it's not tied to an individual, it's tied to activity. What we tend to see in a lot of cases is it's a group activity that's going on. So, if an organization's in a reactive mode, they tend to stop the one as opposed to the many that we see in a lot of our cases. So, I'll pass it over to Jon for the government perspective.

Jon Ford:

For insiders inside governments, there's obviously an intense monitoring of government systems, so they take all shapes and forms as they work across different levels of those classified systems, going all the way from a classified through their most sensitive systems. But when you're working in the government world, they do work very closely with our counterintelligence branch because, often, what we do see is that insiders are those who are being recruited by nation states to essentially become spies and conduct espionage against nations. So, in those you have a blend of a physical action or physical investigation that's going on, as long with a technical investigation based upon some type of predication that may be ongoing with certain actors, or they're watching the opposite side, those who they believe are spies inside of this country who they may be meeting with. So, you have a combination of both physical and electronic.

Luke McNamara:

It seems very similar to the disciplines that have been built up over the years around counter-intelligence for the reasons that you just mentioned, and I'm curious, off of Johnny's comment as well about how organizations are now approaching this from a much more behavior focused approach as opposed to looking at targeting or profiling certain individuals, have there been techniques and methodologies that have been adapted over the years, taken from the government space that we're now seeing in the commercial sector use a lot more of... I guess you could see that similar to other areas of cybersecurity, even, and cyber threat intelligence.

Johnny Collins:

On the commercial side, I would say that we see more advanced techniques than what we would see in the government space. So, for example, in like cleared spaces, because I've done that in a previous life, you would see folks that would potentially bring in a phone to a skift space as an example. But with the COVID life that we have now, everybody has a phone and stealing data is as simple as a snap of a phone picture, or a video as you scroll through a database. So, the prevalence has been there for even a longer period of time. And just getting other types of devices that can get information outside of what we would traditionally see as stuff that you can monitor. But the visibility, too. Some organizations go full tilt on employee monitoring, having cameras on and taking pictures of folks. If they're doing something that then you might wonder if they're doing a video or something like that. So, even the surveillance pieces on the commercial side, I think, are quite a bit ahead.

The difference, I think, and Jon will probably cover this, but the amount of access to intelligence that the government has is very vastly different. A commercial organization can't reach into, say, the FBI as an example and get information on so-and-so employee. They've got to rely on their HR. So, in that regard, they're at a little bit of a disadvantage. They don't know where that particular individual's been. Like if they're a researcher, have they been at universities and other things like that?

Jon Ford:

Yeah. And I would say the targeting is, and to some degree, also different. Right? So, if governments know that they're going to be targeting other government agencies or employees, they know that they have training that goes over that. They know that their employees are more visible and maybe more watched. And what I mean by that is everything they do on their work computers is going to be monitored. So, they only have smaller windows in order to try to co-opt or engage that individual. Now, on the other hand, though, from a commercial side, this is where we start looking at... From an example of research, we were talking earlier, if we look at healthcare research alone and today's environment, what is the value of finding the vaccine the earliest? Who's the one that makes the most money or has the most to gain by being first to market?

And when you start looking at third-party suppliers, as they go through it, everyone that contributes to the final product, these are vast opportunities for either organized criminal groups, individuals, or nation states to inject themselves into this conversation or with these individuals to get a hold of this key data that they may want. And so, from that perspective, there's just going to be much more that can go on. And the opposite side is commercial, as Johnny mentioned, don't have the opportunities to be able to draw on as much information, so they need better technology. And they also have not as long a journey, oftentimes, in creating these insider threats, offerings, or practices within their own organization to benefit from.

Many times, we go to organizations and they have spent quite a bit of time working on the advanced threats that attack them, get ransomware or any other criminal organization group, or sometimes nation state attacks, but they've not realized a same or a similar investment, whether it's time or people or technology and how to detect insider threats. Because we have to remember that from an insider perspective, legitimate access rules the landscape, and really being able to leverage that legitimate access pays key dividends inside of an environment. And how do you watch legitimate access amongst all the other noise in an organization of others who have legitimate access for the same materials? And this becomes a key differentiator when you really apply the intelligence, and what you're trying to discern is who may be your insiders at an organization by following that data.

Luke McNamara:

So, I'm curious now, and maybe we can get to some of the recent examples of cases or incidents that you guys have been involved with where we've seen types of insider activity, and maybe we can focus on the malicious ones because those are more interesting. But where are some of the scenarios that we've seen insider threat play into some of these security issues that we've had to investigate?

Johnny Collins:

So, a few notables from last year that we came across, COVID drove a lot of folks to have to make tough decisions on budgets and lay offs and things like that. We had a few clients that engaged us because of that. Right? They're like, "Hey, we've severed this employee, given them a package, but now we see activity that looks like their IP address. Can you investigate it?" Sure enough, we looked into it, and yes, it was the particular entity. And sometimes it was a disgruntled employee, where they just destroyed everything in the environment. Very similar to what we would see in a ransomware attack, right? Where everything's just getting destroyed. In other cases, they were taking data to help get another job or monetize it in some fashion. We had some other notables that were very interesting, and those include where we saw the SOC/cert type manager, in some cases who hired us, was the insider. Watching the watchers as such a scenario came into play was a growing thing in last year.

In addition to that, we had cases where folks had known that we would be involved, and one notable was a CEO of a large company had decided to start their own business and we were going to get brought in to do an investigation. We said, "We're going to look at X, Y, and Z." I'm not going into specifics here, but once that was presented from the party that was going to hire us, they decided that they would turn over everything. So, they actually rolled before we actually got to do the work. So, it was very interesting where our methodology of follow the data and going through that process was enough to get the CEO, who was going to start their own company, to confess that they were basically going to steal all the clients and things like that. So, large item settlement, but we didn't even start the work. It was just that our methodology was so solid, our statement of work scared him away.

Jon Ford:

I'd also note, too, we also saw examples over the last 12 to 18 months of those who were actual insiders, but initially, our clients engaged us as if they believe they were being extorted by an external adversary. And those extortions, as we started looking into it when we were brought in, we were able to note several items that just didn't fit a real advanced actor or an extortionist that we would normally see. And we were able to work through this and actually identify that there were actually insiders inside the company pretending to be extortionists outside of the company. So, we found that was a couple of interesting times that that did occur, and in both cases, we were able to identify the insiders during those investigations and provide them to the client so they would be able to take their official measures as they needed to.

Luke McNamara:

I know one of the things that we've been seeing for some time are threat actors that have access either because they compromise that access or they gained it somehow, maybe they were insiders, and then hand that off to others to carry out additional operations, whether it's ransomware or data theft of some kind. Have we seen many situations in which those individuals that gain initial access or actual insiders themselves, and they're selling that access in the underground, is that been something that's come up in some of the cases that we've seen?

Johnny Collins:

Well, we had a couple of cases that were very interesting. One of them was last year, there was someone within a finance department who claimed to be the unintentional insider. Come to find out after a deep investigation working with law enforcement, the actual individual was working with an external entity, cyber crime, to get monetized on the back end. So, they were terminated and something was settled out of court, and a bunch of other things happen. But long story short, we do see cases where folks do get approached by large entities outside of their organization to get additional monetization. This particular individual had some financial difficulties and basically relayed her services or his services, for that matter, on the dark web, and those were solicited. And they settled it all outside of normal channels using very interesting monetization, so Monero and things that you wouldn't normally be able to trace, but law enforcement was able to track those down. So, very, very interesting cases, not as prevalent as you might think, but we do see them. They're not completely rare.

Luke McNamara:

Is it a mixture of cases where it's the individual going and offering their services, the insider, or is it tend to be more of outside entities approaching someone and saying, "Hey, you have this access. We want to utilize it. We'll pay you for this," or threaten them in some way?

Johnny Collins:

Yeah, we see both. We see both. In this particular case, this individual was not initially looking for it, so an ad on a forum, and responded to it and then got connected to an invitation only forum. And then, from there, were able to get a contract in place and set it up. So, we do see both.

Luke McNamara:

So, maybe we can pivot this discussion into talking a little bit about the particular service that you guys are running. So, that's part of the reason for this discussion, but some of the offerings that we have around this. I'm curious if you could describe that a little bit, but also go into the thought process behind that, given your experience working these sort of cases where insider access has come up, why is it that you designed these services the way they are?

Jon Ford:

We designed two central services around these. One was round the insider threat program assessment, and the second was around insider threat as a service or insider threat security as a service. The program assessment was designed around those either nonexistent or nascent programs, and they were really looking for, "How do we roadmap a program over a period of time? And what are the key things that we should be thinking about?" In addition, we have another tier that was built around those that had had an insider threat program for awhile but were looking to have it evaluated to see programmatically how it was doing. Maybe there's some areas that may have some challenges or were addressed or were missed, and what can we do to help guide them in those directions. And then, the third offering is for mature insider threat programs where we also do a technical program assessment, as well, to see how well their activities are being captured.

Johnny Collins:

So, we call that our insider threat assessment, and like Jon said, there are three tiers. One is to basically, if you want to build out your program from scratch, that's tier one. If you want to assess your existing program, that's a tier two. And then, if you want to get a full depth and insight on your program, there's a strategic as well as a assessment, we call it our technical security posture assessment, that's where we'll deploy our tech for about a month. And that includes looking for nation state activity through the recruiting process, as well as deploying some end point technology like the screenshots, print jobs, and things like that. Just to be able to see if there's any type of insider threat activity for a period of time. But again, those are all snapshot in time, help you build out your program, gets you to the next level.

Luke McNamara:

And do you see more organizations showing interest in those in any number of those different

services right now? You referenced, for example, the pandemic earlier and how organizations are operating with constrained budgets. But one of the things that I seem to be hearing more about, as well, is an increased concern around insider threats, because now you have more people working from home and maybe in situations where, even in a non-malicious context, they may be exposed to types of risks that previously when they were working inside the office, they weren't. So, do you see that shaping the interest around these services at all?

Jon Ford:

Yes, actually, we do. Especially during the time where this kind of work from everywhere environment has really started to take hold. I mean, companies are looking at their network boundaries being pushed on in a very rapid fashion, and most organizations weren't really ready for that, so having that equipment and pushing them out really may not have been there for what they were needing. And also, now you have people who are maybe less monitored. Now they're working off their home routers, even though they may be VPNing, but maybe they're working off their home desktops. Those are examples. Printers that are not necessarily monitored, what does that look like?

And as really, as you look through this, it really came down to companies became more concerned about is my intellectual property, really staying with us? Is there some type of misuse of our data or technology? Because they really wanted to look at that customer trust and organizational reputation, but right now, also, their investor confidence. And they really needed to look at those three things while trying to protect their organization. And what does that look like for them? So, we did see increase in those looking for us to not only assess their capabilities that they had, but also provide them these additional security services.

Johnny Collins:

Yeah. And I'll add to that a little bit, too. I mean the big ask we get is, "Tell us all the techniques that we can't monitor." And so, we'll dig into those, especially with the remote workforce today, the split tunneling with VPN. Folks not being on VPN is another thing that we see a lot of. I mean, most folks try to avoid a VPN where possible, in their mobile. They're also operating in like an M365 environment where it's all cloud-based and you don't have to be on VPN. And in those scenarios, there are so many ways to exfiltrate data and avoid detection. And our goal when we're working with clients is to give them that visibility and help them understand, "These are the things that you can do, but there are limitations."

If folks want to avoid technology altogether and go old school with a camera, as an example, it becomes much, much harder to track. But we do cover all those different areas, it's just has been a huge uptick. The amount of exfiltration via USB, the amount of folks that have been offered to put ransomware via USB on the system just to give a foothold for an external actor. All those different techniques are coming to play. And I think we can all agree that the COVID life has been very, very challenging, too. There's the stress piece that goes into it, and it's not just all about, "Okay, you're remote. You're having to work remote." There's folks with kids

trying to do WebEx's and Zooms and all these different things. All those stresses feed into different things and can cause people to do things they wouldn't normally. We've seen plenty of insider threats that wouldn't traditionally, if they went into the office everyday, probably would be fine, but become disgruntled because of their situation.

Luke McNamara:

And so, for our organizations that are approaching us and there's interest in one of these services, is that because they're primarily thinking about, going back to the beginning and the different categories of insider threat that you were talking about, they're thinking more about that unintentional, non-malicious insider threat, or some of the more malicious type of behavior that they're worried about?

Jon Ford:

So, I will say that the biggest concern that we're getting a lot lately is data exfiltration, so data leaving, and the biggest, biggest concern is destruction. We've had plenty of clients that said, "Hey, I'm really concerned about one of my admins just destroying our environment," or in one case, we saw where the entire domain was held hostage by a password. Those kinds of things have amazing impact in both the negative and in the positive way. The positive is everybody can learn from those mistakes. The negative is, those are huge impacts. If your entire domain is shut down, nobody's working, nobody's being profitable. So, it's those types of scenarios where it runs the gamut. But definitely a big focus on losing data is a big piece of it, especially when we're talking about intellectual property, or we're talking about government classified information, or whatever the case may be, all those different things become areas of concern.

Luke McNamara:

One area I'm curious on, as we close this discussion around insider threat, is where you see the conversation around this going and evolving. And I think referencing back to a point you were making, Jon, earlier, I think it was in relationship to the Thousand Talents Program, or some of the targeting we've seen over the years with healthcare. It seems like you've seen over the last couple years in particular the Justice Department being very aggressive about charging people connected to universities involved in various types of, I guess, what some of the activity could consider insider threat, theft of data, theft of valuable research. We've seen over this past year, intrusions by various nation state ABTs targeting research, all different components of that, that you've seen examples in the past where you've had insider threat at major prominent tech companies.

From a whole society approach and thinking about the different ways that we have to protect certain types of data or individuals that have access, organizations that work on very critical data, is this something that is going to increasingly be a difficult problem that not just entities and organizations that are doing classified work and research in the government space need

to worry about, but something that from an impact standpoint, increasingly other organizations in different sectors are going to have to think through?

Jon Ford:

Yes. I mean, what we're seeing when you used to think about the original insider, probably, used to think somebody stole something of mine for some type of personal gain, whether that's what they wanted... As Johnny said, they want a new job, they're trying to impress a new employer, or they're simply just trying to monetize it. In the government space, we saw insiders as those who are selling secrets to nation states often. Right? Or trying to do something nefarious.

But what we're seeing is now that insiders are increasingly are being recruited by or interacting with foreign governments. We are in a time and space where you're seeing the whole corporations ramp up very quickly and try to be the first to the finish line to get out technologies of any kind, and whether that has to do with medicine, whether that has to do with the next super computing system, whether it has to do with satellite technology, whether that has to do with anything you could possibly imagine, whether it has to affect Wall Street, whether it's affecting banks, whether it's affecting transactions, all these things matter to others.

And really that's where it starts coming down to, is really understanding your organization's critical assets. Right? What are your high value assets? What are your crown jewels? What would damage your company or embarrass your company the most prolific way? And you can imagine that these are the things that we're hoping that organizations will think to protect, and not just from their own employees, but understanding that nations now are employing those same techniques that they used against other governments are now using very similar techniques against businesses.

Jon Ford:

And this has all ready made the news. It's not going to go away. Many countries are in races right now to see who can be the first, and that also means supporting their own commercial organizations. Some of these organizations in other countries are not commercially ran, they're government run. We would think of it, in our country, in the US, as commercially run. But it is a race to the finish, and they are employing those same techniques and they're becoming much better at it. And there is no light at the end of the tunnel to show that this is actually going to slow down or wane in the future, but will probably only increase.

Johnny Collins:

Just to add to that, the key thing that we're able to bring to the table as part of our service that we call insider threat security as a service, is the follow the data model that I mentioned earlier. But let me give an example because I think it follows with what you're talking about. What does the future look like? The future is very simple. For folks that want to steal data, I'll give it a

great example that we've seen on a recent case where somebody just literally sent something to a coworker as part of a legitimate business via Teams, went onto their phone because it wasn't controlled, and literally downloaded the file. That file was a critical file, and that gave another corporation six months of research ahead of everybody else.

So, it's the simplistic nature is we're so connected via data, but controlling that data and falling wherever that data could go, that's the key difference and controlling how that data is transmitted. Because the data is either worth something or it's going to get leaked. Right? If somebody is very upset or, in the worst case scenario, is that they just delete it and destroy it because they're disgruntled. Right? So, we see those trends just continuing to grow and people trying different techniques. Right? The TTPs, or tactics, techniques, procedures we see for insiders is very similar to what we would see from an advanced, persistent threat doing live off the land. Right?

Johnny Collins:

Similar to what we see with SolarWinds when we're doing our investigations. It looks just like an insider moving around that knows the environment. Well, who better to know the environment than the admin who's been there for 15 years, or the executive assistant who's been there for 20 years, that knows where all the files are? And similar to an advanced, persistent threat, if the data is living on somebody's desktop, they'll just grab it. Why try to log into the database and trip flags? Just grab the file, print it off, and walk out the door. That's the kind of stuff that we see as time goes on.

Luke McNamara:

That's an excellent point. Any final thoughts for any organizations that are thinking about implementing an insider threat program or what they should be looking for in any sort of service?

Jon Ford:

One thing I would hit on, too, is that we are seeing an increasing ask for insider threat security services to be operated by a third-party. Just as an example, we've had, well we've had several, where the insider ended up being part of their own team that was doing either insiders or was the admins. And part of that comes to where even the investigation of an insider, if you work in a closed company, some of these times you're going to know the employees. Right? So, there may be some bias as it goes towards that. But having a third-party that's following the data, who's only seen data moved, removes a lot of bias from the equation, who can then pass those results to that organization for their review and their investigation. So, we're seeing more ask for that, as well, and to doing that kind of analysis of their insider threat alerts that are coming through, as well.

Johnny Collins:

And part of that, too, is what we're seeing a growing trend is prosecution. And when we're looking at prosecution type activities what we tell most clients, and they've already done this in part of their own research obviously, but you have to have solid evidence that's not what we would call hearsay or anything like that in a court, where you're making assumptions. The data has to speak for itself if you're going to do prosecution. And the other piece of it, too, is making sure that you've got all the right councils involved. Right? Both your internal counsel and a third-counsel as well.

That third-party piece is key because we don't care when you're doing a third-party, you're trying to just tell the facts, and the facts are the facts. In some cases, we see multiple facts. Jon mentioned earlier where we had one case where the person doing the extortions was an insider, right? And so, they appeared as though they were a cyber crime unit or something outside of the United States, and so we were able to keep tabs on that. But that's the exception rather than the norm. Most entities tend to be pretty clear cut and dry. But follow the data, let the evidence speak for itself.

Luke McNamara:

Great point to end it on. Thank you both for coming on here. I found this to be very informative. I think others will, as well. So, excited to hear about some of the future cases and examples of you guys are working on.

Jon Ford:

Thank you very much.

Johnny Collins:

Thank you for having us.

Jon Ford:

Thank you.

Johnny Collins:

Our pleasure.