Eye on Security Podcast

The "Big Four": Spotlight on Russia

Transcript

Luke McNamara:

Welcome to another episode of the Eye On Security Podcast. I am your host, Luke McNamara. We're here with the fourth and final installment on our series on the Big Four. Definitely go check out the others that we've done on Iran, and North Korea, and China, if you haven't already. But today we're tackling Russia and who better to do that than the person who's with me here today, John Hultquist, the Vice President for Mandiant Threat Intelligence. John, how are you?

John Hultquist:

Great, Luke. Thanks for having me.

Luke McNamara:

I should note to everyone, John is also my boss. So if some of these questions seem like softballs this episode, or conversely, if I'm not here for the next episode, you know why. The question I think would be interesting to get into first is obviously when it comes to Russian espionage, there's been a long history of them having to demonstrate their capability in the space, going back to Moonlight Maze, Agent.BTZ.

John Hultquist:

Even before that, Cliff Stoll, potentially using the German hackers to carry out activity in the... I think it was as far as the '80s.

Luke McNamara:

Yeah, even longer back then I'm thinking through there. I think now there's probably... When most people think about cyber espionage capability or nation states doing things in cyberspace of a malign nature, even in the larger popular consciousness, Russian threat activity comes to mind, and people are very aware that it's out there. But I'm curious, in your mind, was there a point where we went from seeing what used to be a very elusive threat actor that we knew had this capability and that was out there, to where we started to see them a lot more often, where they started to become more prolific?

Of course, whether that was because of operations ticking up or our collection capabilities changing. In your mind, was there a moment where that shift started to happen?

John Hultquist:

Yeah. There was a couple moments like that, actually. When I was at the State Department a million years ago, it was my area of responsibility. I spent quite a bit of time just thinking about how to find their activity and looking at some of the criminal activity and whether or not that had crossover with the state actors. And we definitely found some stuff like that. But the big Russian wake-up call was Agent.BTZ.

We were, at the time, I'll think a lot of the security or InfoSec offices were actually really focused on Chinese threat, which had just exploded around that time, not just against the government, but against the private sector. Agent.BTZ came out of left field. It showed up all over the world in all these government systems. And there was this massive effort to fight it back. But what was interesting is that actor has this history of showing up, getting caught, when they do get caught, burning everything to the ground and starting over fresh, where we lose them.

This loud incident was not what we'd come to expect from them. They'd been found before. Kevin Mandia himself had tangled with them in the late '90s when they were called Moonlight Maze. But they disappeared again. From our perspective, at least from the commercial intelligence perspective, we were looking at iSIGHT. We really hadn't seen much of the Russian activity until eventually we caught sight of APT28. APT28 was our reminder that they were still out there and slowly but slowly, we saw some of the stuff that we call Turla, which was probably the Agent.BTZ and the Moonlight maze stuff.

And then we saw the APT29 activity, which was just hard to miss because it was... Even though these guys were really high speed once they got into your network, they could move around real fast and gain lateral access, they were carrying out really loud spear phishing campaigns that were hitting everybody and their brother at the time. And there's other-

Luke McNamara:

This is the Office Monkeys area, right?

John Hultquist:

It's the Office Monkeys stuff. Yeah. And then the eFax, I don't know if you remember eFax-

Luke McNamara:

Yeah, yeah, yeah.

John Hultquist:

... that were like... This was like crime, but there's tons of this stuff. Really 28 and 29 where the real loud ones. They just broke the mold that we'd expected from Turla, who would always stay below the radar, didn't like being discovered, wasn't very loud, but was always low and slow.

Luke McNamara:

In your mind, does a lot of that coincide with... Because I was thinking back to iSIGHT partners, when we started seeing that. It seems like a lot of that started to emerge or become more prolific and active following the Crimean invasion and the crisis when Russia started to get involved there.

John Hultquist:

Yeah. Yeah. We're doing a lot of tracking. We're tracking a lot of this adversary in Ukraine. We were fortunate to have a lot of really good visibility there. Then we recognized that was just a massive opportunity for us to learn about this actor. I think at the time too, people were calling it a lot sloppy. The activity was looking sloppy. But I think the other way to look at this is they were in a shooting war. And not just engage in Ukraine, by the way, they're also newly engaged in Syria at the same time.

And so, their intelligence requirements, responsibilities that they had, probably shot through the roof overnight. That just led to more opportunities for us to get visibility into them.

Luke McNamara:

You've talked about a couple of the groups already so far, and there's certainly a lot that we could spend the entire discussion here getting into. But for folks that maybe are less familiar with Russia's cyber threat capabilities at a high level, what are some of the groups that are out there? And in cases where we have strong suspicions of them being attached to particular sponsored organizations, what do those look like typically?

John Hultquist:

Well, we don't always know exactly how that looks, but we've got some good information these days, largely because of indictments that have spelled out a lot of the relationships between these actors that we track using forensics information and being able to connect those back to specific organizations.

I would start with the actor that I started talking about, which is Turla. Various governments I think have actually come forward and indicated that... I think the Estonian government specifically has come out and said that Turla is associated with FSB. Potentially the 16th Center is in the FSB. I think they're the only one thus far who have actually pinned that actor to a sponsor.

In addition to that, there's APT29. APT29's been connected to the SVR on more than one occasion. The big connection I think was probably the one carried out by the Dutch that made it into the Dutch media where they were, I guess, essentially hacking APT29 and able to see them on their systems, carrying out their activities. So maybe the 29's pretty widely believed to be SVR.

We've got really good information on GRU, largely because of their consistent line crossing. They've crossed the line again and again. And so, they find themselves in indictments again and again, and we get right all the way down to the names of individuals with the GRU. They've come up a couple of times, and it's been really interesting because we were

watching different aspect of the GRU actors and we didn't totally understand how they interrelated when they were cooperating and not cooperating.

So at least two actors, one we now know are APT28 is unit called 26165. Got another name, but they seem to be more of a signals intelligence background. And then there's Sandworm. It's 74455, which actually I think it's actually called an IO unit. They've both got other names like Main Center For Computer Technology and things like that. But those were the two major units under GRU.

There's also, by the way, there's recently some information that's come out about a PSYOP unit that may be under GRU. It's not clear whether or not. That is something else that we're currently tracking. We haven't been able to make the connections. Outside of that, I think the only other one that we have really decent information on would be maybe, or I'd say somewhat disinformation on is the actor that was involved in the SolarWinds stuff. That would be UNC2452.

According to, I guess, the Washington Post, that's believed to be an SVR unit, though we certainly don't have the goods. Sometimes we do get lucky and we can ID a unit. That's really tough to do. So usually when it comes to that level, we're looking out for the open source or looking for government statements.

Luke McNamara:

That's one of the things I think is interesting with a lot of reporting for emergent threat activity, or even actors that we've been tracking for some time as we may have an early indication that based on the targeting and nature of that activity, which nation that is probably in support of. And at a very tactical level, we may have a good understanding because of overlap with a code base of a known tool, another piece of malware. We think this is a particular UNC, or TEMP, or APT.

It's often that middle level where it's a little bit less clear, like what the sponsoring intel or military intelligence service is. But I think that's another thing that I found interesting over the years, is seeing these different groups and how they play out. And as attribution to particular sponsoring units and departments and agencies has occurred more with respect to the Russian government, some of the missions, the state admissions of those groups, don't always align with what you see activity. I think maybe the GRU groups is a great example of this. What's your take on that?

John Hultquist:

Well, I think the thing is some cases, these guys are following orders. It may be some sort of taskforce or way that the organization runs. I think about organizations that people forget is they are living, breathing things. Anybody who's ever tried to shift an organization around and put people in different places and stuff like that, there's a thousand reasons why things get moved or whatever. People are going to get promoted. There are people who have certain responsibilities or they just want certain taskings under certain people.

That's really hard to understand how all that plays out, especially when you're looking at IP addresses. It's really complicated. But I think it is still valuable. Not in every case, but in some cases, to have that information. In some cases, it tells us we can actually learn when we go at the problem from the other side. For instance, just knowing that a unit is GRU might change our perspective on what they're ultimately responsible for.

We can learn a ton of stuff from what they've done for sure, but it might be useful to understand that they have very specific military type responsibilities that they're probably going to put above other concerns. For instance, like with the Chinese actors, one of the things that's come out through some of these indictments is the regions that these guys support. And that's super interesting because now we know that those regions really dictate where those guys are focused. If you fall in that region, that means that you need to worry about that guy.

And so, you can start stacking your risks based on information not just from observables, which are hard to do in the spot, but actually from this other side of the problem. I think that's helpful as well.

Luke McNamara:

It makes sense too. I mean, with anyone who has familiarity with Western organizations, you see a mix of capabilities or certain capabilities exist within one particular organization. Different authorities may dictate how those capabilities are used or borrowed from other entities. So I'm sure there's a similar thing that's happening over on the Russian side -

John Hultquist:

I mean, in the United States right now, they've got this national cyber director position. And they've got all these other people who have interest in that space. We have other organizations that have interest in that space. We have other National Security Council positions. We have congressional interests. All those are being balanced out right now to create a new organization from nothing. And it is not as easy as reading the law that's created the NCD position. It's far more complicated than that.

That position is way more complex, and it's tied to so much more politically that you just can't see by, say, maybe just looking at a hierarchy.

Luke McNamara:

One of the things that seems to have characterized at least some of the Russian threat groups that we've tracked over the years, maybe more so than APT groups in other countries, is they're blending together of different types of threat activity. Certainly a big, heavy emphasis on cyber espionage, but what they've become known for as well, the information operation side, the targeting of ICS infrastructure. How do you see that in terms of how they weave those capabilities together, and what are some notable operations or groups that have carried out those operations?

John Hultquist:

Well, yeah. I think there's some different kinds of operations that we're seeing. I think the big one for Russian actors is the one that we see the most, or we talk about the most, is good old fashioned classic cyber espionage. That's stuff that Turla does. It's stuff that SolarWinds was probably doing, that's going after governments, going after people who do business with governments, and using that information to get an advantage in the global competition between Russia and everyone else. They're clearly after that information. That's still their number one priority.

Outside of that, they've got a bunch of other really interesting missions that are going on. One is the disruptive destructive mission, which is interesting because so much of it is about the activity that hasn't happened yet, or is being developed or prepared for. The stuff that we call Isotope either is called I think Dragonfly 2.0, or Berserk Bear, Energetic Bear. That's where these actors have been gaining access to critical infrastructure in the United States.

So much of that appears to be them gaining access for the purpose of contingency. Like they're preparing should they need to do that. Now there's a big question of whether or not it's just them preparing for contingency or even if they are doing it to signal to us that they're prepared for contingency, so that we know that they can potentially affect our critical infrastructure when the time comes. A lot of that has been focused historically on the grid and some on water assets.

We're seeing more and more other arenas they're being targeted. A lot of activity, for instance, has been in the aviation sector. A lot of airports have been targeted. I think they're interested in at least raising the specter of disrupting transportation and logistics. And at the same time, they were gaining access to the power plants in Ukraine, which they eventually disrupted. They were also going after Kiev international airport. So they definitely recognize it as arena that they play in.

But there's this other question of why, like why would you do that, ultimately anyway. So they did. They have turned out the lights in Kiev. They're out for a short period of time. It wasn't really a military objective there. So what was the objective? I think a big piece of that objective is essentially the psychological response to that. One of the things that you've done is undermine the credibility of the government when it says that you're safe from Russian activity.

I think a big piece of the activity that we see from these guys is not necessarily about those military objectives. It's not about turning out the lights because they recognize that turning out the lights is going to allow them to fly bombers over or it's going to cause industry to slow down so that more production slows down or something like that. That's not why they turn off the lights. They turn out the lights to scare people, to prove that the government is not got a handle on things.

That's the same reason why I think they target elections. I mean, they definitely have favored certain sides. They're certainly playing that game as well. But one of the other reasons is just to undermine the validity of the election. They are in election systems. Sandworm, the same actor who turned off the lights in Ukraine was also going after the specific election systems.

I believe they were there not necessarily because they expected to change the outcome there. I think they wanted to make us doubt the outcome. They're even doing that sort of thing in the Olympics. They weren't going to get Russia readmitted to the Olympics. What they wanted to do is make people think that the Olympics, they're picking on Russia by proving that other people were also doping, which was BS. But they released some doping records or some pharmaceutical records or whatever to show that everybody was also on pharmaceuticals and then to suggest that everybody else was doping. So the point is just consistently undermine institutions and it's all related.

Luke McNamara:

We want to get to the Olympics here in a bit, but you talked about signaling. You talked about your capabilities, and with them I perceive to be a conflict in the case of Ukraine. I think that's a great time to talk about that a little bit more, given what's happening right now with them amassing troops on the border with Ukraine and interpretation of how we should read different cyber operations that we might see. Is this something that's a precursor to larger scale conflict, or is this something that's a little bit more of the same that we've seen from them in the past? They may not actually be proceeding something.

Ukraine's also interesting because we've seen, in addition to some of the groups that we've talked about here, some other groups that seem very nichely focused on that, TEMP Armageddon TEMP Vermin. What's your take on that?

John Hultquist:

Those two groups, especially, I think are ones to worry about. Armageddon has this long history of going after Ukrainian targets. We think it's Russian or quasi Russian in some nature. It could be in a similar status as Vermin, which we believe is coming out of the breakaway republics that were formed in the Donbass region. But both of those actors, I would anticipate right now all have been tasked to gain as much intelligence or get their hands as much intelligence as possible.

Part of that's going to be, they want to know, for instance, things like Ukrainian troop movements. They want to know what orders are being pushed, conversations that are going on between Ukrainian government and their allies. Definitely going to know what those conversations look like between the Ukrainian government and NATO. This is one of those scenarios where you could bet your bottom dollar, as soon as they get on a machine, they're going to start literally searching the word NATO.

We've seen that in multiple different Russian incidents. They're going to get on that machine and they're going to look for the word NATO, because they want to know how far they can push if they decide that. Or if they want to know if there's going to be response now. So they're considering all that. Those intelligence collectors are the forward piece of that. That's not just going to be stuck in Ukraine, by the way. That's why we see these things not just in Ukraine, because, like I said, there's the other part of that conversation is going to be NATO, is going to be those allies.

They're going to go after those people as well so they can get inside and at one end of that conversation and the other. But this is exactly what they want to know. They want to know what the temperament is and they want to know how far they can push probably. And they're going to use these collectors to prepare for that. Those collectors, by the way, probably don't have any information on the grand plan by Russia, but they don't need to. Their job is to go and gather that intelligence on that sort of thing. And they're going to be ramping up right now.

Luke McNamara:

But back to what you were saying earlier about knowing not just the capabilities but the taskings of different groups, I think this is one where this becomes important too where those groups may not be the ones that are tasked with, if we do see some sort of kinetic or just disruptive or destructive activity from Russia in advance or in the course of some engagement. Those may not be the groups that are tasked-

John Hultquist:

It's a great point. Yeah, who does disruptive, destructive activity? Sandworm is the main player for that, or always has been. I would not overlook the one we call Isotope or Berserk. They've definitely been in play. They've definitely been gaining access to critical infrastructure. I'm not so certain that they've been gaining access to these places again and again. And they don't have some capability in the back end to carry something like that out.

I think that disruption, destruction, at least in the early state is part of their mission. I think that's pretty clearly why they're gaining access, even if it is a contingency mission. Those are the two players that I would be most worried about from a disruptive, destructive angle. If I were Ukrainian critical infrastructure, that's what I would be thinking about, those players as well. If I were, say, Ukrainian government or something like that, or their allies, for instance, I would be thinking about the other cyber espionage players.

Luke McNamara:

Yeah. Isotope is one that I think hasn't gotten enough love over the years, but they've done some very interesting things, I mean, going back to when we track them as Koala. I think over the years had a very interesting wide set of targets. Certainly a focus on energy at one point, but have definitely demonstrated they've moved out into other areas. Maybe not as high profile as some of the stuff that Sandworm has done, but in some cases, shown some capabilities and interests in some very fascinating places.

John Hultquist:

I think that Andy Greenberg once called them Chekhov's gun, which I don't totally understand the reference or know the reference, but that the idea is I think it's a play or something where there's a gun hanging on the wall. It was introduced from the fact that it has to be part of the story. It's just like they're hanging out. You know something terrible's going to happen when...

It's like it's foreshadowing something that is going to be part of the story. He calls it Chekhov's gun. They're clearly interested in one type of activity. It just is a matter of time before we see them play it out.

Luke McNamara:

You referenced the Olympics earlier. I wanted to broaden that a little bit into, I guess, maybe examples we've seen of how Russia's used its cyber capabilities beyond just information collection and espionage, beyond just spreading disinformation. Although certainly this will apply to this area and the destructive stuff. But where they've used those capabilities to go after things that they seem culturally significant to them.

So certainly the Olympics. I would say also maybe even the activity we've seen around the broader Eastern Orthodox Church, areas where there is something where they see a strong role of the state or something that reflects on Russia's maybe soft power. They seemed to have a willingness to task out those resources to go and either collect on, gather information intelligence on. Or in the case of the Olympics, to counter what they see as narratives against the state and of course for their own.

Do you think there's a cohesive strategy around that or is it something that's more of, as these things emerge, they see opportunities and they jump on them?

John Hultquist:

I think that these capabilities allow them to do everything right up into warfare, to open warfare. They recognize that as a way to compete with the West without necessarily people dying and probably some very serious consequences happening. I also think that they recognize the Olympics as an arena, a soft power arena that they're competing in, much like they would compete in any other arena, just like the Space Race during the Cold War.

The Olympics was an arena, a competition just like the Space Race, or outside of the military competition and where the risks were astronomical. And so, they're using this for an advantage in that space. If you look back to the Cold War, one of the ways that they advantaged themselves in that space was they did things like skirted the amateur role. You were in the Red Army, we weren't technically professional, but all you did was play hockey all day long. And they fed you and housed you and everything else.

So they're not afraid of bending the rules, bending the rules and these soft power competitions. I also think that cyber is just this other arena that we have really got to consider, where the risks are still limited and they can compete in all kinds of interesting ways. I don't think that we've even seen the limits of what ways that people will compete in the space. It's going to only get more interesting.

Luke McNamara:

It's certainly an interesting window into what are the specific areas that a particular state cares about. And I think that's what's interesting to see, with all these different countries, where they task these groups and the things that they're collecting on. It's fascinating to see

that. One question I thought would be interesting to talk about with respect to Russian threat activity is dormancy of threat groups, because we've had that, significant periods with some of these groups.

You know these people aren't going away. These probably aren't people that are going to become a barista and open a coffee shop next month because they got found out in the particular operation and outed and they had to burn all their stuff. So that capability you know is existing somewhere attached to some of these different state sponsors. But I think maybe in particular with certain Russian threat groups over the years, that seem to put a higher primacy on stealth, they go to ground maybe a little bit longer.

But we know that capability is always out there. We know it's out there somewhere. So when you do see these long periods of time where you're not seeing a particular threat actor, there's always the question of, "Have our collection capabilities not kept pace with what they're doing? Are they going dormant for some time? Have they shifted to targeting a different target set, different region, different industry, or vertical?" How do you think about some of those things in relation to these Russian groups?

John Hultquist:

They definitely disappear. They straight up disappear. Like you talked about with Turla, Moonlight Maze, disappear, Agent.BTZ, disappear, and they start showing up. And these are like five years apart from each other, six years, seven years apart from each other. Those guys are really good about covering their tracks. Isotope, or Berserk Bear, or Dragonfly 2.0, before that there was Energetic Bear, Dragonfly 1.0. We called it Koala. Those two look related.

There was this period after Energetic Bear, the first grouping that we'd found, that we were tracking pretty well, disappeared. And then we found the other crew. Remember they showed up in all these nuclear plants, and it was like a year or two... About two years after the fact. But when we looked at the data, the data started up couple of months after Energetic Bear disappeared. So they probably retooled and came back. And when they retooled and came back, we didn't have them. We had to go hunting for them.

That's the thing about hunting spies. It's not easy. There are going to be periods Where you're not going to have full visibility into these problems. They disappear all the time, especially when they take their OPSEC very seriously. We talk about an actor like 2452. The good news is there's a ton of eyeballs on that actor right now. And it's going to be really hard for them to disappear under those circumstances. The bad news is they take operational security, discipline, counter forensics, counterintelligence extremely seriously.

So if anybody's capable of disappearing entirely, it's them. In fact, I'm not sure anybody could match them for all the hard work they put into that problem. When and if they disappear, we may have a real hard time finding them again.

Luke McNamara:

One of the unknowns, it seems like, that's in that question is how long can they go dormant? There's going to be a period of retooling, but there may also be a period where they have a greater willingness based on their taskings and their mission set to have a reduced OPTEMPO that allows them to not be prolific.

John Hultquist:

Yeah, and that's a big question. That's the really important thing, because you can be the spy that no one knows, as long as you don't hit anybody. But every time you have to go after a target, you expose yourself. What was so interesting, like the SolarWinds, what made SolarWinds so interesting is that I think when people saw that number, the 18,000, or that really high number, they said, "Oh my God. These guys are out of control. It's indiscriminate. It's everywhere."

To some degree, it was, but what they were really doing is they had a huge trouping of potential targets. That allowed them to select the targets they really, really, really wanted the most. That meant that they actually limited their activity. They limited their activity only to the targets that they really, really wanted. That allowed them to essentially protect their operational security, because if you're not sending spear phishes out there, everybody and their brother knocking on every door, trying to get in to these organizations, you've got a sure way in and it's only to a limited set of targets that you want the very most. You're going to absolutely limit the ability of people to find you.

That thinking or whatever is what worries me. The good news though is that eventually these guys, they get asked for more targets. They get asked for more work. They get the told to do more. They sometimes get told to do something very visible. And that means that we're going to be able to hunt them down. Like Sandworm and 28. These guys were carrying out during the election, they were carrying out highly visible ops. There was just no way to really hide that. And so, their operational security really wasn't going to protect them in that case, just because of the nature of the work they were doing.

Luke McNamara:

Yeah. So capabilities and intent. This is one I think is interesting to talk about with respect to Russian threat groups. But one of the things that we're always looking at, and oftentimes when there's been some big events and you're being asked for a quote and in the news, there's always this question around the capabilities that we're seeing here, is this a significant departure from what we've seen of this threat actor or sponsor in the past.

And then intent or willingness, is this something that is a crossing of a red line that we've not seen them be willing to do in the past? I think with Russia, we know we're dealing with some of the top players on the food chain here and in terms of capability. And in terms of intent and willingness, I mean, time and time again, we've seen them cross things that we didn't think they would be willing to do. But both of those seem to be somewhat lagging indicators.

How do you think about, from the standpoint of trying to extrapolate out what we might see in the future from them? How does it all play together for you when you think about those things lining up with Russian threat groups?

John Hultquist:

I think one of the things that's important is to not limit our discussion to any one country when we're thinking about where the red line is. Because I think each country is actually learning about the red line from the behavior of the other countries. They got this far, there was no response. I can push it this far. I personally think that one of the reasons that the activity in 2016 was so successful is because the Sony activity done by North Korea was so successful.

I think they're all going to prove that you can carry out a major action, get Americans to change the way they live their lives, and still have them arguing about who did it. The FBI came out and offered evidence and said, "This is clearly North Korea." And people still didn't believe it, including people who are still around in the cybersecurity industry. That laid the groundwork, I think, for 2016. And 2016 laid the groundwork for the next one that we see. They're all pushing the line for the others, until they finally get to this, I don't know, some red line where they feel like they're really feeling pain. But I'm not sure that we've got there yet.

Luke McNamara:

Yeah. I think one example of that, where you can see other nation emergent players in contrast to the Big Four, look at what they've done and try to like use it as a way to say, "Okay, what's acceptable here?" I think one interesting example possibly of that is APT32 out of Vietnam. Maybe their willingness to go after some economic or commercial targets in part is because they've seen that the tolerance-

John Hultquist:

It's coming to the other direction. Yeah.

Luke McNamara:

Right. Yeah.

John Hultquist:

That's a really interesting case study because a lot of that really early information that was released on 32 was by a Chinese cybersecurity company.

Luke McNamara:

One thing, since you're here, I think would be a good capstone to this series that we've been doing, looking at each of these different players, and I'm not going to ask you which is the most significant threat as I've seen some people ask before, but how should

organizations think about... As they think about all these different groups that exist, these state-sponsored groups, and they're worried about the capabilities that they see. I think in each of these discussions, it's been apparent that they even within the country have different taskings, those specific groups.

But if they're trying to think about them from a risk standpoint, what might be different factors that weigh into their decision-making and risk mitigation strategies where you may be operating from a regional standpoint? How should organizations think about that?

John Hultquist:

Well, everybody's threat profile is different. There are a lot of different pieces that are involved. One of them would be the simplest one, frankly, is where you do business. It's not uncommon for us to see... For instance, one of the things that we've noted with a lot of the Iranian activity, is that it's, say, very focused in region, in the Gulf and the Middle East, versus what we saw very early days when they were carrying out really, really aggressive attacks in the United States. It seemed a lot more of the disruptive, destructive stuff is in that region.

Well, if you're doing business in that region now, or doing business as part of another company, a joint venture or something like that, you might find yourself actually still targeted by Iranian actors, even though they've withheld that from a lot of other places. That's one piece. One of the questions that people have to ask themselves is like, who's part of the company? Leadership often have very public stances. They say things that might change your risk profile.

We've dealt with organizations on multiple occasions who had very vocal CEOs, leaders that drastically changed their threat profile, just based on their support for... For instance, we've seen leaders who are CEOs that were highly supportive of Israel. We've seen the Iranian threat focus in that direction. So higher level politics can figure it into that. And in many occasions, it has. Then their involvement in critical infrastructure. It's important not to have a real narrow view of critical infrastructure.

When we look at the critical infrastructure that we've seen in these adversaries' target, it's not just energy or the lights. Transportation and logistics has been an extremely strong target for a lot of these actors. Broadcasting news, television, that sort of thing. They've targeted that on multiple occasions with disruptive, destructive attacks. And that's important to remember as well

Your intellectual property, of course, will attract certain actors. Probably, but most importantly, is intellectual property that has dual use purposes. We definitely see intellectual property targeted. The stuff that's most targeted really is the stuff that has military applications. Outside of that, I look for stuff that is named as priorities for certain States. China, for instance, names there in priorities. Every country on earth, by the way, will be very interested in biotech till long after, Luke, you and I are gone.

You cannot go wrong investing in the security of biotech because every state right now has recognized that if they cannot figure out how to do their own immunizations or respond to

these crises themselves, they are not going to be able to compete on the world stage. So they're all thinking that right now, and they're willing to steal to catch up. That's a few things.

Luke McNamara:

Well, part of the reason I asked this, because this goes to a conversation you and I have had before, but the role of threat intelligence in not just informing organizations and individuals over a particular incident. Here are the TTPs that were used, the malware, here's what was targeted, etc. But now, especially over the last five years, as you've seen threat intelligence organizations in the private sector, governments talking more openly about this, you've seen that enter the larger conversation.

I think that one thing that a lot of organizations, or even just the general public still has a hard time with is what should I be scared about? Because everything sounds scary. What are the things that I need to prioritize? I think a great example of this is we spent a lot of 2020 talking about ransomware because of how prolific that was to so many different sectors and regions. At the very end of that, you have SolarWinds. Very, very different sort of threat, and from a very different sort of threat actor.

John Hultquist:

Yeah. Black swan, right?

Luke McNamara:

That's continued into this year, with Accellion, with the Microsoft Exchange vulnerabilities. And so I think one thing that you're... And this is something that you are obviously involved a lot in at the company, is helping make sense of the larger trends in this space, in addition to just breaking down the particulars of a specific incident.

John Hultquist:

Yeah. It's a two-way conversation. It's like you've got to understand the threats out in the space, but you need to understand what your assets are that matter to those threats, or in how they match against those threats. You really can't do one without the other. I can feed you threat intelligence all day long, but I can't tell you which one's going to matter the most to you without your help. You've got to tell me because it might be brand. Brand might be your most important asset.

It might be intellectual property that's something's stolen. It could be something that we're not even considering. What was really interesting with the Microsoft Exchange incident was at some point we realized that I wasn't worried about the Chinese hackers and their threat to the unpatched systems because the people that still hadn't patched were mostly small and medium companies. They really had very little...

My dentist doesn't care about like Chinese state hackers. And he probably shouldn't. He's got other things to worry about. There's a pandemic on. But what he should worry about though is when that exploit gets into the hands of the ransomware operators who will ruin

his day by locking up all his files and making his life very complicated. That's why thinking about the threat in perspective of what your own assets and your own profile matters so much.

Luke McNamara:

Another piece of this that I think you see increasingly is, and I'm curious your thoughts on this, is the politicization of intelligence. As an intel analyst or specialist who is using carefully caveated language, confidence levels, and then you see something that makes its way out into the public and you see how politicians or others spin a particular event-

John Hultquist:

[crosstalk 00:40:30]. Yeah.

Luke McNamara:

This sort of problem is not new to threat intelligence. But again, as the discussion around cyber threat intelligence and some of the operations and campaigns and actors that we track are increasingly discussed in more public and general conversations, what would be your advice to analysts, individuals that are involved in writing intelligence and wanting to make sure that they capture things accurately, but avoid having those very nuanced language and analytical assessments mistaken?

John Hultquist:

That's a really tough question. I mean, with reference to the election shenanigans, they came out... I guess, that the ODNI came out and said Russians were pro-Trump, Iranians were pro Biden eventually. Let me tell you something, we knew that years ago, but it was not easy communicating that. It's hard to communicate that without being accused of being partisan. That's a massively complicated problem. It's only worse if foreign actors are engaging our system. But the bottom line is that the problem is the foreign actor. You have to describe the problem as such and stay in the realm of the adversary, and their nefarious behavior.

No matter what side you are on politically, I think the one thing that we should all agree on is that we don't want foreign intelligence agencies involved whatsoever in our electoral process. I think that's something we can still probably all agree on. And so, we have to just define common ground there, especially. But it's a super complicated problem. Because, frankly, it's going to get, like you said, politicized anyway, Like by the media, by politicians who recognize advantage in the way they discuss.

I can tell you one of the ways that I tried to keep things from getting politicized at one point was saying like, "I wouldn't push too hard on one side because there's literally this Iranian thing going on at the same time, and it's a double-edged sword." Right. And that helped in some occasions. But these guys will take the stuff and run with it.

Luke McNamara:

Yeah. It's been interesting over the years to see, even outside the context of things like the collection security, which granted have become more political, unfortunately, but just other topics, putting out reports. I'm sure every organization that has been involved in putting out a white paper or a blog about a certain type of threat activity, that they've tied to a state actor, it's always interesting to see what corners amplify that or what narratives it gets attached onto when they're just trying to report on a threat actor that's doing something.

John Hultquist:

Yeah. And sometimes, honestly, it's not worth even engaging with because it's going to be... The conversation's going to get so tripped up and weird that you just don't want to necessarily be in that space. So you just communicate with your customers and try to stay as far out of that as humanly possible.

Luke McNamara:

To bring this back around to Russia and wrap things up, one of the things that we like to end on... Or first, one of the things I realized I didn't do the first two episodes in this series was ask the people I was interviewing who their favorite threat actor was from that country. Did it for the China. I feel like there's no point in doing it with you because I think we all know what the answer is going to be. But if you want to change your answer...

John Hultquist:

No, it's still Sandworm. No, I find them utterly fascinating still to this day.

Luke McNamara:

The final closing question that I will give you then is, as we're seeing... We talked about some of the current buildup and potential conflicts of the border with Ukraine and some of the other things that they've been involved in the past with respect to Olympics, what might be some things that you'll be looking for this year, that will be interesting deviations or anticipations of Russian threat activity?

John Hultquist:

Well, so we're always worried about that Chekhov's gun that's hanging out, Isotope activity, the airports, and stuff of that nature. I'm always worried that eventually one of two things will happen. One, they'll get the order and do something weird. Just maybe they even test it. Or two, they screw up. When you get into that many places and some of these places are that critical, who knows what will happen.

Luke McNamara:

And we've seen them do that in the past. They've made mistakes in the past.

John Hultquist:

Mistakes have been made. Absolutely. I mean, I'm not sure the WannaCry, for instance, was not a mistake. Three days after they got their hands on that exploit, it was all over the internet with notes and insight. I'm not sure that they had any idea how bad that was going to go. NotPetya I'm not sure they had any idea how far outside... I mean, it was actually built the target within Ukraine, and I'm not sure that they had any clue it was going to be this massive, extremely economically devastating capability.

Mistakes have been made multiple times with the Trident incident. We're not sure that they meant to knock that thing over, that plant, when they deployed their malware. It may have actually just been the act of deploying the malware, which messed up the system and shut the whole thing down. Then goes all the way back to the bonus steel incident, which was like a million years ago where a steel plant came to a shutdown possibly because of a piece of malware that wasn't where it was supposed to be. So I'm always waiting for the accident in that space.

Espionage is not going away. We're having some really serious discussions on how to fight the Russian cyber espionage. Nobody is stopping it. Joe Biden, no president in history will be the one who stops Russian espionage. It's not going to stop. It's not in the cards. So I hope that we recognize that we can't really put an end to this and we start fighting it harder. But we're still going to be fighting it because essentially the United States is doing it to everybody else as well. And it's just too important.

I guess that's the good news for those of us who are wondering what we're going to do when it all went away. I don't think it will. The ransomware problem is getting extremely aggressive. One of my concerns is that it is tacitly approved by the government, if not encouraged by the government. We're going to be in some strange places there, because it's just moving so fast. It's evolving very quickly. And every evolution is an aggressive evolution.

John Hultquist:

It's like you start out with a tadpole and you're ending up with like a crocodile at this point, and God knows where it's going next. They're moving so fast in this aggressive posture, because we haven't found a way to put a break on their economics or any legal costs and legal trouble for them. That really worries me more than anything, that we're going to see more innovation out of there that's going to cause problems for more people and pain for more people.

Luke McNamara:

Do you think with things like the Olympics... We still have that coming up this year. We've got some notable elections, I believe as well in Europe, these other things that we might see more event-driven operations, some of which might dip into that disruptive, destructive activity beyond just espionage.

John Hultquist:

Yeah, I think so. I think with the administration change, there's just going to be more reason for espionage. Right now, administration change, nothing brings on espionage like administration change. It's just like literally overnight, the politics of the United States will do a 180 with regards to a lot of different problems. That means that people need to know... Intelligence communities, intelligence services want to know what the hell is going on. So that's going on as well.

But that might also tell them to retool and get ready to start carrying the stuff out again because things aren't even in a position that they're happy with.

Luke McNamara:

Well, as we sit here recording this at the beginning of April, I think the one thing that we can safely predict is that the rest of the year will not be boring with respect to Russian threat activity.

John Hultquist:

No, never.

Luke McNamara:

I think that [crosstalk 00:48:58] feel fairly confident saying that.

John Hultquist:

This won't be the quiet year. Yeah.

Luke McNamara:

Always great to talk to you. For folks that aren't already, where can they find you, follow you on Twitter?

John Hultquist:

I'm John Hultquist at Twitter.

Luke McNamara:

There you go. Go there for-

John Hultquist:

Or @JohnHultquist at Twitter. I don't know. You get the idea.

Luke McNamara:

Go there for all up-to-date Sandworm hot takes and other information. Take care, John.

John Hultquist:

Thanks, Luke