EPISODE 499

[00:00:01] AH: Okay. Well, I'm absolutely thrilled to be speaking to you today about MSTIC. And I wonder, just to start off, can you just tell our listeners a little bit more about what it is and what it does? And just help us break it down for us. What are you doing and where are you?

[00:00:19] TP: Yeah sure thing so my name is John Lambert. I run the Microsoft Threat Intelligence Center. I started at Microsoft 20 years ago in security. Early on in my career, we had the era of internet worms as we call them, MS blaster, code red and things like that. Some of you may remember in the audience. And those were worms that were exploiting vulnerabilities in Microsoft products. And I spent about 10 years after that working on essentially code quality or improving the security of Microsoft products from attacks like that. And what that led me to was, "Who is behind these attacks that we often call zero-day attacks, zero-day exploits?" which are exploits for vulnerabilities and there is no patch available. And that often led to the world of cyber espionage, and nation state attackers and cybercrime groups.

Today, I run the Microsoft Threat Intelligence Center, sometimes called MSTIC, and that is a group of analysts and engineers that have the skill sets of cyber security. So these are individuals that know how to reverse engineer, that do malware analysis, that understand how nation-state, state-sponsored threat groups hack, and understand the techniques that they use to go target victims and exploit them. And then use the data and resources we have at Microsoft to put tracking in place. Understand what they're doing and disrupt those attacks to protect customers.

[00:01:50] AH: Cristin, do you want to join in?

[00:01:53] CFG: Sure. Sure do. I'm Cristin Flynn Goodwin. I'm the General Manager and Associate General Counsel of Microsoft's Digital Security Unit. So my team works in partnership with John both with a team of cyber security lawyers as well as a group of threat context analysts. I've been at Microsoft for about 15 years. I came into the security space in early 2000 when I moved to Washington, D.C. I left a legal job on the 85th floor of

Tower 1 of the World Trade Center and helped MCI WorldCom build up their cybersecurity practice at a time when obviously there was so much happening and 9/11 was really in the forefront. So I spent a lot of time in DC helping with the First National Strategy to secure cyberspace, and the original Homeland Security Act. I spent time in some operational roles for other telecommunications companies doing national security and emergency response work, and presidential advisory committee engagements, things like that. And so I've been at Microsoft since early 2006. And I absolutely love being a part of the security community. With a 9/11 background, I'm a lifer. I'm here to stay.

[00:03:05] AH: And I must admit, when you put the terms advanced persistent threat and cyber threat intelligence alongside general counsel, it sounds like a bit of a nightmare to be completely honest, but it's not.

[00:03:19] CFG: Absolutely not. No. Because one of the coolest things about being here at Microsoft is that we're looking at all tools to go after these attackers who are impacting our customers. And so if one of those tools is leveraging the legal system and the way in which we can share information through contracts with governments or partners around the world, then let's do it. Let's find ways to continue to be creative and innovative, because these attacks, these advanced persistent threats harm our customers. So yeah, power to the lawyer. It's not a bad thing.

[00:03:53] AH: And John, you were thinking about what's the superpower that Microsoft has. And I wondered if – Everybody loves to hear about superpowers. Could you tell us a little bit more about the superpower that Microsoft has and your founding MSTIC?

[00:04:11] JL: Yeah, sure. So people often think the attackers have all the advantages in this space. But the reality is defenders, we have a lot going for us. Microsoft is the only company or one of the only companies that is a platform company with our operating systems, a cloud company with Azure and an enterprise company. So the combination of those three things together, it gives us the ability to understand what's going on on endpoints all over the globe to know what's going on when attackers come after our cloud customers. And those enterprise customers, those are often in the crosshairs of these attackers. And so if you want to know what's going on with these attackers, you have to

understand what's going on with the victims. And that intersection across all of those three things really gives us the opportunity that we have to go do something about it.

The products and services at Microsoft are a lot of how we're able to intervene and disrupt. We have an anti-virus Windows defender that runs on hundreds of millions of computers around the world. And also it's part of the email protection product that we have and lots of customers run it on-premises. So once we get sighted on one of these attacks, that's an amazing tool to get data and telemetry and also to disrupt those kind of attacks happening on hundreds of millions of computers or what have you. And so the ability to take that intelligence we have and then turn it back into signal that is consumed by our email product platform, the cloud platform, the endpoint products that we have, those are some of the super powers that we're able to go do stuff with.

[00:05:49] AH: And part of the super powers as well is that the Microsoft has eyes and ears all over the world in the form of its software, of its products on computers in numbers in the hundreds of millions like you say. And I wondered if you could just unpack telemetry a little bit more, because I found it quite interesting. Just speaking about attack and defense, you turned something that was seen as a flaw or weakness and re-harnessed it and then aggregated it to turn it into a form of defense. Can you talk a little bit more about that?

[00:06:25] JL: Yeah. One way to think about it is if you're a customer of Office 365 or Azure, you're going through the service at Microsoft to use that product or service. To send information to Azure, you're going through Azure's firewalls and it's front door services. To go deliver a malicious email to an inbox, you're going through the layers of protection that the service has. Those layers of protections are instrumentation points that we are able to go put in detective controls that are able to recognize malicious code, phishing attempts, things that we've identified through tracking these actors. And the attackers have to go through those layers to go after the victims in our services. And that's an example of how we're able to go have that visibility, because they're going through our cloud services to try to reach those customers.

[00:07:19] AH: So it's like you know when you get an error message on your computer telling you that something's happened and then it asks if you want that information to get

sent back to the people that have developed the software, it's like that. But if you aggregate all of that information together, then you can start to find patterns and detect who's doing this type of stuff. Is that right?

[00:07:43] JL: That's right. And if you understand how to look at data from a security perspective, you can often learn things that are actually an attack in disguise. And understanding the difference between what's an attack and what's not, that's what we try to do.

[00:08:02] AH: One of the other things that I find quite interesting is help us understand the role that MSTIC plays within Microsoft. So say, for example, it's the Office of Special Investigations. And we can think about where they are within the role of the U.S. Intelligence Agencies or something. But Microsoft, 8 million square feet, 50,000 employees, a trillion dollar company. Help us understand like where is MSTIC in relation to the organization? And where is it housed? And yeah, just give us a better understanding of your unit.

[00:08:41] JL: Okay. Yeah. So one way to think about MSTIC is, at Microsoft, we believe that security is a team sport. And so my team, which I'll describe in a second, where we sit, we work with all of the other security teams around Microsoft to go deliver protection and disrupt threats. The part of the thesis behind why I created my team the way I did was a typical approach is to have security teams embedded in our products and services. And we absolutely have that. We have Azure. There's an Azure security team. We have Office 365. There's an Office 365 security team and so on.

I knew we needed a team focused on the adversary. Wherever the adversary went, before they ever attacked you, after they were done attacking, you need to follow them all the way through their life cycle and study them. Actors study us. They study our customers. They study our technology. So we study back. And by understanding what they're doing through their full life cycle, you may see them coming before they've ever launched their attack and able to disrupt that. Or you may understand who they're going to go after next. And so that was part of having a team that was focused on threat intelligence, focused on the adversary. And then using that and working with all the other security teams across

Microsoft in that team way to take what we're learning about them and then go disrupt and intervene and protect Azure customers, Windows customers, you name it.

[00:10:07] CFG: And so then we evolved that concept to take the threat intelligence and build out threat context. And so that's where my team in the digital security unit comes in, because John is expert at looking at who is it behind the attack and how are they executing the attack? And my team will look at why. What are the motivations for the attacker? And who are the victims? So that that way we can understand the holistic view of the attack so that we know it is this nation state actor and they are geopolitically motivated. There's a bilateral negotiation coming up. Or it's Russia, the Ukraine. There's a big Ukrainian holiday coming up. So we're going to watch the Russians go after some infrastructure in Ukraine and make life difficult heading into a holiday weekend. So we're looking at the why of the attack and who the victims are so that we can then go share information back to customers and to the world to help really understand the macro view of why are these attacks happening.

[00:11:09] AH: Wow! That's fascinating. Here at the Spy Museum, we look at some of the motivations that people have for spying. And there's an acronym, MICE, money, ideology, coercion, ego. Is there something similar for the reasons why people do this stuff, like money obviously, ransomware, whatever, ideology? Maybe you're trying to defeat liberal democracy or something? And then, I guess, some people just want to see the world burn. Some people just do it for badness. I remember when I got my first email account with Yahoo and someone said, “Yeah, you need to be careful of viruses.” And I was like, “What?” And they're like, “Yeah, there're these viruses.” And I’m like, “But why do they do it?” They're like, “They just do it because they just do it.” I couldn't get my head around it. But yeah, I mean, that's another one. People just do it because they just want to be destructive. So help us understand a little bit more about how you sift through and analyze and categorize all of those various motivations, Cristin.

[00:12:11] CFG: Sure. So there're different tiers of attackers, right? You've got the hacktivists, the types that are harassing people with their Yahoo accounts and spam and a lot of cybercriminal activity, ransomware. Those are big categories of attack activity. Where we're focusing on is the pointy end of the spear, and that's the nation state piece, because

you tend to see that when nation states are investing money and resources to develop new tactics and new techniques to go after targets, then that gets out into the ecosystem and others will follow, right? Why reinvent something new when it works so well?

So when we're looking at nation states, and that's really the brilliance of John's team, is that they're experts at finding the needles in the haystacks of these nation state actors amongst the data. What we see in the why and the victim space is that these are intelligence taskings. Just like in the good old spy versus five days where you'd have a target and a collection and a mission. Now we can do that all digitally, remotely. It's completely changed the game.

And so you'll see if there's an upcoming negotiation about a major treaty, or if there's a G7 meeting, or if there's a geopolitical issue like Covid. You'll see nation states targeting health information. Or they're going after virus information, or it's related to an issue of importance to a government. So that's why what's so fascinating is that we see so many think tanks and policy shops in the victim space right now is because the intelligence collection priorities of governments is aimed at what's the other government going to go do? And so they're trying to gain access to that information. It's a really fascinating space.

[00:13:54] AH: It really is. And I want to get back to offense and defense in a second. But you mentioned geopolitics there. I mean, it sounds like – I don't know. It sounds like really fascinating. You've got people like John with his skill set. And then it sounds like you have a team that's boned up on Geopolitik. You mentioned Ukraine people following elections in Ukraine and so forth. Yeah, tell us a little bit more about that, about are you recruiting now people with international relations PhD's, because I'm on the mark. I'm just teasing. My boss is going to listen to this.

[00:14:35] CFG: Well, the applications are open. Yes, so we've been hiring threat context experts. So what we look at is a range of intelligence background, your experience in analyzing data from teams like MSTIC, technical information, being comfortable with that. And a deep understanding of the politics of a particular country, region, their political interests and influences, their sphere of influence, and then language skills. It's really important to understand not only being able to read political and technical and hacker slang

in local language, but to be able to then help us contextualize that. And so we bring those skills in to support the MSTIC organization. Right now we track what we call the big four, most attacks come from Russia, China, Iran or North Korea. So we've got geopolitical intel and language experts for all of those domains. We're always expanding.

[00:15:35] AH: Wow! That's fascinating. And I just want to go back to offense and defense, John. Can you just help us understand that a little bit more? And feel free to use whatever sport you wish to try to help us understand it. It could be tennis. You get defensive players and offensive players, or soccer, football, whatever. Help us understand that offense defense kind of dynamic. And maybe the best way to do this is to give us like an example of solar winds or something else. Give us an example to hang our hat on.

[00:16:09] JL: Yeah, sure. Like Cristin mentioned, one way to think about my team is a bunch of computer scientists that understand these attacks that understand the world by reading The Economist. And we know that we need a deeper understanding of geopolitics than that. And that's an example of why the partnership with Cristin's team is so important to us to know why these attacks are happening and contextualize them.

An example of an attack that we identified was earlier in the year there was an actor based in China that had exploits for Microsoft Exchange, which is our email product. We discovered through our tracking of this actor that they had these exploits and they were for vulnerabilities that were new. And we worked with the security teams at Microsoft to ensure they had the technical data to understand them so they could patch them.

Other security organizations around the globe also discovered that there are other security companies that are protecting their customers that see attacks against them, Veloxity and others that also send in that information as well. And the Microsoft response apparatus, which is like there's this latent DNA that all Microsoft responders have to just when a crisis happens to just mobilize. And we work together often so we know how to do it. We know how it works. And for that, Microsoft worked to put out patches for exchange.

And one of the things we found was that there are a lot of customers especially in small and medium business who had not been updating their Exchange products. And these are

products that they run on-premises themselves, which is different than, say, Office 365, which is run by Microsoft and was not affected by this vulnerability. So we needed to put patches out for versions of exchange that we had stopped supporting years ago, that they could just apply that pinpoint fix for. So the product team ultimately put out, I think, patches for over 20 different versions of Exchange to support them. And then we also put out one-click tools that would mitigate this exploit for customers that didn't have the IT staff to even put on patches. If that step was too hard for them or too complex, this was a one-click tool you could download and run and it would mitigate these patches, these exploits.

[00:18:31] CFG: If I could add in there, John, like one of the cool things about that one-click tool was that we were partnering with the White House at that point in time. They were really focused on how do we help get simple tools into the hands of small and medium-sized businesses that really don't understand the complexities of exchange? Because if they hadn't updated it since they installed it, they really weren't going to be well-equipped to do a lot of heavy engineering. And so that was the really cool partnership between the White House and the teams involved in this really extraordinary response was our ability to come up with a technical solution that was really simple and easy to use to help address something that was really complicated.

[00:19:15] JL: And then one final uh comment on that is while, originally, these exploits were in the hands of a group we call hafnium. Every group that we track, we assign a name from the element periodic table. The attacks that really started to see and gather, and this is the nature of offense and defense, were performed by copycats. And so as the information about the vulnerabilities becomes public, they reverse engineer patches, you start to see these copycat attacks by cybercrime groups, sometimes other nation state groups that want to quickly use the closing window that they have on exploits before the world patches. And it's really that those copycats that have attacks where most of the volume is. And that's the race to what if a ransomware gain starts using it? What if some other volumetric attack starts happening that can outpace defenders?

So while we are initially in this sort of cat and mouse game against these nation-state groups that are doing low and slow attacks that we talked about earlier, the derivative

attacks that we see by copycats is really where most of the volume and harm takes place. And that is the race that we're in every day to make sure customers stay ahead.

[00:20:29] AH: It's really fascinating that, yeah, it's a constant cat and mouse game every day. And I wonder if you could just talk a little bit more about how all of this shakes out in terms of like the different actors that you mentioned, Cristin, so Russia, China, Iran and North Korea? Why is MSTIC looking at them? Is that like a tasking in partnership with the government and they've asked you to look at them? Or is that just your setting looking at Microsoft products and that's where most of the attacks are coming from? Or, yeah, help us understand that kind of like matrix.

[00:21:05] JL: A simple way to think about this is we look at where our products are used by customers and we look at attacks against them. As customers move from on-premises where they were the ones that had visibility into their attackers, as they moved from on-premises to our cloud services, they brought their adversaries with them. Their adversaries didn't lose interest in them when they moved from their castle walls into a cloud service that Microsoft operates. The adversary said, “Okay, well, let's go understand how to attack them there.” And that brought – We track over 70 different threat groups from over 20 different countries in my team. That's a sign of really the broad global customer set that Microsoft has and the diversity of threat groups that are out there that are coming after them. And so in a way, it's the attacks on customers that decide why we focus where we focus. And those attacks that are coming after them is really what's driving the volume, the priority, and you name it.

[00:22:10] CFG: And so once John's teams identified the attacking states, then my team will get involved and we'll look at how are we notifying our customers. One of the things that we do in partnership with MSTIC is oversee our nation state notification process. So we track data. Now that's one of the great things about the instrumentation of this. And the telemetry that MSTIC gets is that we're then able to create our own database of the attacks and understand what the volume looks like.

So going back to August of 2018 when we started keeping data, we've notified over 43,000 customers either a targeted attack or a compromised attack from one of the nation state

actors that we track. That's where we're able to, using data, come back to say the majority of attacks were coming from the big four, from Russia, China, Iran or North Korea. Because out of the 70 major attackers and the 20 countries that John sees, by volume, it really whittles itself down to a small number of countries on repeat.

[00:23:17] AH: And that sounds like a phone call you really don't want to get. You're being attacked by some of the most sophisticated hackers on the planet who are backed up by the Russian government. It's going to take the edge off of my Thursday, that's for sure. How do you notify them? And yeah, help us understand that a little bit more.

[00:23:39] CFG: Yeah. Well, we won't show up at your door, but we'll figure out how to get in touch, right? So for a consumer accounts, we see a lot of nation state activity against consumers, consumer accounts because, of course, those are our people that may have geopolitical roles, but they have personal accounts too. So we'll provide electronic notifications to many of our consumer accounts. Or we will use the secondary or tertiary contact information in profiles for our enterprise customers that are attacked. Every enterprise customer tells us who they want us to work with in the event of a crisis. So we'll contact that person. If we believe that we cannot contact them by email because of compromise, we will call them and find a way to get a human on the phone.

There have been a small number of times when people didn't believe us and we've had to call back and say, "No. Really. We are Microsoft and we're calling," and we'll help them validate who we are so that we can have that conversation. Because the most important part is for us to give the victim information that they can use to help protect themselves so they can either identify the attack or put some protections into place, because what we don't want to see is a repeat of the attack.

[00:24:56] JL: Part of what I was just going to add with these notifications that's very valuable is an attacker can change up how they attack. They can come up with new techniques. They can move on to new methods. But the interest they have in their targets is often evergreen. They're going to come back. And so these notifications are often turned into a basis for partnership with these organizations that are repeatedly targeted. And that's very valuable from a threat intelligence perspective, because we know the attackers will

probably come back there. And if we have a relationship with that organization and they're able to contact members of my team or members on Cristin's team when that's happening, we have an opportunity to understand about the new attack, the next attack. And often we'll use that, those insights that we get from that, to go spider-out, pivot around and find out more about the breadth of what the attacker is up to now. So it's yet another tool in the toolkit that comes from this very valuable program.

[00:25:55] AH: Wow! A few, like maybe a month ago or so, we had the Acting Director from the National Counterintelligence and Security Center on SpyCast. And he was saying that after the episode, people were getting in contact with them looking for advice and help. For you, like for customers, for small business owners, for people in the IC out there listening to this podcast, yeah, should they get in touch with you? Is there a way to do that? Or like are you kind of doing something separate by tracking the adversaries? Yeah, help us understand that a little bit more.

[00:26:35] JL: Yeah, maybe a couple of ways to answer this. So one is we do have regular communication paths with the cyber security industry, those companies, the major platform providers. People you think, "Hey, you compete with Microsoft," and somebody say perform. Clearly, you don't talk to them, or cooperate with them, or work with them. And I think you'd find that a lot of people that work security, security gets in their blood. We all face common adversaries. We all see the adversary from our own perspective. And I will tell you the analysts that track the threat groups from whatever country, they all know each other. They all talk to each other. And we have ways that we collaborate across lines of competition across countries and so on. So all that is there.

If people find vulnerabilities in a Microsoft product or service, there's a program we have called CVD, which is really about coordinating with Microsoft to tell us about those vulnerabilities so that we can fix them in our products, make customers aware of them and do that in a coordinated way that tries to minimize the harm from these copycat attacks that we talked about. So that's another very important program that we have. Those are some of the ways that we reach out to people. Probably that's customer of our products or especially a customer of our security products that builds in a flight path back to Microsoft.

[00:27:56] CFG: That's the most traditional path. I'd also encourage for any of your listeners that are in the U.S. government to contact the major coordination centers. If there's something that's kicking, CISA and the Department of Homeland Security is there to help coordinate on the civilian agency side. Obviously, DOD and the other agencies in the intel space have their own cyber coordination capabilities. And so that's where reporting inside the federal government, they'll use their traditional channels to be able to reach out just like they do.

It's really terrific. John brought up coordinated vulnerability disclosure. We love it. If somebody finds a vulnerability and then they report it, and we've given credit to the NSA when they've reported vulnerabilities to us that we can then go and repair. And we give them credit and coordinate our response there. We've done that in the past with GCHQ as well. And so we love getting reports into our traditional channels and support mechanisms to help us. And those who are invested in the day-to-day of security response for the U.S. Federal Government, other countries, they know how to get in touch with us too.

[00:29:11] AH: I want to pick up on something you said earlier, Cristin, about the game changing. To me, this is like so fascinating. To me, with the invention of the aircraft, it meant that civilians could be on the front lines, because aircraft can bypass the front line on the ground. And it seems to me in the cyber era that every citizen, everybody with an iPhone, everybody that's connected to the Internet. And one way or another is they're in the game much more than they used to be. In the Cold War, maybe, say, you were a corporation that that was developing advanced aeronautics. Then, sure, people could try to steal your blueprints or something. But now, yeah, it seems that more people find themselves on the front lines of this kind of ongoing struggle. So I guess I just wondered if you have any thoughts on that, because like infosec, like information security, used to predominantly, like you say, spy against spy. It would be locked up in the Russian embassy in D.C. It would be locked up in the State Department. But now it's out there. The lines of battle are broader. More people are involved. Help us understand, yeah, just your thoughts on this change in the game that you mentioned, Cristin.

[00:30:29] CFG: Sure. Well, obviously, governments are spending billions of dollars in cyber offensive capabilities, right? So that traditional inside the four walls of an intelligence

agency in Russia or China, that hasn't changed. That's just a part of the game. One of the big things that's changed has been the inclusion of a of a community or growth of a community that we call private sector offensive actors. You're seeing smaller countries that don't have the tools necessarily to do their own surveillance operations, or information exfiltration, or monitoring. They will contract with these companies to provide them services.

And there's been a lot of attention being paid to this space recently, even as recent as September 14th. Apple was pushing out an update for a vulnerability that was being used by the NSO group, an Israeli-based company. That's Pegasus Software has been involved in surveillance of human rights workers, journalists. There're lots that's been published about this. And they're involved in litigation with WhatsApp for a vulnerability that they had also leveraged there. And we contributed to that lawsuit and filed an amicus brief back in December of last year talking about the harms that these types of companies perpetrate.

We saw, I think it was September 15th, the U.S. indicted or had reached a negotiation agreement with several individuals who had been a part of the U.S. intelligence community and then had gone to work for companies in the UAE violating their obligations to protect U.S. information. So it's a fascinating space, right? You're seeing the growth of money coming into this, creating tools and technologies that can enhance a country's capability or law enforcement capability, because law enforcement now is moving into the domain that had been that of the intelligence space. So is forcing us to have to think about.

And Microsoft is really leaning into the global conversation about cyber peace and the norms of government behavior and appropriate behavior in cyberspace and the harms that these technologies can create when unchecked, because it's one thing if you're seeing a very small use, one major country against another major country. But when there's a broad market for it and venture capital starts coming in, it really changes the tone and tenor of the space. And so that's an area of concern for us.

[00:33:06] JL: I was just going to add, Cristin, that a lot of what we've talked about attacks against sophisticated organizations. And we have a lot of consumers that have to worry about cyber threats as well. Anything that comes into your inbox, is it a phishing mail? Is it

something you should or shouldn't click on? And everybody, you have to have a password for all these different websites these days. Everybody hates having to manage all these passwords. The only people that really like passwords are criminals. Because people – If the password's complicated enough to be secure, you're not going to remember it. If it's simple enough to remember, it's not going to be secure. And so you have to have solutions for just these everyday problems.

And just this week we released new features that allow people to just not have passwords anymore for their Microsoft accounts. You can use a secure app like an app on your phone or your phone itself to approve logins to your account. And that's just a much more secure basis than people having to remember yet another password they're probably going to reuse on a dozen other sites. And if any of those sites gets hacked, your main account is now vulnerable. So solutions like that that make it kind of easy for sort of everyday main street users. And everybody, every Wall Street user is still a main street customer in that sense, right? We all have our personal accounts that we use. And those are very important to us. Providing solutions that work there too is very important.

[00:34:33] AH: I mean, it seems to me that it's almost like calling for a whole of society approach. And I just wondered, obviously, you guys are doing the lord's work, and there're other agencies that are involved. And there's people out there that are trying to protect just **[inaudible 00:34:51]** public on the street who's gone about his business. But how do we get towards the stage? Or is that somewhere where we should go where we have everybody being at some level a cybercitizen who's doing their good part to make sure that cyber security in the United States or/and it's allied countries is all it needs to be?

[00:35:16] CFG: Well, there's certainly an action and reaction going on in the geopolitical space recognizing this conundrum, right? You see that the Paris poll and the tremendous energy that's come up with the countries and commercial signatories that are recognizing the need for norms of behavior in cyberspace and how governments need to exercise restraint and minimize impact. Absolutely, right? Microsoft has been at the forefront of those conversations. And I know we plan on being there.

At the same time, you're seeing major investment from governments coming into the offensive capability space. And we saw in China, it went into effect September 1st, some of their new vulnerability of reporting legal obligations for Chinese companies. So you're seeing China wanting more vulnerability information. So that's where if you're thinking about the balance of building offensive capabilities and the need for defense, it really highlights the important work that John's team is doing. The ever vigilant side and the products and services we have like the Microsoft Threat Expert Service and other tools that we're bringing to the table, because money is coming in, governments want to expand their ability to see and not have to put people in harm's way from an intelligence collection perspective. But at the same time, as John said, and I completely agree, these are attacks that impact people. And at some point there will have to be some international détente on that issue. And until that happens, Microsoft will be in the middle and trying to lead that conversation where we can.

[00:37:00] AH: And a slightly playful question, does Apple have a similar unit to MSTIC that's gathering in data from all the Macs, and all of the OS, and all of their operating systems and software?

[00:37:14] JL: It's really hard for me to comment about what they do. They certainly have security people. They respond to vulnerabilities. They're affected by some of the same attackers that Cristin talked about earlier. And they have cyber ranks over there. We know some of the security folks, yeah.

[00:37:30] AH: One of the other things that I find quite interesting is if you look at the history of intelligence over, say, the past 100 years, quite often the places, the nodes and the system that are most critical are a place that is the focus of attack. So I'm thinking of people like Filby Ames, Robert Hansen. I mean, you couldn't make some of this stuff up. Like the person who's responsible for running Russian counterintelligence just so happens to be a Russian agent. So I guess that's like a long-winded way of saying do you have to run your own kind of counter-intelligence operation to make sure that MSTIC and the people that work for, your buildings, your physical infrastructure, to make sure that's all secure and that's all safe?

[00:38:22] JL: Yeah. Maybe a way to address that is to become a Microsoft employee you go through screenings. Obviously, if you're an employee that handles any kind of data that is classified, you have to go through those processes. We have a fairly rigorous process at Microsoft when it comes to rules around access to data. And part of those controls and rules are technical controls. Part of those controls are a separation of duties between what investigators can do and then what actions can be taken based on the investigation. And we work with members in the legal team to decide sometimes the right course of action to take based on what findings that we have. And that partnership kind of across the divisions across the roles and responsibilities are part of how we make sure that we're honoring the obligations that we've made to customers. Working to keep them safe, and trying to give adversary setbacks.

[00:39:17] CFG: All of those are important elements of basically what we call our insider threat program, right? And so we don't have the same issues like Alder James and the counterintelligence types of operations like that where you you've got the Kim Philbys of the world. But, absolutely, insider threat is an issue in the private sector and one that we take very seriously. So all the elements that John described and others are central to how we think about those risks.

[00:39:51] AH: And I read somewhere online that you have people that used to be in the intelligence community as part of the team. And they circulate throughout the security world. So I wondered if it was just the case of they've applied and they happen to be an intelligence community. Or if those are skill sets that you're looking for or types of people that you're actively seeking out?

[00:40:15] JL: I'll say not exactly. A lot of the folks that are in my team come from a technology background. They come from incident response. That practitioner world is very helpful. Speaking for myself, I never worked for any government. I got a computer science degree. Went to work at IBM outside of college. I fell into security there, because as the new person, I got the last pick of what to work on. What did nobody want to work on? Security. And I fell in love with it, attack, defense, cat and mouse, the perfection required, all of that stuff just got into my blood. And then when I came to Microsoft, started in security, and understanding the technology in our customers and then thinking of how

attacks manifest on that. That's the DNA that we look for, that passion, that ability to work in a team way across the company and across. As much as I can have a hundred stories of amazing behind the scenes stuff, it is this work with other companies with target organizations and governments that really help us put this picture together and work this problem every single day.

So you might think, “Oh, you want everybody that has done this professionally before for a government.” Not so much I would say. That instinct, those investigative instincts, that technological higher-order bit, those are the things that we look for, that passion.

[00:41:42] CFG: Now I do hire out of the intelligence community, because the skill sets that I often need require a lot of experience in parsing intelligence, lots of disparate data sets. And then coming up with a narrative, and marrying that to the geopolitical often is a skill that is best honed inside the intelligence space, because as far as we know, our threat context and analysis team is the only one in the world. And so we are drawing from those skills, which has previously been the domain of government to think about how do we mimic those skills. And so that's what we're trying to learn, is not to be an intelligence space, but how do we write? How do we communicate? And how we then communicate to the world? And so that's really the types of skills that I’m looking for when I’m hiring, is the writing experience. So we've also looked at people with a lot of writing backgrounds too.

[00:42:43] AH: I mean, one of the interesting things that strikes me just based on our conversation is the levels of translation that have to take place. So to go from zeros and ones and to forming a picture where you're looking at specific actors or countries, and then that could be – We're talking about different languages, like you said, Cristin, Korean, Mandarin and so forth. And then that has to be translated into a narrative, which inevitably compresses, and edits, and selects, and privileges certain types of information. So I guess just across that whole kind of panoply there, just help me understand how information gets passed off from your team, John, over to Cristin’s and vice versa, or out to the company.

[00:43:38] JL: Yeah. Sure. So you can think we approach this space both top-down and bottom-up. Bottom-up might be our tracking work helps us understand attacks are taking place. They're trying to guess the passwords of a customer at Microsoft or trying to deliver

a malicious phishing mail or malware delivery. And from there, we already have some understanding of what group may be behind it because of the tracking work we did ahead of time to discover that activity in the first place. And then who is the victim organization. And do we have some understanding of why they may be targeted? In some cases, it's completely obvious from history or based on traditional geopolitical purposes. In other cases, it's not clear why they're targeted, and it takes some work to understand, “Oh, that's some obscure company in the supply chain of something-something. And that's potentially the reason why.” And pulling that picture together, especially with the why this why now perhaps. Like what is going on that this is happening at this point in time? That's where working with Cristin’s team. And they see all the attacks that we discover and uncover. And they are there helping zoom-out while we're working the technical, because knowing about the attack is one thing, but you have to do something about it at the same time if you haven't already. And my team is often focused on those technical. But Cristin’s team is there to go take the pieces of, “Okay, what does that mean? What is the picture going on with that? And what does that mean is going to happen next?”

[00:45:06] AH: Do you have any thoughts on that, Cristin?

[00:45:10] CFG: I’d add to that that like when we were in the SolarWinds attack, for example, thinking back to this December, John's team was doing some brilliant Olympic-level gymnastics to go through data to find. Like how did the attacker get from this on-premise environment into this this victim? And my folks would then step back and look at all of the victims to say, “Wow! Look, there's a real focus on the IT sector here. What is this Nobelium actor going after? And how do we talk about that?” And you could see that in the blogs that Microsoft was releasing where we were sharing with the world, like, “Look –” I don't remember off the top of my head the percentage of victims that were in the IT space, but we were breaking it out by country, by sector so that people could understand what was Nobelium going after. Why and where? And so that was really interesting. And so that's what we'll do, is once they've found that needle in the haystack, we'll record it and run with it and see where it takes us.

[00:46:12] AH: Wow! And one of the things that I was wondering as well, John, given that you're kind of zeroing-in on these actors on a daily, weekly basis, how are these – For

people out there that are maybe still running a Cold War operating system, help them understand the new information security kind of environment. We often hear in the newspapers that they're affiliated or linked to, say, the SVR or Chinese intelligence agencies. Maybe through an example, help us understand that. Like what does affiliated mean? Does it mean that they look the other way or does it mean that it's basically a proxy and they're running a program and it's kind of off the books but kind of on the books? Or is it something else? And where are these people getting the skill set? Do they go to like – Is there like a Russian intelligence course for black hackers or something? Or is it just is it just something that they're picking up? Or, yeah, just help our listeners that are kind of not as familiar with this world just understand these dangerous actors that are out there.

[00:47:24] JL: I would say it really varies. No doubt some of these people are government employees. They work nine to five. And you can conduct what's called a pattern of life analysis of the attacks and go, “What days of the week is this occurring? What time of day? What time zones is this occurring?” It's not attribution. So don't think it's the same thing as that, but it's a data point. And you can tell, as Cristin talked about earlier, sometimes on certain holidays, national holidays, there's no attacks that day. They seem to knock off after 5pm or what have you. So some of this tells you this is a nine to five job for some of these folks.

For other cases, it seems to be a nighttime job. So they have a daytime job. And at night, their hacking skills are put to effort for enrichment purposes. And they use that to go hack companies to enrich them and their group of hackers. So it really does vary across the globe. A lot of what we're trying to do is track an actor from the perspective of if you think about an actor or an attack having four different components, one is what is the attacker after? The second is what victims are they going after? Another is the infrastructure they use to conduct their attack, the IP addresses and servers and all of that that they use? And then the last component is what capabilities do they have? What malware? Do they have zero days? What are the tools and those techniques? Those four components, and you look at them together and analyze them across many different attacks. You get a sense of, “Okay, this is the capabilities of an actor.” And then once we understand that well enough, we will assign them a name from the periodic table and we'll have a Nobelium, or we'll have

a Strontium or, Thallium or what have you. And that's really reflecting the maturity of understanding that we have on how this actor operates.

Who that person is behind that group often is not necessary in order to track their activity. Do they wear a uniform? Do they wear a tie? Are they sitting in a basement? You need to necessarily know that step in order to continue to track their activity. And to defend customers, what's really important is tracking their activity, of course.

And then it is often or frequent that we will track an actor and some other authority, sometimes the United States government or someone else. There'll be an indictment. Well, they will go that further step and say, “Hey, this attack on this entity which we saw and observed,” they will do that level of attribution on. And then that's sometimes how these things are linked.

[00:50:01] CFG: And that's a really important point, right? Because what John is drawing a distinction in is that Microsoft needs enough information about activity groups and actors to be able to protect our customers, whereas if you're moving into that law enforcement space, attribution down to a person for the purpose of bringing someone to justice, is not generally something that the commercial market space needs. And so that's really something that needs to be in the domain of the government. And so governments need to be focused on that level of attribution and using their legal tools to make that happen. That is not something that Microsoft is pushing into because, of course, that is not something that we need to help protect our customers.

[00:50:45] AH: So with something like cozy bear, you're looking at what they're doing. You're not necessarily trying to say this is who this is, or they're a Russian intelligence or they're not. That’s something for the government. Is that correct?

[00:51:01] CFG: Well, in order to attribute back to an individual, that requires subpoena powers and legal authorities to be able to gain access to information that we don't need in order to do the things that John's team is talking about, writing the protections that help us with our customers. So those legal authorities are best left in the hands of governments.

[00:51:23] AH: And I just want to go back to something you mentioned a minute I go there, John. You said amazing stories behind the scenes. Can you share one with the spy cast listeners?

[00:51:32] JL: Sure. I mean, maybe one example from this last year that happened with SolarWinds was FireEye was really the first company to break the story on this attack on their attack. We learned that they were attacked because individuals there reached out to members of my team to help investigate it. Why would they do that?

Part of this goes to no one company can do this alone. And those individuals knew folks from my team. Some of them were former employees from over there. They had trust relationships. And in a crisis, you're going to call people that you trust. And that's going to happen across, like I said, lines of competition, because you trust that person, right?

Now, what can Microsoft do? We can take the specific elements of the attack that they were seeing. And in cyber security you know. You're not seeing everything. You cannot guarantee you're seeing everything. You have enough humility to know that. So you want to always try to get the bigger picture, right? Because if you remediate and try to block an attack, and you've only done part of it, the attacker is still there. So you want to gather as much information as you can in order to be successful. And they can take what they're seeing locally and work with Microsoft and what we're seeing globally and try to get a better sense of what's going on and then hand them that information back so that they can go better protect what's happening to them. And that kind of partnership, I was there early when that was happening, the back and forth that's happening across the multiple levels of interactions between the companies and organizations as we're identifying this. And then our teams working together and their brilliant work to identify, “Hey, it's the SolarWinds software that has a problem. That's how they got in.”

And what does that mean? How broad is that problem? Was it something very tailored just for them? Or was that method of access happening to all customers of SolarWinds? And where did that go? And that's really where we could work with them and try to understand, “What's the breadth of this? What does that mean and how far does that rabbit hole go down?” I would say that that several months while that episode was going on, I sort of

measured the day by, “Was this a day I could get out of my pajamas or not?” That's how busy every moment of every day was working this thing. But those events are what people in this space are ready for. That's what they are here to do. Again, as much as I can tell you, Microsoft has a lot of great people, we do. But it is those partnerships with other companies and organizations that's so vital that's part of this.

[00:54:13] CFG: One of the things I add is that when you look at other organizations or other sectors, they'll talk about industries and groups. Security calls itself a community. And so when you see an incident like SolarWinds, it's all hands on deck. And so that's the cool thing, is John's right. When you've been in your pajamas for two days and you haven't left your keyboard and you're exhausted, you know that if you pick up the phone and you call somebody in another company, they're doing the same. And so that focus on protecting the customers, understanding the incident responding to the crisis, that runs so deep that you sort of don't notice it until you sit up and realize it's dark out when you thought it was nine o'clock in the morning.

[00:55:00] JL: I remember a conversation with Kevin Mandia, the head of a FireEye where this was several weeks, several weeks after it had all started. And I told them when they reached out to help for people on my team, they worked FireEye’s breach as if it was their own they felt. That level of personal involvement and commitment and interest to it. And they work nights and weekends to try to pull what they could together for it. I just think that kind of sense of mission is something people would probably not be surprised to find is common in the cyber security space. It's just very important.

[00:55:37] CFG: And we all had to tell the world about it. I think John might remember the number. I think it was like 32 or 33 blogs by the time we had finished the incident and communications was really front in our minds, because it was such a big, big incident. And that collaboration was such a huge part of how we responded.

[00:55:58] AH: One of the things that I’m hearing, and I don't want to put words in your mouth, but one of the things that I’m hearing is that like members of your team, they kind of appreciate and enjoy the game of blocking attacks, defending people, the intellectual stimulation that comes along with it being a dynamic and fluid field. But there's also an

underlying sense of mission and of service. And I haven't been paid by Microsoft for saying that, but I don't know. That's something that I'm picking up. And we often hear of like that kind of mentality and the intelligence community. Sure, it's the government. They don't get paid well. But they could get good benefits. But they have the sense of mission. But what I'm hearing from you is there's also a sense of mission in MSTIC.

[00:56:56] JL: That's right. I mean, in cyber security, there's a good guy, there's a bad guy, and the responders and defenders feel like that's our role there to go out and try to unravel and disrupt this and protect customers so they can go about their lives and their business. And the pursuit that, that hunting, the intellectual exercise that are in there, it makes these people tick. It is part of that investigative puzzle. And when they get a breakthrough, it is thrilling. And even when the breakthrough means look at all this bad stuff that's happening, for everybody else that might be a bad day, for us that is something we're ready for and pursue every single day. And then we can go do something about it.

[00:57:40] CFG: But we're so proud of all these teams, right? It's the Microsoft Security Response Center, it's the defender teams, it's the individual product teams that are involved. Yeah, there's a huge sense of community and a huge sense of the fact that we are all on this mission and we're not going to stop until we have remediated the threat. And that goes right up to the top with our execs, right? When we were having daily calls during SolarWinds, I never thought I'd be on a call with our senior leadership team wearing a baseball hat and the same fleece two days in a row. But it was because we were all in, and the whole company was. And so that's really exciting when you know that an incident is so important that it requires everybody to bring their best.

But the amazing thing about John's team and all the security teams here is that they do that every day. I mean, it doesn't matter what the incident is. They're still bringing that level of effort and energy. And so it's been a privilege to work with them as their lawyer, and now in the threat context space, because there's no better place to be. You're a responder all the time.

[00:58:45] AH: I mean, one of the things that I find quite interesting as well is with like information with intelligence, one of the things that I've thought about, and indulge me, to

me, if information – And this is kind of a little bit of a cliché. But if information is the new oil, then America is the Saudi Arabia of that kind of game. And because of its corporations, because of its universities, because of a whole variety of different reasons. But I guess what I'm trying to say is how does that feel where when it was about oil it was about the U.S. government, it was about the military. But now that it's about information, that kind of – Some of the onus or some of the responsibility has been pushed on to corporations that have the expertise to be able to deal with some of this. I just wondered if you had ever thought about that, the way that you're doing something that maybe not long ago it was the domain of the government, but now as a corporation. Yeah. I don't know. Any thoughts?

[00:59:58] JL: I would just say that this world has always been a public private partnership. Anything that you could probably say, even oil, like you talk about, there's probably public private companies going back. And every country is responsible for that. And certainly everybody's information is important to themselves and they and they should be able to protect and they should have a right to privacy on it. And it's important that we work hard as defenders to make sure they're able to do that against the face of very sophisticated people pursuing what they have. And if there's thing I guess your listener should know is there is no one company that can do it alone. Everybody needs to do their level of responsibility and set very high expectations for them and be aware of what's at stake. But it is that working together across public and private and within the industry that is just such an important part about this.

[01:00:51] CFG: I'd add that we saw a really big wave of digital transformation because of the pandemic as people had to shift their lives to working from home. And that meant a lot of people moved to cloud services in domains and in areas where they probably never thought they were going to right away. So that digital shift is going to continue to put pressure on the migration to the cloud. And frankly, that's wonderful, because we see nation state attacks, because we see them in the cloud. If you're thinking about security from an on-premises perspective, I can only see what goes on through your window. And if you close your blinds, I can't see inside your house when you come into the cloud or at least the condo manager. So we have a sense of the types of attacks that are coming in and impacting our customer.

As the world moves into the cloud, the numbers that we see are only going to go up. But that's not a bad thing, because what that means is that we're actually identifying the issues that were there all along, as John had said. And so the importance of digital transformation is that it brings more transparency to the threats that are out there and helps customers. And the world understand why leveraging security technology is so essential to the foundation of how they want to live their digital lives going forward.

[01:02:14] AH: And I know that we have to wrap up soon. So I just wondered if you could – If you had any thoughts to leave SpyCast listeners with. Is there anything that you would encourage them to do? It could be something they should read or something they should do. Other than downloading their updates, turning on two-factor identification and crossing their fingers. What else should they do? Or where should they go for more information?

[01:02:41] JL: Yeah. I mean, I would say like while these attacks can seem overwhelming, the reality is there are steps everybody can take to protect themselves. And some of the steps you mentioned there cut down on 99% percent of the attacks that you're going to see. And the simple act of turning on multi-factor authentication not just for your primary email, but for the other services that you use, the other accounts that are important to you, that is one of the most critical steps. And we see you know 99% of the kinds of you know password attacks just stop working against people that have gone and done those things. And even if you've done it, there's probably somebody you know that hasn't taken that step yet that probably needs your experience and help to know it didn't mess anything up and you can actually do it. Those kind of things are steps that everybody can take.

[01:03:32] CFG: Yeah, can I get an amen? Because cyber hygiene is not a topic that we hear about. It is so essential. It's the diet and exercise that we all have to do. It's so easy to talk about this advanced thing or this incredible exploit. But really what matters is the diet and exercise. It's the strong passwords. It's the patching. Get rid of all of that, and really make the attackers work for what they're going after. Make sure that you don't have mail-forwarding enabled in your personal accounts. Change your passwords. Go passwordless. All of that hygiene matters. It matters at the individual level. It matters at the enterprise level. And for the 43,000 people that we've had to talk to in the past three years to highlight that, it's a game changer.

So yeah, I know you're looking for things, ways to go learn information. We publish a lot of blogs and a lot of technical data about all the awesome things that our products and services can do. But get cyber healthy. That's really the most important thing to make sure that we don't have to call you.

[01:04:41] AH: Well, thanks ever so much for your time. It's been fantastic speaking to you both. And yeah, thanks ever so much for your time. I really appreciate it.

[01:04:51] CFG: Thanks a bunch Andre, that was fun.

[01:04:52] AH: Thank you. Thanks, John.

[01:04:53] JL: Yeah, thank you.

[END]