Sandra Joyce:

Thank you so much for having me, and I'm going to be talking about the global threat landscape. And a lot of people ask me, "Well, you make a lot of claims, Sandra, how do you know what you know?" And the way that we know is that we are responding to about 1,000 incident responses every year. We have about four security operations centers that are operating around the globe watching for campaigns that are arising in our customer base. We also have our partnerships with other companies and organizations that provide us telemetry. And then in my organization, we also are monitoring adversary infrastructure. We have a global collection apparatus managing thousands of personas in the underground and watching, listening, and understanding what threat actors are doing. So what I'd like to do is convey to you in 15 minutes what we're seeing around the world, what to think about, and then maybe some tips and things to think about for your organization.

I'd like to start with Russia. It's kind of an important place to start when you are thinking about what drives cyber activity around the world. Very clearly, Russia is driving the most destructive and disruptive operations that we're seeing right now. We're looking at all three of the major intelligence services really participating in the effort. And think of this like the FSB, the SVR, the GRU. We have seen them on the so-called cyber front lines. What they're doing there is causing more destruction and disruption in the cyber domain in the first four months of the war than in the past eight years combined of what we have seen. They're also doing this concurrently with kinetic operations. We saw 10 instances where Russia was deploying cyber activity and cyber attacks while they were running kinetic operations. On the battlefield, we've also learned quite a bit. What we saw is when Russian forces were advancing and taking over territories, we saw that they were also taking over networks, which means to us that they had embedded cyber action teams with their units as they were rolling through.

Another thing to think about is that all three of the INT intelligence services, we have now watched them utilize the criminal ecosystem to do things like grab credentials or conduct some of their operations. And we also saw some disruption in the criminal ecosystem where they were actually kind of splitting between ideological lines where some of them were pro-Russia, some were pro-Ukraine, and they were causing some disruption, which is always great to see in the criminal ecosystem.

So we are also seeing some pretty interesting collaboration with hacktivists. Now this is where it gets a little bit interesting. So the GRU, let's say that they would go and before they deploy wipers, are stealing data from Ukrainian systems, and then what we saw is the same data get dumped on Telegram channels in a hactivist group that we call Hack Man. Now that happened four times within 24 hours of the GRU doing this. So either there's some collaboration or some loose affiliation between the hactivist and the GRU or it's actually the GRU themselves. That we don't know at this point. But it's very interesting how they have that sort of very tight alignment that we've been watching.

So moving on to North Korea, this is a very innovative, scrappy cyber capability. They have basically no resources, but their cyber capability, really what us we say is they punch above their weight class in almost every way. During the pandemic, we saw North Korean actors really go after pandemic related things like research. They were trying to find out information about vaccines, et cetera, and that really took their focus away. But we're seeing them now return to their classic mission sets. Espionage particularly around nuclear capabilities. We're seeing them target in the United States dissidents and doing some really interesting things with crypto.

So we just recently graduated a group called APT-43. And when we say we graduated a group, it means that all the threat threat clusters, thousands of threat clusters of activity, were able to draw a line of high confidence and say, "This is the National Reconnaissance Bureau of North Korea." We call them APT-43. And by the way, we use numbers APG-43. We don't use names, Fuzzy Bear, Fuzzy Snuggle Duck.

Most of it is because we don't want to glorify, it's like prison numbers for us. Let's serialize them. Let's not glorify them.

So what APT-43 is doing is they're going to go and steal crypto from wallets and then they will use that crypto to rent hashing services. And so they're going to mine crypto using the stolen crypto. And now what they've got is a wallet that has no association with the blockchain from before. So think of it this way. You steal gold and then you go to a silver mine and you say, "Hey, would you mind some silver? I'll pay for it with this gold." And now you have fresh silver and everybody's still looking for gold. That's what they're doing. Very innovative. And they use that new crypto then to fund new C2 for their activities, new infrastructure for the things that they're working on. So again, really, really innovative and really, really scrappy.

Another thing they're doing to collect sort of that strategic intelligence is that they're spearfishing or simply sending emails pretending to be journalists. And we've seen this and we have a lot of examples of this to academics, other officials saying, "Hey, can you please comment on this?" And then they have a whole list of what I call collection requirements. And because academia's very open-minded and willing to share, they're getting answers to things like what will happen if the North Korea launches another nuclear or test a nuclear device? Or what's going to happen if, and they put all their questions, experts around the world are answering them and giving them that information.

I'd like to talk about China as well. So we've watched the Chinese, this is more of a case study to just sort of illustrate what we're seeing in the cyber domain. Now, in my position, I lead the intelligence organization at Mandiant. Now under Google Cloud, we've got great visibility and it would be really inappropriate for me to have a favorite threat actor. But if I did have a favorite threat actor, it would be APT-41. They're an incredibly bizarre group. So literally by day they're conducting reconnaissance and looking at carrying out strategic aims of this Chinese Communist Party. By night, they are cyber criminals making money with some of the same tools, targeting organizations like gaming systems and manufacturing and other things. So they're also incredibly innovative.

Now, the reason that I wanted to point out APT-41 is that about a year ago we saw them targeting and gain access to, or trying to gain access to 6 US states. And it was pretty easy. So they exploited a sequel injection and some directory traversal capabilities. They were easily contained. We kicked them out, kind of another day in the life at Mandiant. Two weeks later, they were back in the state government because they had exploited a zero day in an app called USA Hearst, which is an app that some states use to track diseases in cattle populations. So again, think of the attack surface that we're dealing with is very vast and very complicated and doesn't have anything to do with what you might think is an intrusion factor.

The other thing that is really interesting about China specifically is that the hackers that we're seeing, especially with APT-41, are very fast to exploit when something is public. So with responsible disclosure, if there's a vulnerability in software, what you'll typically do is make sure the vendor knows there's a patch and then you have an announcement. We all live through Log4j. That was dark times. Within hours of that going public APT-41 was already exploiting it. So for us, the lesson learned here is when you're doing your patch management program for those very critical patches, they need to go very fast. And prioritization of patches. Is it being exploited in the wild? Can you access it remotely? There's got to be a criteria because the ones that are critical need to go really fast.

So let's look at some high risk trends. So speaking of zero days, we're watching a trend definitely sort of overall lot more zero days being exploited. Now in 2021, we saw something like 88. That dropped to 55 in 2022. But if you zoom out, the curve is still going up. We think that in 2021 they just were able to take advantage of the pandemic and all that. But what we saw was, we attributed about 16 of these. China had the most of the ones we could attribute. And again, we can't attribute all of them. We do our best.

13 of them are cyber espionage related, 3 associated with commercial vendors, we had 2 from North Korea, a couple from Russia and China. But then four were associated with financially motivated actors. And most of those had to do with ransomware.

So ransomware, I actually for once, have good news about ransomware and I'm so excited to tell you about it. So what we saw was actually in raw numbers, what we saw was a decrease of about 15% year over year in ransomware incidents. That is fantastic. Now the bad news is that it's still very prevalent. It's the thing that we are responding to the most at Mandiant. So it's a golf clap, not a huge celebration.

But another thing that we're seeing is other sort of statistics also going down, and I'll tell you about those. So typically what'll happen is a threat actor who is deploying ransomware or trying to extort you will also dump data on a victim shaming site. They'll dump it if they want to just prove to you that they've got some data, they'll dump it if you don't pay the ransom. So there are a lot of reasons why they'll dump that. So we monitor a bunch of these dump sites and what we saw was a 7% decrease in victims that had their data spilled in these sites. Another bit of sort of good, goodish news.

The other piece of it is the proportion is changing. So we saw about a 10% decrease in the proportion of dump sites that were US based over to Europe. So good for us, not great for Europe. A lot of things probably contribute to this. There were changes in cyber insurance. There are changes in some law enforcement efforts that are gaining ground. People are hardening targets. But also some of the perpetrators of ransomware tend to be, most of them tend to be in Eastern Europe and Russia and they're kind of busy right now. So it's probably not one thing. It's probably many things, but good news all the same. And I never get to tell good news. So I'm pretty excited about it.

Another piece to think about with ransomware is it is a very resilient ecosystem. That's why it's a little difficult to get really excited about a 15% decrease because that could change pretty quickly. But I'd like to tell you a little bit about the types of things that we're doing and why we know what we know.

So during the colonial pipeline incident, if you recall that disrupted oil and gas distribution along the eastern seaboard a couple of years ago, that was done by a group called DarkSide Ransomware Gang. And Mandiant responded to that. That's publicly known. But what we did in the intelligence side is we got ourselves recruited by DarkSide Ransomware Gang. The way to do that, by the way, is to have somebody on your team in a different country who speaks perfect Russian, coming off of a different type of keyboard. And what we saw on the inside really helped us understand what this ecosystem is all about. Once you're recruited by a ransomware gang, you're given a control panel with easy to use access. You don't have to build any of the infrastructure yourself. There's a chat in case you're running into any problems, they will help you. Very nice, very helpful. And then the sliding pay scale is the more ransom you demand, the lower your fee.

So what happened with that was, so we learned quite a bit, and the interesting thing is, at one point, if you remember DarkSide Ransomware Gang went public. They said, "We didn't know it was an oil and gas situation." They even donated to charity because they're standup guys, and then just at one point there were so much pressure for them to shut down, it started to cause a lot of disruption in the criminal ecosystem. So we're watching, I told you we're managing all these personas in the underground and they are getting on each other's case. Don't mention ransomware, there's too much pressure right now. Those guys start getting mad because these guys are recruiting their affiliates, these ransomware operators, they start de-dossing each other. It's wonderful. So basically they decide they're going to go dark and they just said, "We're done. You caught us, we're done." And they disappear. Two weeks later, they're back up under another name. A resilient ecosystem in ransomware where people, they don't know each other and they've never met and they have a lot of redundancy.

So basically some considerations. Use threat intelligence to really guide your prioritization, think about that patch management piece, practice what you're doing, have a tabletop exercise about ransomware. Don't let that be the first time that you think about who is going to be essential to the process on the worst day of your career. Make sure you have that all sorted out beforehand. The people that we have worked with who are best prepared are the ones who have done a few rounds in practice. Make sure that the people that are there are people like general counsel. Make sure you have your comms person there. Sometimes people forget a lot of these threat actors are getting very aggressive. They're going to go public, she's good. Don't worry. They're going to go public with your incident. And sometimes they're going to get very aggressive. We've had people actually threaten the siblings or the spouses of the people who are working on the IR. They're going to threaten to do all kinds of crazy things.

So make sure that you test that, you practice that, and then build your ecosystem of people that you work with. Make sure that you've got external to your organization, that you have the right relationships with government, non-government, you have an IR retainer in place with a really substantial SLA that'll get you what you need right away. So with that, thank you so much for your time and have a wonderful rest of your conference.