Jim Coyle:

I appreciate you all being here. Got a couple of things I want to talk about today. So I heard some of the earlier panels was talking about my beloved subject of TikTok. Couple of things I want to talk about. So first, there's really kind of two issues that I'm starting to see. The first is a data sovereignty issue, the second being algorithms. I'll get back to that. So first, let's talk about some of the data that TikTok is collecting. Now we're talking about IP addresses, we're talking about device IDs, various items to be able to pinpoint individuals to devices. Mostly used for advertising, geolocation information based on SIM card data, and there's a few other things such as keystroke rhythms, and that just from a cyber perspective, my skin crawl for a little bit.

Now, TikTok is not alone in collecting this data, right? We've got other social media platforms that are also collecting the data. I'll get back to that. But more importantly, because of everything that's going on, we saw Project Texas started to get involved, right? Where TikTok's parent company, ByteDance, wanted to move data centers into the US. So any data that was coming out of US would be stored in the US. Now there's been news stories that have been coming out about a employee that was in charge of Project Texas that met with a executive of ByteDance who was asking very pointed questions specifically about operating system information, where Project Texas was going to be physically located, as well as hardware platforms that Project Texas was going to be utilizing. For anyone in the IC community, you may start to recognize some of this as Tradecraft.

Now, there was another news story that broke just about two weeks ago on BBC, that a reporter was getting geolocation tags and the information getting basically put up against ByteDance employees, specifically TikTok. And they were trying to track employees talking to the press. Now, what really perked my interest on the story was the fact that she doesn't have an account. The reporter does not have an account, but her cat does. Again, if you're in the IC community, you may notice this as trade craft because somebody had to do the legwork to understand that a cat was being tied to a reporter, right? And then further go in to understand the information that I have a ByteDance employee that's meeting with a reporter that's tied to a cat. Now two US individuals as well as two China individuals were involved with geotagging that information and doing the resource collection.

Now, when we talk about China, there's roughly about 25 or so roughly threat actors that the industry tracks as a whole. And a lot of these various different threat actors have different reasons for being there. Some of that is industrial espionage, some of it is military targeting, some of it is economic dominance in specific regions, especially when we talk about Belt and Road initiatives. But there is a lot that China does overall. One of the things that they've most recently just got caught red-handed for was meddling in the elections within Canada. So they have been getting involved with the election meddling for the last, I'd say, probably about five to 10 years, and they're getting better. So remember when I said that there were two problems, one being data sovereignty? The second is the algorithms. Now, I'm not saying that this is happening today. I'm saying that the vulnerability exists, that we know that China is meddling with elections and there is a possibility of TikTok having its algorithms altered to sway public suggestions one way or the other.

But as I said, it's not just TikTok. And I do want to be very clear about one thing. This is not malware we're talking about, right? This is just pure data that's being accessed. Now, what I've got up here on the screen here, we've got some other companies, which we've probably heard about over the last 10 years that have had their business practices pulled into question by the government for various reasons, all of them tied to possible nation state activity. Now, TikTok, as I was mentioning earlier, it's a very popular social platform, right? Now, the business model is to make money off of advertising. So there's a lot of data collection that's happening much like Facebook, right? Much like other platforms that are out there. And if you remember Cambridge Analytica, we got to see what happens when the data ends up in

the wrong hands. Now, one other thing I want to bring up is a company called Temu. I'm not a sports person. If you're watching the Super Bowl, you may have seen an ad for Temu as a shopping app.

It's basically China's version of our Amazon, if you will. The parent company who owns that is a company called PDD Holdings. I'll get back to that. So there's another app that PDD Holdings owns, which is called Pinduoduo. Again, it's a shopping app. Now, what's kind of interesting is both of these apps are highly popular. If you go into the app store, if you go into Google Play Store, it's a top app that's being downloaded, that's for free. Now, what makes really interesting here is there was a Chinese researcher who goes by the pseudonym of Dark Navy who put a blog post that said basically PDD is... Specifically Pinduoduo has some exploits that are looking at Android devices. And so we had to do our due diligence. We took a look at it and we found, sure enough, there have been Trojan-eyed versions of this app that are out there.

But again, what makes this really interesting is that the developer signing key, which is used to sign the app that says, "Yes, this is my development," was utilized in the malicious malware versions. There's kind of three answers to this, on why that's happening. One, key was leaked; two, there may have been a supply chain compromise; or three, this was deliberate. Now what, again, makes this further interesting is CNN had put out a report where they confirmed that there were a 100 developers specifically looking into this exploitation capability. Today, 20 of them remain at Pinduoduo, 80 of them have been moved to Temu. But we've got some other apps to talk about. So when we take a look at mobile APTs, and in particular what we're talking about is, I'm going to do this in air quotes here, "Lawful interception."

We see a lot of this in Iran, Pakistan, North Korea, Lebanon, there's a bunch of other countries on this list here. But what makes this the most interesting is there is a abnormally high amount of malicious apps that are coming out of China. So what I want to talk about is Moonshine, and this is state sponsored malware that was targeting Chrome browsers specifically, and we happen to dive into this code pretty deeply, what really kind of sparked interest here is all the apps that you see on the screen, they all had the similar code of this malicious capability of this exploit looking at Chrome browsers. Now, when we take a look at Moonshine itself, just as the malware, it's your standard kind of surveillanceware. It does a lot of things. Mainly it pulls as much data as possible, right? So we're talking about whether it's calls, whether it's SMS messaging, whether it's contacts, what's going on with the camera... Typical what I would call surveillanceware.

So what's really interesting, from a researcher perspective, is that it also has a SOCKS proxy capability. For the non-technical folks what this means is this allows a adversary to utilize the app as a back door to gain access into protected networks. So if a device connects to a Wi-Fi, I now have access to that network because of the app, because I can now ride the connection through the app and land onto the network. What that means is lateral movement onto those various networks. So we're seeing a lot of mobile as being a first initial vector. So there's a lot of... I'm sure you all have received some sort of SMS messaging with a link on your phone that says, "Hey, we tried to attempt a package delivery. Click here to reconfirm." Maybe it's, "Hey, your Netflix account has been disabled. Click here to re-enable it." Right?

I mean, obviously a lot of these we can talk about or we can see. But what really gets interesting is when you start getting very highly targeted phishing messages, right? You start to blur the lines between, well, it could be, right? And unlike a computer, you can't just hover your mouse over the link to see if it's going somewhere that that's suspicious. All you're left with is hitting your thumb on a link that may or may not be malicious. So again, when we talk about China, what's really interesting is they tend to practice their tooling and creating workflows, making sure that their tools are working on their minority ethnic groups. And so when we start to see things like dissidents, pro-Taiwan, Tibetan or Uyghurs, this is

typically their running ground. So I'm pretty sure at this point everyone's wondering, "Hey, that's great. This is all happening in China. Why should I care?"

Well, what's really interesting is depending on who you read your research reports, the majority of the IR firms today are starting to put out more and more releases about mobile as being that first vector. And so keeping with China as being the adversary in this particular talk here, one of the things I do want to talk about is that APT10 has been highly active, specifically in Japan currently, but that is right now the MO, is going after Japan, utilizing mobile as that first initial vector. APT40 has been highly active within the US, going after intellectual property and trade secrets. And so really just to try to wrap it up here, as I see the clock here, we've got some other ones that we can't currently talk about. I had to remove the last threat actor. We're just not ready to talk about it yet. But needless to say, there's quite a few that are out there. In fact, we have tied APT41, which if you were here earlier, you heard Sandra Joyce talking about if she had a favorite threat actor, that might be one of hers.

We have been able to attribute them to bad spy. And so a lot of the threat actors that you're hearing about now are moving into that mobile first category. So this is how I'm going to end it. Right now... Again, this is just talking about China. We've got over nine million apps that we've identified that have some sort of C2 or communication back to Chinese owned addresses. Now we have roughly 210 million devices that we're able to analyze. We've got just as many apps that we've done reverse engineering on to pull out of this data. So when we start looking at from a global presence perspective, you can start to imagine when we start looking at our top adversaries such as Russia, right? What's going on there. North Korea, Iran. We're starting to accumulate a lot more again, of that mobile first initial contact as a way to get in or breach larger environments.

So the bigger question that I have for you today is, are you currently ready, from a mobile perspective, to be able to answer the call to when you have a breach that mobile may or may not have actually been that first initial vector? As we start to see that increase, I'm out here trying to raise the awareness of this is something that needs to be seriously thought about in your planning moving forward. This isn't something that you want to wait for a last minute from a decision perspective. But with that, I think I'm left with about one minute. So if there's any questions, feel free to grab me. You can reach out to me. But definitely appreciate your all's time today.