Eye on Security

The “Big Four”: Spotlight on China

Transcript

Luke McNamara:

Ladies and gentlemen, welcome back to another episode of the Eye on Security podcast. I'm your host Luke McNamara. Today for the third in our series on at the big four, we are tackling China. And joining me today to help me do that, I have Lloyd Brown, principal analyst on custom intel team here at Mandiant. And Scott Henderson, a principal analyst on our cyber espionage team. Lloyd, Scott, great to have you here today.

Scott Henderson:

Thank you, Luke, it's good joining you guys.

Luke McNamara:

I didn't realize when we were sitting down to plan and discuss this episode that this was coming up on almost the anniversary of the APT1 reports, which was released about eight years ago. So this is great timing, however accidental. It'll be a little bit later when this is released and is live. But certainly and one of the other reasons of why this was the episode I kind of wanted to do a little bit later, after we had tackled North Korea and Iran is because there's so much to discuss here. There's so much history, cyber espionage campaigns and activity, we'll primarily be focused on the cyber espionage side today, but I think we'll get into some of the discussion that dovetails into what we've seen more recently around information operations, and other types of activity.

But I think where we can maybe start this conversation is the similar framing that we use in our analysis that I've seen in reports in the last couple of years. And looking at and framing the activity as sort of 2015 and earlier, and then what we've seen since 2016. So maybe to start us off, Scott, help us think about and characterize what are some of the characteristics when you think about that pre-2015 activity? And there's a lot of it that goes back to kind of the early 2000s before, but what was that period characterized about?

Scott Henderson:

Sure. It's kind of funny that you should talk about APT1, I was actually doing some research today. And I was looking for the first incident we had of Chinese cyber espionage. And it was in

2003, which was, of course, the 2003 2004 timeframe, which was APT1. And it's actually kind of funny because I have been looking at how we categorize or look at the evolution of Chinese cyber espionage. And for myself, I've kind of broken it down into four different stages. And to give you an idea of how we've done that, it's based off of our observations, primarily, our observations being FireEye, what we've observed as actual incidents of Chinese espionage. Some official Chinese documents about how they're saying that their intelligence structure and their cyber espionage operations, military operations, have evolved, and also independent outside analysts, government organizations, and things like that. But primarily, it has been off of our observations.

The first period, and I'm sure both of you guys will remember this, is sort of that nascent period. And that's what I was getting back to you, the APT1, that first like, 2003, through probably, what, 2013. It was the Wild Wild West. You guys remember that, right? I mean, the Chinese were everywhere, they were omnipresent, they were loud, they were noisy, operating globally. And they didn't seem to care at all about attribution. I mean, they would sign their infrastructure with their Chinese hacker aliases. And I think I remember this distinctly too, what was it, the CVE-2012-0158.

Luke McNamara:

I was going to bring that up.

Scott Henderson:

Right? Yeah. Because if you saw a lure with 0158, it was Chinese. I mean, that was just... I mean, obviously not, but it was kind of Chinese operations. Then I think, and this is where I kind of want to pat our company on the back a little bit, was the Red Line Drawn, we're a cybersecurity company that looks at cyber espionage. And we had, I think, the courage, to say, "We're seeing one of the top adversaries decreasing operations." And we were on the cutting edge of that, I think we were one of the first companies, if not the first, to come out and say, "Chinese cyber espionage operations are dying down." And I think in hindsight, when we look back at that time period, which was probably, what, the 2013 through, let's say, 2016 timeframe? There's some definite reasons that was happening, and Lloyd probably even knows a little bit more about this, and maybe you do as well, Luke.

What was happening during that time period? And number one, I think, and this is probably one of the catalysts, a big catalyst obviously, was that Xi Jinping took power in 2013. And he took over from Hu Jintao, right? And I don't know what you think about this, Lloyd, but I think that Hu Jintao was more of a financial health of China guy, he was that sort of nondescript bureaucrat who... he was a good place keeper, he was a good maintainer of the organization. And he'd guide them through the big financial crisis, and he was also there, I mean, we'd had some dissident activity with Tibetans, and as China views that. And then I think when Xi Jinping takes place, to me in my mind, he's an old school strategic thinker. And so when we see him-

Lloyd Brown:

Yes.

Scott Henderson:

Right? So when we see him coming into power in 2012, he goes through that old school, sort of the Chinese way of you consolidate your power, start getting rid of your adversaries, and they had the anti-corruption campaigns, which expectedly happened to people who are your rivals. So he gets his rivals out, and he's reorganizing the military, so that he is taking over that. And then one of the things I think a lot of people think about during that time period was the Obama-Xi agreement. And yeah, give it all the credit in the world, but it was also kind of fortuitous timing for Xi Jinping, because that was also the time period when they restructured the intelligence apparatus.

Luke McNamara:

And that time period is sort of late 2015, I believe, right? When Obama-Xi agreement took place?

Scott Henderson:

Yeah, absolutely. I think it was September-ish timeframe, somewhere around there. I think that was the Obama-Xi agreement. And we had actually called the Red Line... And the reason we call this period the Red Line Drawn is just because of the report we put out on it, just to give... People might not be aware that, I was very proud of that report that the company did. And so we'd actually seen that decline at least a year prior to the Xi-Obama agreement. So I think what happened, it was kind of fortuitous timing for Xi Jinping, he's like, "Yes, I want to reform the military, I want to get these organizations into place." And that was when we saw the strategic support forces coming into play. And that was under the network systems department, which kind of subsumed, I think, 3PLA.

So there were a lot of, I would say, outside factors besides the Obama-Xi agreement that contributed to that rapid decline we saw in Chinese cyber espionage activity. And this is one I think I may have invented. You guys could correct me if you think I'm wrong here. But I call it the post reform intelligence restructuring, and I'm really proud of that basic term that says nothing. Yeah. And essentially what it means, I think you guys have probably gone through reorg, restructures... When I was in the military, we would do that, and they would come out with the block line chart, and everything was supposed to be good. However, you know that there is a period of time, and it looks like from some of the research I've done, it took place between 2016 and 2018. And that's sort of that stabilization period where the reforms have taken place, all the mandates have gone out, however, things still aren't operating quite exactly how you have them down on paper.

So I look at this is as that transitional period where we know what's happened, we know what the transition looks like, however, it's still not functioning exactly as it is on paper. And I think now, we've actually probably entered into the current structure. And that's where we've seen everything is in place, we think that the cyber espionage teams are acting in accordance with that restructuring. I kind of want to tease this out, because I'm really proud of the report that we've got coming out, essentially, and this is sort of that bottom line up front, and we did a survey report, it was a four year period, that is saying that China's cyber espionage operations pretty much... the realignment mirrors the five new military theaters that they came out with in 2016. And hopefully, that report right now is in coordination, should be published next week. So a little teaser on that, but kind of looking forward to that coming out.

Luke McNamara:

So we definitely want to get into some of the characteristics and TTP shifts, changes in the threat actors active that we see connected with China since 2016. But I want to explore just a little bit more of that sort of earlier period of Chinese espionage. Just got to remember back when we were working at iSIGHT Partners in those days in 2013, 2014, a lot of what we're looking at from a cyber espionage perspective, overwhelmingly, was Chinese CE activity. You think about some of the notable operations, Operation Aurora, Titan Rain, I think that was back in 2003, the OPM breach in 2015. So many there's been several big, significant campaigns and events that we've seen from Chinese threat actors. But I think the big story in that period is just how prolific so many of these groups are that never made the headlines. Lloyd, what's your take on that period of Chinese espionage?

Lloyd Brown:

As we were just talking about earlier, there are so many groups that we have that aren't formally rolled into APT groups that we've seen active, which we still call UNCs, uncategorized groups, and there was so much activity at that time, going on on different fronts, with different groups targeting all around the world, really. A lot of targeting in the US, a lot in Europe, but even a lot more in Asia itself. And so you can see the amount of resources that they put in to targeting, including using a lot of custom malware, a lot of CVEs and you could see that gradual shift Scott was talking about with the realignment, where we started to see them become more resource focused, you see them you using more shared builders, using more publicly available malware, a lot less custom malware, and the consolidation and the focus allows them to be even more effective now than they were then.

You could see back in that time period that certain groups had certain mandates in terms of their targeting. But then now we're seeing a lot more emerging of groups with overlaps between three or four or five different groups that we've tracked. And we're starting to see them use a lot of the same things and a lot of the same tools and become more focused. And just from government understanding and working in the government for so many years, you know that, as you were talking about earlier, Scott, that when they do these restructures, it

does take time, it takes time to get everybody on board with the plan, it takes time in order to bring the groups together and explain how the shifts are going to occur. You've got to get through cross-cultural barriers. There's the use of civilian espionage organizations, there's military, there's use of contractors, all of that needs to be realigned. And so that two year period that you were talking about from 2016 to 2018, that's roughly a good time period of how long it would take in order to get things aligned, and everybody gets used to the new structure.

Luke McNamara:

Two things that each of you said that I want to point to, Scott, I think he made a really good point in the Red Line Drawn paper, that one of the things I think sometimes it's misread about that change and shift in Chinese espionage activity is that a lot of it came from the Obama-Xi agreement. But you're right, we saw that sort of drop off in activity preceding that, as much as that agreement itself was a sort of maybe more formal acceleration of a trend that was already happening. And Lloyd, I think something you said, too, is another piece that's often been missed, which is, in that transitionary period, there was still a lot of activity, and especially I think were some of the more emerging threats started to come back that happened within the region. So I think having just a US-centric focus on what do we see over that period over those years, sort of misses what was happening over there.

Something else that I think both of you touched on that I'm curious in hearing more about is, you've kind of touched on the fact that this was also an organizational shift. So a lot of the activity that we saw pre 2015, very much linked to PLA units, PLA support, we start to see that shift and change. From what we know, in terms of how those capabilities and those resources have been restructured, what is our sense of what that looks like now?

Scott Henderson:

I really think, and this is kind of interesting, I really do think what we see now is, on the PLA side, is an alignment with the five new military theaters. Just to give you a little bit of history on that. China has operated off the mil regions forever. I mean, I forget when they first started, how many different mil regions they had, but gradually, most people in the area were a member the seven military regions. And so what we saw during this restructuring, realignment is the forces were structured down into five different military theaters. Backing up even a little bit further, I think when people say China, they think of this homogenous country, that it's plug and play, you can go from the east coast to the west coast, and everything would be exactly the same. And that couldn't be farther from the truth. North to south, there's different languages, there's different dialects, there's a different culture. And same if you go east to west.

So what we saw with the restructure with the military regions is sometimes the military commanders, they start garnering a lot of power in their particular region. I mean, they act kind of like politicians, they act like regional governors. I mean, they have a lot of power in these regions. So what Xi Jinping did is he mixed them back up. So if you were in this military region,

you're now in this military theater. So it kind of dispersed their power, took it a little bit away, they're more reliant on his good graces than they are their regional power.

And to kind of give you maybe an idea of these military theaters versus military regions, I think a good example we might want to talk about is Tonto. Tonto is one of the first teams that I was able to say, "This is PLA." Because sometimes that attributions, "Is is PLA, is it MSS? What is it?" It's a tough thing to do the attribution on that. Tonto PLA, upfront. And one of the reasons we kind of knew this is, I think it was... I forget exactly the years. Early 2011, 2010, something like that. One of their passwords was a MUCD, which is a military unit cover designator. It's a five digit group that all the military units use, so that we're not Shenyang Military Region, cyber espionage operations, or MUCD650, whatever.

And with them, one of the ways we could track them with through their malware, and what we saw was they were operating out of the Shenyang Military Region, they were targeting Japan, they were targeting Russia, and they're targeting South Korea. I mean, geographically from the Shenyang Military Region, which is up north, these are the exact countries you expect them to target being regionally targeted, and it played out perfectly for a long time. Then what we've seen with the shift to the military theaters is now some of the Northern actors that we typically see, I think you guys are well aware of those, we see Tonto, Roaming Tiger, APT21, which we used to call Junbao team. We see them all active in the northern theater, but the northern theater is expanded. And it looks like the northern theater now... It actually looks like Japan may have dropped off down into the eastern theater, while the northern theaters expanded from South Korea across Russia, Belorussia, out toward Europe.

So it looks like it may have expanded the geographical region. And obviously, one of the other things we did when we were researching Tonto Team was we looked at language training, and we were able to backtrack them through their MUCDs, and say, "Okay, they do have Russian language training, they do have Korean language training, and they do have Japanese language training. So we think that that's how your resources are allocated." So we think that that Russian language training, obviously folks as well for extending the northern theater out. So I think that might give a little bit of a structure of how we see them realigning. The same with the southern theater, eastern theater. One of the theaters that we're probably a little less... it's a little bit more ambiguous is the western theater, we're not sure exactly how far the western theater goes out.

Now clearly, the western theater, sort of militarily is a deterrent to India. But cyber espionage operations, it seems like it may stand out toward Turkey, there seem to be some skipped zones. And obviously, it kind of goes along with Belt and Road construction, but they do seem to be aligning up that way. It's kind of like a neat math formula. So when you take away all the CE groups that conform to this sort of military theater, regional alignment, and act outside those norms is MSS. And they act globally, they target western groups, they seem to be hitting North America, Europe. Also, it seems like they do internal dissident stuff, that'll be like Hong Kong, and maybe out in the west, we're not clear on that. But like Tibet, and the Uighurs things like that. So it seems to be aligning structurally, almost exactly how you totally think it would.

Lloyd Brown:

Think one of the things that helps with how we track the espionage campaigns that we see is, which you brought up with tracking the languages and just the volumes of data. When you understand political and military and espionage goals, then you're able to branch out from that, and gather data that helps us align this with the cyber hacking that we observe from China. And it would be the equivalent of the same way where they would strategically see a reason to target something like OPM in the United States, that has a large volume of personally identifiable information, where they could use that to correlate with other sources. And just like we, as an intel analyst, and intel company, bring the multiple sources together in order to figure out and understand what may happen next, or what these Chinese groups may be targeting next, so that we could share that information with our customers and our stakeholders, we do have to understand the different layers of what MSS's mandate would be, what the PLA's mandate would be, and what these theaters focus on.

And it also helps that when we conduct investigations globally, with Mandiant Consulting arm of FireEye, where we're able to help explain these, the purpose of the activity when we are able to attribute it to some of these Chinese groups and the history behind it to executives, so they understand that they may be in a company or in an industry that's going to be strategically important for Chinese groups. And that if this hacking has occurred, then the attackers are likely going to come back, and there will always be a focus. And there are certain industries that are always that way. For example, telecommunications, there is no hacking group in the world that wouldn't want a good tap on telecommunications. COVID targeting and healthcare related vaccine information now has become important.

And so the same way that we saw those shifts happen back in 2015, or 2016, if things happen globally in the world, then the government has to shift its priorities. Same with the, and we'll touch on this a little bit later, with looking at election campaigns and conducting misinformation, information operations with that. Or the shift in alignment that needed to occur when the Hong Kong protests started, and trying to understand what was going on there. And now with the Uighur targeting, the way that the different groups and how they target specific regions, all of those can be realigned depending on the needs of Xi Jinping and his government and this is what the overall realignment allowed for more swift, easy maneuvering and focusing resources. You could go into a room and have everybody who's in charge and just point them in the right direction, "Now, this is a priority one for us. Can you please go after information related to that?"

Luke McNamara:

One of the things I know, again, from reading a lot of your work and the work of other analysts here, they've been looking at the sort of shifts in activity from Chinese espionage groups since 2016, has been the increasing focus on tactics and techniques that are much stealthier than what we saw in the past. So as Scott kind of alluded to earlier, the stereotype I think that for a long time you had of Chinese espionage groups was that they were just incredibly clumsy and

noisy, smash and grab. And I think if any of these different nations Russia, China, North Korea, Iran, you have a range of different capabilities, certainly groups that are more, you could say, advanced in some aspects of their operations and the development of their malware, you have groups that put a higher premium on stealth and secrecy and counter attribution efforts. And I think that the same is probably true of China, you have way more groups to even factor in there.

But what's something that you think characterizes... We think about how there seems to be a higher premium placed on some of these stealthier techniques, what are we actually seeing that differs that activity versus what we saw pre 2015, that era?

Scott Henderson:

Yeah, I think in my mind, and it really is an evolutionary process, as you point out that sort of Wild Wild West period, where like you said, there wasn't any problem finding Chinese espionage activity, it was sorting through it to find out what's the highest value, because there were just so much of it, as we had talked about too, between infrastructure then and infrastructure. Now, when you would go back to look at who had registered a domain or website or something like that, you would typically find that they would put down this city in China, they would sometimes use a alias. I mean, it was fairly easy, "Yep, there is your attribution right there." Now we don't see that, obviously. They'll use fictitious western names or it'll be protected anonymous protection type activity.

And I think with malware, we're seeing them go to a lot of open source stuff like Beacon and things like that. So it kind of blends into the background activity. I think obfuscation has become very important to them of who's doing it. And this is funny, I think you might remember this as well, Luke, John Hultquist, he used to be very adamant about Tibet, saying that we needed to look at Tibet, I was just on-boarded to the company, and finally, one day I got the [inaudible 00:22:23], I was like, "Why are we looking at Tibet?" He said, "Well, here's the reason. It's a perfect petri dish. Who is going to target Tibetans? It's going to be the Chinese. Yes, there may be somebody else, but 9 times out of 10, it's going to be Chinese. And that way we get the first look at the malware coming out. We can attribute the malware. We can attribute the infrastructure." So I think back then that was something we could use as a sort of a bellwether of if we see this malware outside of Tibet, well, it's Chinese.

Luke McNamara:

It was a useful differentiator, you're looking at like a campaign that hits, as Lloyd was saying, a telecom, who wants to hit telecom? Everyone does. Targeting of G20, everyone's going after the G20. But then they also see targeting of Tibetan activists, that's a little bit different.

Scott Henderson:

Yeah, Hong Kong activists. You say, "Oh, this seems to at least lend some weight toward it

being Chinese motivated, because they clearly have a vested interest in this area." But for the obfuscation thing, they really are upping their game, their sophistication level, I think from the early 2003 to 2013, it's elevated way beyond what you would think in that amount of time. Because I mean, you're looking at a decade of Wild Wild West activity, essentially. And so from 2013, to current, they really have, I think, gone to obfuscating targets so it doesn't look like we're directly targeting this, we're going to telecoms, we're going to more open source malware, we're not making it really easy for security people to look at infrastructure and see this is Chinese related. So I think those are some of the key ones that bang around in my head when I think about it.

Lloyd Brown:

I'm just touching on the point that you mentioned with the petri dish. In the Asia Pacific region, some companies are more developed and focused on cybersecurity than others. And I think a lot of times when people look at Chinese espionage, and they look at the maturity of the targets that they're going after, the regions in the west, and the regions in Europe have a heavier focus on it than the regions traditionally have in Asia Pacific. It's growing at a very rapid rate, but it's not necessarily exactly at the same level overall, as it is in the west. And so what you get is the Chinese focus on things in the region, because they want to make sure they know what their neighbors are doing. And then you get less strenuous cybersecurity practices, also in the region, and so it becomes a place where they can practice and see what works while they're targeting their neighbors and getting all that strategic information politically with military information. And then they are able to use what they've learned there and exploit it elsewhere.

And in terms of sophistication levels, I think just as a company, we used to be heavily focused on zero-day activities, I think the whole industry was. And now we're at the speed that CVEs can be exploited. If somebody tweets about it, they've grabbed it and used it by the next week. And by the time that we were able to get in front of these executives, or we've been called in to conduct an investigation or manage defenses alerting on it, and we get in front of them, and we explain that this new CVE came out, you need to patch your systems, it's almost too late, because they've grabbed it, and they weaponized it, and they've used it so quickly.

So when we track the campaigns of the groups that we're looking at now, as soon as some sort of CVE comes out, they're immediately all over it and using it. And then we also see them prior to the incidents, the recent incidents, of doing supply-chain targeting, and third-party compromised. And that has been a staple of theirs for a few years, the CCleaner compromise is a good example of one, where you saw two stages of it, we saw them target multiple organizations globally, and so they affected many organizations, and then you could see them focus down strategically on the 10 or 20 organizations that they cared about.

And now that this is becoming even more prevalent, and China would be looking at operations, like the success of solar winds that occurred, then there may be more of a shift and a focus into this as well as the speed of CVEs and looking at different third-party applications that most

organizations may not traditionally think about. We've even observed them, keeping an eye on companies inside of China, and outside of China with their tax haven, and text casts or malware where there is malicious software that was associated, or at least the software for an update for a Chinese tech's program needed by programs that are operating inside China or with Chinese companies, could be used maliciously. And I think some third-party reporting from other vendors did claim to observe this being used maliciously. And that's another example of sliding in malware in an update. So I think this trend is also going to continue with Chinese groups.

Luke McNamara:

Well, this is one thing in particular that I wanted to get your perspective on. Because I've seen the reporting around... We're seeing more of these groups come back APT10, APT31, other groups, we're seeing indications that at least malware developers are reiterating on older pieces of malware, maybe in support of a new group, maybe we're seeing that malware being used in regions that we haven't seen before, again, probably indicative of some of those shifts and reorganization of assets and resources.

But I guess the question I have is, if we know we're seeing more of these sort of information, supply-chain targeting, we know we're seeing these examples where there's targeting of things like telecoms, historically, we've seen targeting of entities like law firms that have access to a wide range of organizations data. If we're trying to understand the extent to which the volume of activity is returning to somewhat maybe close up we saw in that pre 2015 era, what should be things that we should be looking for? If maybe just counting individual breaches isn't necessarily the right way to judge how prolific and active these groups are? Because they are going after targets that potentially allow them access into a wider array of targets than going and popping those organizations individually.

Lloyd Brown:

I think organizations need to understand that they may have a larger strategic purpose for China than they believe that they do. So professional services companies and examples like the Cloud Hopper, APT10 campaign, organizations that have a plug into multiple organizations. I use an example of a techs company in the US, or a techs company in Korea, organizations that provide services to multiple different business partners, government and private entities would all be a potential target for any Chinese group that wants to keep a pulse on their customer list.

And so if you're an organization that services multiple governments, or provides even something as simple as like an HR payroll to multiple organizations, you're potentially a target. And so having companies understand the strategic threats in their tech service, and what strategic value they may hold for China is important to understand. And I don't know if we necessarily looked at it before, or if companies necessarily looked at it in the past.

Scott Henderson:

Yeah, and I think you bring up a good point when we see these groups coming off of hiatus, I think as you pointed out, you had APT20, actually, Tonto Team came back, a lot of these groups started reappearing, like what, around the 2018 timeframe? There's TEMP.2cam, we saw Icefog activity, which is still kind of a little bit-

Lloyd Brown:

Yeah, still going.

Scott Henderson:

Yeah. Fuzzy too, in my mind because you saw that sort of transition from the original Icefog report that came out, to the new stuff that's going on. And like with TEMP.tick TEMP.tick was more of a separate group from Tonto Team. But now we've actually seen some pretty significant overlap between those. So maybe they've merged in with this larger northern region, 33A team, that was a really old team, we used to see all the time, they were hitting all the western organizations, 2017, we saw them kind of pop back up. Conference Crew, they've been down for a little bit now, 2017, we saw them pop back up and they're hammering Hong Kong. So we've seen some of that.

And I don't know if we'll return necessarily to the volume of activity we saw, or I don't know if we'll see the volume of activity that we saw. I think you're looking at an adversary that's much more stealthy, that does hit a lot of third-party software that does have different angles, they hit peripherals, companies working for companies that they want to target, like you said, with the law firms. Was it the law firm? Or was it the clients of the law firm? So it clearly is probably clientele that has a lot to do with this. So I don't know if we'll be able to say this is the same volume we've seen, but I think probably more strategically focused, might be a way I would view the future trend of it.

Luke McNamara:

It's part of the game that you know you're always missing a significant chunk of the iceberg, but you're never quite sure how big that is, how significant that is.

Scott Henderson:

Yeah, absolutely.

Luke McNamara:

One aspect that I also want to get into a little bit is, we've touched on the reorganization, the sort of refocus regionally of some of these groups. We've talked on what that has looked like in terms of the shift and TTPs. I want to get into some of these larger drivers, though, I think,

Lloyd you mentioned Belt and Road. And I know, Scott, you've written a lot about this as well, not to give our company another pat on the back, but this is our company podcast, so I will.

Scott Henderson:

Yes.

Luke McNamara:

I think we were one of the first ones to note and highlight how, as you were starting to see some of these groups come back and the Belt and Road initiative, as it got rebranded from One Belt One Road, was going to be a significant driver of espionage. I think that just made sense historically, when you looked at how they've used that capability in support of their economic interests. So I'm curious, as global as that initiative has gotten, and I think depending on who you talk to, you'll hear varying degrees of how successful from the Chinese perspective it's going, there's a lot that's kind of wrapped up in there. But where does that stand right now, in terms of is that a useful framework for understanding some of these campaigns and activity, particularly as you get further outside China's near abroad? I believe that's the correct term. To get onto these larger and other areas, just trying to get into Europe, for example, or Central Asia. How is that shaping and driving activity?

Scott Henderson:

I would say it is a huge driver, if not probably one of the number one drivers. Belt and Road is Xi Jinping's signature project. I mean, I think it's got his name stamped on, its success or failure reflects on him. And I think we have to look at China historically, as well with this. China right now, it has a strategic focus west. When we looked in the history in the past, China had several different strategic directions. You have to understand it in the form of their power projection as well. In the earlier days, we saw that they kind of had a western folk... they were worried about the west. So everything was focused to the east, all their military bases, everything was geared toward preventing the west from coming in and doing horrible things.

And then we saw, they kind of had a fall out with their neighbor to the north, with the Russians. It focused northward. And this is all on that premise of a week in China, kind of the week man of Asia sort of mentality when they felt like they had that, had to be more defensive in nature rather than a, I don't want to call it expansionist, but expansionist, so it's more of defensive, it's hunker down until we start to gain power. And I think, as we've seen them progress economically, they've said, "Okay, it's time to move out." And the west is clearly their direction toward Europe. It makes a lot of strategic sense. So when you start creating this Belt and Road, it's not just financially, does it make sense? It's strategically makes sense.

For the longest time, the Malacca Strait, that was where China was going to be cut off, the string of pearls theory and all that came into place. But with the Belt and Road, goods and services provided by the Chinese can move into Europe. And I think that's what we're seeing is

they're moving out there. So each area that touches on either if it's elections, so in Malaysia, there's an election going on that could possibly impact the Belt and Road, somebody who's positive about it, or somebody who's negative on Belt and Road, they're going to monitor that. I mean, it's very important to their signature project, to Xi Jinping's signature project. And the farther you get out, it's not just the Belt and Road, it's also sort of the cyber piece of that as well.

So if Huawei is... they want to move 5G into that, well, they're going to monitor that as well, if we start to see some negative press coming out of that. So essentially their line of communication is getting stretched out all the way from China into Europe. So I think it's huge. I really do think it'll be a driver for years to come for the Chinese and operations revolving around it.

Lloyd Brown:

Yeah, I definitely agree with that. And we still see and we observe a lot of targeting in region, as you highlighted, of governments and with a regional government that is strategic to the Belt and Road, what's their take on Chinese investment projects? Are they pro-China, or are they against China? Because we've seen a lot of reversals with some of the projects that China's tried to implement along the Belt and Road. Like in Malaysia, they had a giant project that recently, when the government changed, they started to put the brakes on that. We've seen that occur also in Indonesia, as well.

And so in order to stay a step ahead of their investment opportunities, they will conduct espionage campaigns against these governments to keep track of that information, so they know what to do next, politically. It's important to understand that the espionage drivers are driven through politics, economics, and through the military. And so when you observe what the government does outright, on one front, then you can understand where espionage activity may come with another. And so when you look at the trade pacts that they are signing, I think they signed another one in Italy, and some of Eastern Europe. And some of these drivers they have, you can see the types of espionage activity that follows that as well.

Lloyd Brown:

And then they're doing it not only on the cyber front, but people also forget that China is also very prolific in the human front too, and human operations can help enable cyber operations. And it also helps validate the information that they took, or they may have stolen, they can use to help align with their political objectives. So if they managed to obtain a source inside a government organization in Eastern Europe, then they can hack and pull some of that data and that information and correlate it together to have a stronger sense of what they may need to do next, politically.

Another thing too, dialing back a little bit, when we talked about the shifts, the South China Sea in the Spratly Islands, was still a very large driver of Chinese espionage. And they're still

keeping a very strong track on Southeast Asia, and Asia in general, with government and military because they are still strategically seeing this as their backyard, and that they're trying to control those resources, and those waterways. And we still see instances of in Indonesia, a fisherman catching the Chinese submarine, because they're still very concerned with this. So as much as they look towards the west, as well, they're keeping a very strong eye on their neighbors. And that way they can get influence, and especially with the way that politics has been out of the west in the last few years, and they can continue to garner and build influence to the point where the nations are relying on China even more. And all this drives their espionage activities.

Luke McNamara:

You touched on, I think, earlier, the activity we've seen around elections related to Chinese threat activity. So I want to go into that a little bit more, because I think that's a piece that hasn't gotten this discussion as much, I think maybe in the west. We've certainly been examples, I think like in the case of Cambodia, where there's been more widespread reporting around that. But this is alongside Russia that has certainly been active in targeting and interfering in elections. This has been activity we've seen from China in multiple cases at this point, right? And what does that typically sort of look like? Because it has been different than what we've seen from Russia.

Scott Henderson:

I think this is kind of what those areas, too, that are a little bit different. And I think Lloyd will probably have a lot better perspective on the IO side of this, which we've also seen, which may have been kind of subsumed under the network systems department, looks like IO 4th PLA might have gone there as well. But with China, I think typically what we see is monitoring, it's not influence operations. In other words, they're not... At least from the cyber espionage side. It's not an operation that says, "Okay, I want to go in and influence Malaysian lecturer, influence the Cambodian election." What it is, is they want to get strategic, I guess, advancement, they want to have advanced notice of what's going to happen, who's going to be pro-China, who's going to be against the project. And so that's kind of what they're looking at versus necessarily picking a winner or a loser in that election. Now, with the IO operations, I think Lloyd might be able to say a little bit more about that because I'm honestly not that well versed in that side of the actual influence operation.

Lloyd Brown:

Yeah, so I think you're right. They're not necessarily trying to pick a winner with their operations and election targeting. But they do continue to try to influence either pro Chinese sentiment or like anti-western or anti-strategic sentiment. And so if the other side, in a political situation in the country is not necessarily aligned towards China, they'll go twofold. They'll use AI generated images, they'll use coordinated inauthentic behavior on Twitter, on YouTube, on social media, they'll use that to help paint a negative light like they were doing this constantly

during the Hong Kong protests of making the protesters look bad, saying they did things. And I mean, there's hands off the amount of things that they would say, like protesters are responsible for shooting a child or getting a child killed, they really delve deep in and try to divide that line.

And then they also do it just outright publicly. I think politically, they've become a lot more brash in what they've been saying on Twitter. I mean, I even saw a tweet from a Chinese diplomat open, that just called a US Congress woman, I think, a bitch, just outright, in response to a tweet. And so they're very blunt and forward with using even images that are not true. I think this happened recently, also in Australia, where they tried to paint a bad picture of Australia in Afghanistan. And they use some misinformation and mispictures with that, and got called out by the Australian Government. But there's really no apology or no denial from that point. And so you have outright diplomacy that's making blatant statements and being very forward. And then you have the inauthentic behavior that they're using in order to try to build sentiment for their cause or against their cause that is regularly happening.

Once you get a hold of this, and you can even see with just different countries, that globally, we're seeing it in Latin America, we're seeing it in Asia, we're seeing it in South Asia, it's very low cost now to conduct inauthentic Twitter campaigns where you have one bot tweet something and then 10,000 bots tweet it, and all with accounts that are easily auto generated and auto created. And so it's a low cost, high return move, for them to constantly conduct this type of behavior, and run these campaigns, and just regularly run them in support of what they're doing politically, militarily and economically.

Luke McNamara:

And I think a very important point here is the fact that cyber is kind of one component amongst a lot of different tools that they have at their disposal. So when it comes to elections, maybe we don't see the usage in a disruptive or destructive way, or maybe in the sort of hack and leak style that we've seen from some Russian operations. Maybe you don't see that particular avenue to influence sort of the democratic processes, but we know from other reporting elsewhere, the usage of newspapers, traditional media, the sort of activity you're describing here, increased presence on forums and social media, everything kind of takes a different flavor when you're looking at the different state sponsors of this sort of activity. And it seems to be also based on the different tools they have at their disposal.

We can't always forget, back to the point I think they were making earlier about insiders and the sort of human threat, Lloyd, there's something we've seen increasingly, I think, here in the United States, these indictments and cases that have come out particularly from universities where you've had people who were working on behalf of the PLA undercover. So cyber is only one tool they have at their disposal, and how that interplays with other operations, but again, the human spaces is interesting to see.

Lloyd Brown:

One thing to point out with what you just said, with the indictments in the US, the US has been a lot more public about calling out the activity that they have observed. But the US is just one portion of the world. Who knows to what level that is occurring globally, all around, that just doesn't get called out because they don't want to highlight any embarrassment? Because there's also a lot of countries that may not highlight very obvious Chinese espionage cyber activity, because there's an economic piece tied to it. They're receiving millions and millions or billions of dollars of investment, and they can't outright call because of either military or economic ties, they won't come out and say it. The US and a lot of countries like in Europe, that may or may not be as reliant on Chinese investment, have been taking a step forward in calling this out, but this was occurring all the time, and just kind of being swept under the rug or kept out of the public eye because of the big strategic aspect of the Chinese money.

Luke McNamara:

You mentioned money. So that's a perfect segue to the next question I was going to ask, which is in each one of these episodes it's been interesting, while we're primarily looking at state sponsored espionage, some of these other areas start to come in and one of those is sort of the nexus between espionage and cybercrime activity. So in the case of North Korea that we covered, obviously very well documented, and our sort of analytical assessment of that is that a lot of that activity targeting traditional finance, cryptocurrencies, etc., it's activity on behalf of the state to support the Kim regime and the government and some of the programs there.

Sarah talked about, in the last episode, Iran, examples where we've seen some Iranian actors engaging in cybercrime to support those operations. But when we give them a case of China, and activity we've seen, probably most notably in last couple years, at least by APT41, how does that actually play into this? What are we looking at when we talk about an actor that's engaged in both cyber espionage and cybercrime? What do we really mean and what's going on there?

Scott Henderson:

You bring up a great point, and I think APT41 is one of my favorite group. And it goes back to a guy named Tan Dailin. I've been tracking this guy for years, probably around 2006 2007 when he was basically just a hacker. He had started out, he had a website it was called MG hacker. And if you know Chinese and pinyin, MG is the pinyin, it's méiguī, which is Rose. So you'll see him called Wicked Rose, Withered Rose, I believe some of our competitors have named their teams Wicked Panda. So he's a well known actor. And he's well known... I don't know if you guys are familiar with a guy named Willie Sutton. He was a bank robber in the US. And at one point, somebody interviewed him and they said, "Why do you rob banks?" And he said, "Because that's where the money is." And I swear Tan Dailin has reminded me of Willie Sutton forever.

And one of the things when I used to read his blog before he obviously became a member through the indictment process that we saw a member of APT41. He was stealing like crazy. And one of the things he wrote in his blog that I read about it... This is one of the most open and damning things I've ever seen anybody just publicly commit. He was talking about the old generation of Chinese hackers, patriot type Chinese hackers, they wouldn't hack internally. That's because they were patriot. And he said, "No, that's not the reason at all. Basically, it's because the Chinese were poor, they didn't have disposable income, there was nothing to steal." So that's why they were always going out. And you saw them doing gaming, that was a big thing for Chinese hackers during that period. That's how they were getting a lot of revenue, was going out doing gold farming, stealing characters, reselling them on these websites and stuff like that.

I don't know if maybe it's just vestigial for groups like APT41, who've typically maybe made a revenue stream from that and is still carrying on. Because it clearly doesn't seem to be a state... At least, I haven't found that state thing where, like North Korea, it's clearly provide revenue stream for the sanctions and things like that. China obviously doesn't appear like that. So I don't know if it's maybe some of these groups that the Ministry of State Security has contracted or actually worked directly for. But these guys are side hustling, because they've done that, that's a big part of their character. So I honestly, I don't know the answer to that. But when I start hearing that sort of mixture of cybercrime and cyber espionage, he's the personality that really springs into my mind.

Luke McNamara:

You're suggesting that there's more of a tolerance for letting some of those groups, some of those resources, get used for activities, some extracurricular activity? As long as you bring back, maybe utilize some stolen certificates, to help out some of your day jobs to operations, then go ahead and do some stuff on the side, we're okay with that.

Scott Henderson:

Yeah, I think you're right, Luke. That's my thoughts on it. They tolerate it. It's part of the things that they do, but it's obviously... State tolerates it, but it's not their primary function, I don't think.

Lloyd Brown:

I think you're right, there's definitely a massive underground cybercrime marketplace that occurs within China that we have observed, and there is some targeting of large data of like PII information within China, but when you tie it to the groups that are responsible for helping with espionage, they do look more on the outside. And it's interesting, because if you were to look at the Tigers and Flies campaign that was all anti-corruption, you would think that maybe they would try to adhere or keep their contractors, or potential contractors towards just staying

focused on the mission. But maybe that's one of the benefits and it's also good practice is to let them go out and moonlight on the side.

We have observed them doing everything from dropping crypto miners to conducting extortion campaigns in addition to the APT41 tie in with the Malaysian executives in terms of selling game characters. And I think, or at least my personal opinion, is that we'll start to see a lot more crime activity, not just out of China, but just the APTs in general moving on because it's very lightweight. When someone breaks into somebody's house, they're looking for an important document in a book, and then there's jewelry that's expensive sitting there on the counter. It's like, "Well, I'm here, why not go ahead and take it?" And so that's the same way in terms of when they drop their crypto miners, and they'll at least get some Bitcoin farmed out of it, or some other cryptocurrency farmed out of it. They'll continue to find new ways of conducting these operations. And I'm wondering when it may possibly happen that they start doing the kind of ransomware operations, if they ever pivot to that level, or if that scene is too loud, since we talked about them needing to be a bit more stealthy?

With the different investigations that I've observed, they've been more or less under the radar and just talking to executives in terms of extortion operations. But I think that there will always be an aspect of cybercrime tied with some of these groups, especially, and mainly the contractor groups that are used by China. And I think, internally, there's a lot of research on contractors and the roles that they play with APTs, and we'll have a piece coming out on that in time.

Scott Henderson:

Oh, nice.

Luke McNamara:

Yeah, I think it's a fascinating example of an analytic problem where you're trying to assess command and control of these resources, how tightly they're controlled by the state sponsors that they are serving, how much free rein do they have? And you could make the argument in some cases where you see crypto miners being deployed or other sorts of activity, and maybe they'd make that case to the superiors, "Hey, this is a good way to obfuscate what we're really here to do." Makes it a little bit harder to maybe determine motivation. In some cases, maybe, particularly as economic conditions tighten around some parts of the globe, maybe it's something that operationally it's being used to fund some of their operations, such as we've seen, potentially with Iran. But then maybe it's for the personal wealth collection of the individuals who are moonlighting on the side or seize an opportunity to grab that jewelry, make an extra buck.

Scott Henderson:

And we've seen historically, Beijing is tolerant of that type of activity within the military. Before

the reform, we had senior military commanders who were running industry in their particular region, we've seen them... And a lot of this wasn't necessarily fact that they were making money, I'm sure they were. But a lot of times, these guys had to get extra money to pay their people, to feed their people, we would see the Chinese, the military take time off to go do planting and harvesting. If you picture this in your head, you've got a professional military who's doing side operations to feed themselves, to clothe themselves, to get equipment. So they're doing similar type things. And Beijing was very tolerant of that type of activity.

So maybe that carries forward, that mentality carries forward into cyber operations where these guys are making a living, and not just from the salary that the MSS or whoever is paying them, but also doing some of these side jobs.

Luke McNamara:

Well, we've covered so much here, and I feel like we have only barely even scratched the surface on this problem set. I want to kind of wrap up, though, and get both of your takes on what we could expect to see potentially this year in terms of some of these threads, pulling on them, some of these trends that we've been seeing start to take shape and form some time. Whether it's the drivers of economic investment, things like Belt and Road, whether it's the increase focus and importance of key technologies like semiconductor chips, you've seen right now, as Lloyd mentioned earlier, sort of a renewed focus around supply chain, both in the hardware and software standpoint. Information operations and the greater way that that may be rolled into other sorts of operations that China is doing in cyberspace.

So what are some of the things that people should be on the lookout for this year, as potential milepost for continuations of activity, pivots to something else, or just something that maybe we're not seeing yet that you could see change very quickly?

Scott Henderson:

I hate forecasting, because I am always wrong. I am always wrong. It's just that way. Flip of a coin, 50/50, I'm going to get it wrong. So I'm not going to step too far out on a limb here, but I think what we're going to see... I think it's going to be mirrored a little bit with their diplomacy, we're going to see aggressiveness. I believe we're going to see more aggressive operations. I think they'll obviously continue the obfuscation, but I'm not sure if they're going to be as sensitive to being exposed. So I think we might see a little bit of that. I think we're seeing a more efficient beast animal out there. I think they've started getting better at their job. And I think there's going to be operations that could surprise us. I think one of the things that Chinese do really well and have always done well is reconnaissance, which is something we don't talk about a lot. These guys, if you start up a new service with your company, they'll probably know it before anybody else does. They might know it before the CEO of the company knows it.

So I think we'll see aggressive targeting. They put the P in persistent for APT. So I think these

are some of the things we'll see. What industries they'll target? Clearly, I think things along Belt and Road. And especially if we start seeing some negative pushback like the debt trap stuff that we've seen, so I think the people are pushing back against that might be targeted as well. So any kind of pushback or major elections that come up, I would definitely say that that's going to be a prime target. And that's as far as I'll go on forecasting.

Luke McNamara:

You're going to have to be bold Lloyd.

Lloyd Brown:

Oh, yeah, I'm throwing it out there. Again, my personal opinion and observations, keep an eye on Taiwan, Taiwan is going to be a testbed for a lot of things in terms of targeting and the new administration in the US. And now that Hong Kong has seemingly come into the fold, and China, I expect there to be a lot of tests with Taiwan, you could already see more aggressive military flights happening there. And so I think espionage operations are in conjunction with that, and the United States trying to counter influence.

COVID, and information about the handling of COVID. There's a lot of highlighting success that China says that they have with handling COVID and the vaccine, and then making other countries look less popular in relation to how they handled the virus. You're right, with the Belt and Road, that's still continuing, as well as the South China Sea, you'll continue to see targeting of that. We get questions a lot with organizations that have a presence or are conducting business in China and wondering about the cyber risk associated with that. But when you are mandated to use certain things in order to do business in China, those create third-party risk. And that's something to look at, because they may not accept any other form of submitting for a real estate license in China other than using a specific program. And they could go and target those websites and get in maliciously that way.

You would still see potential social media targeting of different companies and analysts like us, the amount of weird and odd requests that we get, especially those who will be speaking in public, they come from somebody who has three friends and went to Beijing University, is very interesting. And I think that it's an easy thing to observe, you saw with the North Korea social media targeting shows how prolific you can be with researchers. And I think that it would be low effort for them to conduct those types of operations. And I expect them to continue to quickly use and weaponize CVEs to come out for popular programs.

I still think this third party compromised trend is... Last year was year ransomware, this year is third party compromised for sure. We're already just in February, and the amount that's occurred already has been very high. Things that strategically... to see them politically with what they're doing with countries like Australia and influencing coal production. So key trade industries that they focus on, like rare earths, and rare minerals, which China produces a good majority, like 80% plus of that, I'd expect to see activities around that.

I spoke earlier about telecoms, never going away. The Huawei push is such a strategic one, that we'll see them continue to focus on that, on mergers, everything from organizations that are responsible for regulating telecoms, to contract or mergers between organizations, to companies that are helping bid for providing infrastructure related to these, I'd expect to see that. And even though in the Western world, we observe a lot, and we talk about a lot openly of the operations that they have, cannot emphasize enough how a majority of the operations that they conduct are in their backyard in Asia as a whole. And they are so heavily involved in every country in the region. They are pouring a lot of resources because they want to make sure, and I think this goes back to traditional Chinese thinking, that their homeland is secure, and the areas around their homeland is secure before they expand outward.

I would also be interested to see if activity continues in terms of India as well, because that has been a hotbed of activity with the skirmishes that have happened on the border with India. And India also has a very capable cyber offensive capability as well. Then, even looking into Vietnam, Chinese targeting Vietnam because there was reporting of Vietnam actually targeting China. China still has to play a defensive game. Everybody's good at offense, but no one's good at defense. The internet wasn't built for defensive purposes, it was built for sharing. And so I'd expect to see continued targeting of China.

And then one last thing I'll touch upon is Myanmar. And it's interesting because Xi Jinping was there around the 19th or 20th of January. And I don't know if they were able to forecast the coup. And it's interesting that they have not outright said or made a statement in response to the coup and whether or not that's because they had cyber espionage sources that they had already hacked and they had an understanding of the situation before it happened. Or maybe they were caught off guard, and they're just being silent. That way, they're not seen as taking one side or the other, because there's a lot of geopolitical interest with what's happening there, and watch on what's happening in the region.

And we'll still see continued targeting of Uighurs and Tibet, and the things that they're doing in that region, it's just incredible the amount of leaked documents that have come out about it, a lot of testing of malware that gets installed on Android or Apple phones, the use of facial recognition and AI to help supplement a lot of their activities, which is why they keep stealing large swaths of data because they have very poor front AI capabilities, and they can use that information in order to comb quickly through the data and correlate, create patterns that they can use for future human targeting, they can use for future espionage targeting. And so I expect to see them continue to do that.

And then the made-in-China 2025 plan, and their five year plans, if anybody wants to know with a magic eight ball what's coming next, just read their policy, because they tell us outright and you just have to take the time to read it and understand it.

Luke McNamara:

So in summation, expect targeting of everything.

Lloyd Brown:

Yes.

Scott Henderson:

One of the things I really liked, I'm going to coin the phrase and steal it from you, Lloyd. We've heard about brown-water and blue-water navies. I like that for the cyber espionage, brown cyber activities regional, and the blue-water cyber espionage activity extending out, so I like that.

Luke McNamara:

So last question. And I can't believe I didn't ask this of Fred or Sarah and Lee in our episodes, but favorite APT group or operation or campaign? If you had to pick one that really stood out to you.

Scott Henderson:

For me, it's always been Tonto. And it's really because I think I understand them better than the other groups, honestly, I've got a much more detailed infrastructure, the different actual military organizations that support the military region. So I think Tonto is definitely my favorite. And it's so focused on some of the more high profile nation states that we've seen, Russia and Japan and South Korea. So it's got some real high profile type targeting and industries that we've seen, so I'm voting Tonto on this one, Luke.

Luke McNamara:

Lloyd?

Lloyd Brown:

I'm going to be the obvious, and go with a big powerhouse, I don't know, the Lakers, or the former patriots, I'm going with APT41. I got to work side by side with FLARE and Mandiant on the MESSAGETAP operation. And it's just the different levels of complexity to go to everything from video game targeting, to being able to read text messages in real time and have that insight and that strategic thinking of what they did is just incredible. The range of things that we've seen those operators do, and how they continue to refine their operations, what they do, it's incredible to me. And if anybody hasn't read the APT41 report plug, it's a good one. It's a long one, make sure you go and take a look at it because it's incredible.

Luke McNamara:

No, definitely agree with that. There's so much there. And I think we've talked about the sort of historical transitions and shifts in Chinese cyber espionage, and APT activity. That's one that I

think really personifies a lot of the direction that China's going towards today. Well, there you have it, APT41, the Lakers of Chinese cyber espionage. Well, Lloyd, Scott, great to have you today. Thanks for helping us break down what we've seen historically, today and going forward, what we might expect from China. So thanks to both of you, have a great day.

Scott Henderson:

Well, thank you for having me.

Lloyd Brown:

Take care. Thanks for having us.

Luke McNamara:

Take care.

Scott Henderson:

Take care, guys.

Lloyd Brown:

Cheers.

Luke McNamara:

All right. So we initially recorded the first part of this episode, and then there was an event that happened, which would make it very weird to release that episode without at least touching on it. So in order to not miss that sort of glaring operation that has taken place and sort of dissect a little bit of what it means, we have Lloyd back here on again to talk about some of the recent activity that in the news has been discussed about as the HAFNIUM activity that Microsoft has reported about targeting Microsoft exchange.

Luke McNamara:

Lloyd, great to have you back again.

Lloyd Brown:

Thank you. Thank you.

Luke McNamara:

I guess frame for us for what we know right now about this, and then maybe we can get into back from our earlier first part of this discussion, maybe sort of how it relates to what we've seen more recently from Chinese espionage groups and what's kind of fortends going for it.

Lloyd Brown:

So when this activity came out and we took a look at it, internally we attributed this activity to two different UNC groups, UNC2653 and UNC2648. And we attributed these UNC groups to Chinese espionage activity that aligns up with what Microsoft talked about, but essentially four different zero days were used to exploit Microsoft exchange, and then there's been reporting of just a very large number of targets. And so this actually ties into the wrap-up discussion that had previously, where it was suspected that China would utilize supply chain compromises, third-party exploitations. And so that's exactly what occurred. And this also just goes to show how we have to stay current on threat Intel because the threat landscape continues to change and evolve.

And so upon discovery of that, tons of organizations have been examining the Microsoft released a very simple patch to kind of help mitigate some of the factors from this, but we also are realizing that not only did two suspected Chinese UNC groups do the targeting, but also there are other, at least three other clusters of activities that we track with this and some that's been recorded publicly as being criminal as well. And so it also shows the speed at which criminal organizations also conduct this targeting.

There are reports of ransomware and crypto mining being quickly exploited after the vulnerability was announced, but this also shows more brazen activity from China knowing that there are really no real repercussions for them conducting large scale targeting. And when they deploy their web shells to multiple organizations, this gives them the ability to pick and choose where they utilized to go back and try to perform additional compromise of networks that they find adventurous.

Luke McNamara:

Yeah. I think one of the things in there that I think is noteworthy in what you're talking about is when we do see zero days being utilized by APT groups like we're seeing here, which I think as we noted in the first part of this, has become less frequent with Chinese espionage groups and even a lot of other APT groups that we track. But when you do see the disclosure around those, typically there are a range of threat actors from different adversary motivations that jump on pretty quickly and try to exploit this before organizations have patched those systems. And I think that piece going to the point you're making about, we have to separate into two specific UNC groups that are tied to the piece of this that we believe is connected with Chinese APT activity, then there's also we have that separated from several other clusters that we're tracking that are also doing this exploitation of these particular vulns in Microsoft exchange.

And I think that is to a larger piece around the importance of correct attribution and clustering

of groups, because you don't want to start looking at the entirety of what's happening right now in terms of the targeting of Microsoft exchange and lumping that all into the same set of activity. And I'm sure we'll probably see more clusters of groups over time, but is there anything, I guess maybe about the activity itself, and obviously this is still unfolding, but in terms of the targeting, we know public and private sectors impacted during the United States and I think Southeast Asia and maybe elsewhere, but anything still that we can kind of characterize as in terms of like the intent of this activity with what we're seeing?

Lloyd Brown:

This likely fits into just their general overall strategic targeting. And they just did release an update to their plan. We're seeing that it's pretty much the same with a little bit more targeting as before in terms of what China finds to be a strategic interest.

Luke McNamara:

You're talking about the five-year plan, right?

Lloyd Brown:

Yes.

Luke McNamara:

Of the 14th five-plan that just came out.

Lloyd Brown:

Yeah. Wait, I think John Hultquist, who's one of our Intel higher ups. He made sure to mention that and he highlighted that too. So check out his tweet on it. And we also have internal Intel highlighting that as well. This kind of reminds me a bit of the shadow pad incident, where they used CCleaner and they targeted a bunch of organizations and then narrowed it down to what they want. So it's not like this is super uncommon that they have the capabilities and wherewithal to try to conduct this type of targeting.

We did see a large amount of, at least that it's been reported, that there's a large amount of targets within the United States that were hit. There were small to medium enterprises, which is a little bit different than what we've seen before, but PII information is still PII information and it's still of value. And when you have large data repositories and artificial intelligence capabilities, gathering as much data as possible so that you can correlate it and use it for patterns, it's still of high value. And they are obviously capable enough and have the abilities to gather all this information so that they can utilize it and go back and potentially exploit it later in the future.

Luke McNamara:

Yeah. Well, will be interested to see how this develops going forward, and I think it is interesting, not just the particulars around this particular incident, but the fact that it's following on from the solar winds and sort of the discussion that you're seeing emerge more and more, refocusing the conversation around the security of the supply chain. So it'll be interesting to see where that develops.

And I would also mention, given that we've talked a lot about UNCs here, however ruin, go check out a blog that we put out recently. I believe it's called DebUNCing Attribution, but it talks a little bit more about the clustering process that we do around emergent activity like this. Lloyd, thanks for coming back on and hopefully between now and when this episode is supposed to release, nothing big happens again, but if not always great talking to you. So take care.

Lloyd Brown:

Always great talking to you too. Thank you.