Eye on Security

The “Big Four”: Spotlight on North Korea

Transcript

Luke McNamara:

Welcome to another episode of the Eye on Security podcast. I'm your host, Luke McNamara. And joining me today, we have senior analyst on the cyber espionage team here at Mandiant, Fred Plan. Fred, how are you today.

Fred Plan:

Hey, Luke, doing good. Thanks for having me.

Luke McNamara:

Definitely. So this'll be the first in a series that we're planning on doing. Because I've now said that publicly, we're committed to this, but we wanted to do a series to kick off the new year, 2021, talking about or focusing on a podcast each on the big four, what we colloquially refer to as the big four in this space, Russia, Iran, China, and today we are here to talk about North Korea. So who better than you to kickstart us here.

Fred Plan:

That's right. Democratic People's Republic of Korea, North Korea.

Luke McNamara:

That is the Korea that we are here to talk about, yes. I was thinking about this and we were talking about this a little bit beforehand of where do we actually start if we're to talk through sort of North Korea's cyber capabilities, what we've seen historically from North Korea and potentially some of the more recent activity, but how organizations should think about North Korea and cyber operations. But I guess for someone that's completely new to North Korean operations, to give us the cliff notes sort of history of what we've seen from North Korea, what they've dabbled in when it's come to cyberspace activity, kick us off. How would you frame that?

Fred Plan:

Yeah. So that's a good question. There's a lot of different ways to think about North Korea as a player in cyberspace. But I always like to take it back to what the country fundamentally is about, right. North Korea, of course, is a relatively small nation state in Northeast Asia. Their primary geo-political concerns are vis-a-vis there relationships with their neighbors, especially South Korea, China, Japan, as well as the allies of those countries. So in the case of both South Korea and Japan, North Korea is extremely concerned with the United States.

Not going into too much detail, but the other thing that North Korea's really known for is the level of control that the regime in Pyongyang has over pretty much all aspects of society, over the military, over the status of the country as a whole. So one thing to consider about North Korea, especially when looking at cyberspace is, how North Korea's relations, not just within the region but globally have steadily degraded over time. And how there's kind of this inverse relationship with North Korea's cyber capabilities continuing to increase and improve in terms of quantity and quality, and how that is in contrast to how badly their relations with their neighbors have become.

And so North Korea's in this unusual position where here's a relatively small country that has steadily developed increasingly capable cyber operations despite economic sanctions, despite steadily eroding diplomatic relations with it's neighbors. But then at the same time, this is kind of the corner that the North Korea has painted itself into, right.

So backing out a little bit. Trying to talk about the nation state example a little bit further, The vast majority of nation states, of course, have different ways of relating to other countries or different tools of statecraft available to them, so diplomatic relations, economic ties, and things like that. North Korea is at the point where it doesn't have these things. It's only remaining friend of significance, really, is China. It's heavily burdened with economic sanctions, it doesn't really have many tools of statecraft left at it's disposal except just the annual parades that show off North Korea's military might. And so North Korea just doesn't have many options left to it.

What the state does have however, is they've put a lot of investment into their cyber capabilities. And this is kind of North Korea's only remaining tool of statecraft left. And it has a huge impact on the kind of operations that we're seeing from the country. And conversely, I believe that it's reflective of the kind of concerns that North Korea has as a state.

Luke McNamara:

And that's one I think we'll definitely get into a little bit later, talking about some of the examples that we've seen this year of North Korea and cyber-espionage in particular and what that potentially allows us in terms of a window into the things that are priority to the state, to the Kim regime. One question I guess I have, when we think about the sort of expansion of activity, and North Korea would definitely be, I think fair to say, in the category of more

emergent cyber-power in the last several years, five to seven years, than China or Russia that's been established for some time. Talk to us a little bit about I guess, what we used to see five, seven years ago from North Korean threat activity, in terms of the sort of regional focus. Wasn't a lot of it more focused around South Korea? You talk about this sort of regional, neighbors that it has different relationships or lack of relationships with. A lot of that we've seen expand to different sectors and different industries, but we've also seen expand away from where it originally began, in terms of South Korea.

Fred Plan:

Yeah, for sure. So as I mentioned, South Korea is absolutely North Korea's biggest concern. They're right up there, they're the biggest rival regionally and in terms of everything that North Korea's trying to do. And so the vast majority of the early cyber-operations that we observed were pointed from North Korea to South Korea. And this is kind of typical of what we see of emergent cyber-powers in general. A lot of these started very basic, they were DDoS attacks, or website defacements, and things like that. And these were, I mean they're comical now in comparison to what North Korea has grown to become. But yeah, these were really basic attacks, they were largely disruptive, almost all of them were pointed against South Korea, different government offices, financial sector, Korean media, things like that.

And then over time these became progressively more complex, they became more capable, and North Korea gained more confidence in their ability to carry out these cyber-operations. Then the big coming out party for North Korea really was the Sony attack, right. At that point we had seen North Korea interested in targeting outside of the region. They had targeted, for example, US forces that were in South Korea. They had targeted other US government organizations, US military at that point. But to see them step over the line and target the US private sector, to target a corporate entity was really the point where North Korea grabbed everyone's attention, right. It was North Korea seizing the moment and coming out as, we are both willing and able to carry out this kind of operation and target a corporate entity with destructive attacks. And things have just ballooned from there.

South Korea has become progressively more destructive, they have expanded their targeting beyond just South Korea and the United States. They're activities have expanded beyond just espionage operations. Now they're doing a lot of financially motivated activity. Their espionage operations now target a lot of other countries. So not just within Northeast Asia but also financial industry or financial institutions in Southeast Asia, in Latin America. And yeah, it's escalated very, very quickly from there and North Korea's now a global player in a way that it previously would not have been without this cyber capability.

Luke McNamara:

Yes. And for sure, no longer an emergent player, but a player that has emerged into the space. And I guess we can't really talk about the sort of nature and current landscape of North Korean

cyber-operations without really diving into the groups. And that's always, I guess, the discussion about any of these different countries we talk about is the sort of nature of how organizations such as ours group threat actors and separate out kind of the different clusters of threat activity. And in the years have changed and morphed. So in terms of the big ones that we track, the big clusters of North Korean threat activity we track, what are we looking at when it comes to their cyber-operations and activity.

Fred Plan:

Yeah, I mean, so kind of getting back to what we were just talking about historically, how this has grown. I mean, again, North Korea's a relatively small country and it's central control is very strong. So early on it was pretty easy to assume that any cyber operations that we were able to observe out of North Korea were all interlinked, it was all a relatively small subset of activity that was interconnected. But over time it became very clear that there are multiple, distinct groups that are operating out of North Korea and each of these groups have different specializations and different focuses. So, yeah, just very quickly off the top so some of these groups are very focused on, for example, financially motivated operations. APT38 is the best example of this I can give. This is an operation that was very focused on carrying out long-term, extended deep dive bank heists against global targets. And that's really the main focus of what APT38 does.

Then there are other operations which are more concerned with conducting cyber-espionage campaigns and strategic intelligence gathering in the general sense that we usually talk about, APT groups. So groups like that include APT37, as well as groups that are publicly referred to as Kimsuki is another one of these operations, or there's this multiple clusters or multiple UNCs that we track that are linked to groups that we generally lump together as TEMP.Hermit. A lot of times the TEMP.Hermit ones especially, are called out publicly as Lazarus. Largely based on malware overlaps, linked all the way back to the Sony stuff.

But if you look at how those groups split up and the kind of activities that they're doing, it's pretty clear that there's multiple subsets of activity that are all doing different things. Some espionage stuff, some financially motivated stuff, some of that activity is very focused on targeting the US military and defense sector for example. Whereas, there's other UNCs that almost exclusively do financially motivated activity, the cryptocurrency stuff for example, or more recently more of the majcarp or web skimming activity that we've seen coming out of North Korea.

And then outside of those clusters that I've mentioned, the TEMP.Hermit stuff, the APT38 stuff, there's the Kimsuki espionage stuff. There's another cluster that's kind of off to the side and that's the clusters that typically get reported as Andariel. And this is another espionage operator that we see going way back, very focused on the South Korea espionage campaigns early on. And then over time those also started targeting more globally, especially against the United States.

So there are several, I don't know if you want to call it mega-clusters, but I guess it depends on how... What are your units of analysis, right? What units of analysis, at the country level or at the operational level, or at the tactical level? But for sure, these groups are distinct in their tool sets and how they do what they do and the targeting that they have. Again, North Korea's a relatively small country. There's a ton of sharing between these groups, especially in terms of malware. There's a ton of overlap in terms of their targeting, especially against either South Korea or the United States. Now that's created a problem in terms of attribution and in terms of defining what is a group, especially when it comes to North Korea.

Luke McNamara:

Yeah. And I think that's one of the reasons why I wanted to start of the series by talking about North Korea. Because I think there's some interesting aspects of what makes attribution and the separation of different clusters somewhat difficult, and I think highlights how messy sometimes attribution can be. Or rather, the difficulties of attribution with really messy clusters like what we see coming from the North Korean groups.

What I think, in particular I guess, two things to pull on a little bit more, you mentioned the financially motivated activity that we see. That's interesting to me, when we see... In some cases, you could make maybe the case for increasingly different types of, what historically we've thought of as cyber-espionage clusters that have engaged in some activity that looks financially adjacent, shall we say.

So for example, the analysis and analytic line around APT41 and the extent and kind of way that they approach financially this sort of cyber-crime and kind of how we frame and think about that is different as we perceive them to kind of be contractors than how we frame groups from North Korea like TEMP.Hermit or APT38.

Fred Plan:

Yeah.

Luke McNamara:

And I think that part of this comes into, I guess our understanding of how we think about North Korea as a state, right, to go back to some of your points at the very beginning about this. But maybe walk us through that a little bit of why kind of we've reached those analytic conclusions in terms of the financially motivated or cyber-crime activity of some of these groups, that it looks different than what we've seen from other countries.

Fred Plan:

Yeah. So part of that, like you're alluding to, part of that comes down to how we believe these cyber-operations emerge in these states in the first place. So for example, in the case of

APT41, which is just Chinese operation that conducts both the financially motivated cyber-crime, as well as cyber-espionage. We believe that much of the cyber capability in China had kind of grew up on its own in a way. There's this big underground, in China, there's this developing body of underground actors that were kind of doing things... red hat hackers and stuff like that. And APT41 is a natural extension of that. Here's some guys who are doing financially motivated activity and then decided to become contractors and continue on with both types of activity, espionage and cyber-crime.

Fred Plan:

North Korea's is really different because in North Korea everything is controlled by the state, right. You don't get to go online and become your own hacker in North Korea. And so most of the capability developed because the central authority put some number of military units through training, they organized a pipeline effectively of specialized trainees would be carefully selected based on their loyalty or their different skillsets, or how they performed in training. And they would be set up to be part of these specialized units that really were decided from the top on down. As you guys will now be the cyber special forces or you will be the specialized cyber units that will be carrying out the will of the regime, you will be carrying out the will of the Kim family and Pyongyang in cyberspace.

And so it's a very top down sort of capability that was built up. It comes down to the level of control that North Korean state has over the people. Not everyone can access the internet, not everyone can access these sort of training or these skills. And so that shapes it in such a way that pretty much all of the cyber operations that we link to North Korea are almost certainly all linked to the military, even when we find that they're linked to different cell companies in different countries, or they're operating in a way that it's clear that they're conducting cyber-crime activity and making money, it's still ultimately for the North Korean state. It's still ultimately for the regime. And everything that these operations are doing are in the interests of the regime. And again, that's very different from say, Chinese cyber-crime actors who are making money on the side for themselves or Russian actors where there's very clearly espionage operators that are acting on behalf of the state but then there's this enormous body of different underground forums and crime groups and carters and all this assorted cyber-crime activity that's completely beyond what the nation state would be actively supporting in Russia.

And so it's a very different structure and that's what shapes how these North Korean groups operate and the way they relate to each other in terms of tool sharing and operational similarities, but also in terms of what they're pointed against in terms of North Korean problem sets, right.

So what are the things... Maybe this is going to be me preempting your question... But it's the case where a lotof these North Korean groups, you could kind of see them as a proxy for the things that, you can see their operations as a proxy for the things that are most concerning to North Korea's interests at that moment.

Luke McNamara:

Well, I guess this is a preempting of my question. I guess I was going to ask you is, with that framing, is it almost an inevitability that we would have seen North Korea eventually turn this capability, which as you noted has become more capable over the years, they've dabbled in a little bit of everything, the disruptive activity, the espionage, but they now have this resource that, particularly against the backdrop of over the years increasing sanctions... And then you think about the other thing that in Opensource, they're well documented and known for is having extensive operations related to money laundering and counterfeiting currency. Is it almost inevitable that we would have seen this sort of activity with... whether it's the targeting of crypto currency and the sort of advantage that they saw there, particularly kind of early on, going after these exchanges in South Korea that were getting kind of stood up and maybe didn't have the best security, to what we've seen in terms of the big bank heists that we've seen with respect to APT38? Is that somewhat of an inevitability when looking back on that?

Fred Plan:

Yeah. Was it inevitable? I don't know if you can say that, but for sure it was the path of least resistance. Like you said, North Korea already had this capability in real life, in terms of counterfeit pharmaceuticals or just straight up meth. They had the money laundering at works. I mean, ultimately North Korea is still a nation state, so there's a lot of things that they can do that you can do when you're a country. They had this capability when they were plugged into these financial networks. And so, it was kind of a natural extension of what North Korea was already doing. And when these different cyber-operations delve deeper into the world of cyber-crime, the world of crypto currency targeting, which again, it's very natural because their primary rivals, South Korea and Japan were quite early on the crypto currency game. So it was natural that North Korea would target that.

But yeah, then it becomes a natural extension of, since North Korea was already doing this kind of cyber-crime activity, what other kinds of cyber-crime could they get into, right. So bank heists, yeah, in the big scheme of things it's easy to see it slotting in with this money laundering capability and this well-developed espionage operational mindset, which lended itself very easily to these kind of deep, long-running bank heists like the ATP38 is known for.

And then by extension, you see an expansion in the kind of financially motivated activity that North Korea's now doing. So for example, just earlier this year we saw the first instances of web skimming that were linked to these UNC groups that were carrying out financially motivated operations. And that was something that we haven't seen before.

And then related to that, maybe this is me preempting another question, but it would not be a shocker to me if North Korea pivoted over to conducting ransomware. They already clearly have the capability, they've deployed it before, but mostly for disruptive of detraction, destructive reasons or to distract incident responders. But it would be really natural for North

Korea to go where the money is and ransomware is that thing now. They clearly have the capability to process that incoming revenue, they definitely need it given the continued sanctions. And it would be a very natural extension of the kind of things that North Korea's already doing.

Luke McNamara:

Yeah, that's a good point. And we'll definitely get into some of the stuff we've seen this year. I had forgotten about the web skimming activity, because that was the beginning of this year which now feels like an eternity ago.

Fred Plan:

Right.

Luke McNamara:

That feels so long... So I wanted to return to one of the points you were making. And this goes back to the sort of grouping, how we think about grouping different threat actors, particularly North Korea and looking at not just the malware families and the lineage of the malware, if you will, but looking at operationally how was it used, what are the TTPs around the spearfishing campaign, the infrastructure. What are some things when we look at that... And again, paint with very, very broad brush strokes because individual campaigns and even clusters can vary a lot. But one of the things I think we've seen a lot of, from a malware standpoint, with North Korean malware development is repurposing of a lot of code. In some ways makes it difficult to do some of these groupings and maybe in part why we have such sort of messy clustering in this space, in this industry with respect to North Korea. Talk about that a little bit.

Fred Plan:

Yeah, so that's a key characteristic of a lot of North Korean activity is this very widespread sharing of code. So there are certain tools that will have specific characteristics and for lack of a better way of explaining it, it's just widespread copy/pasting of this code. And then over time, you can track who copied which section of code from which malware at what times and how those have kind of branched out.

And so, initially, in the wild, early days of cyber espionage attribution, a lot of times when we saw code similarities or similarities in between two pieces of malware that look like a clear copy/paste, you could kind of assume, hey, here's two groups that are sharing resources. They're probably the same groups or it was the same code master or same programmer that built these tools. But then it became clear over time, especially as these tool evolved and they were being used in different ways, that these were not the same operations at all.

So a really good example would be groups like APT38 and the TEMP.Hermit espionage stuff. There's a lot of overlap in those tools, especially in the code that's included, but the way those tools are used and their role in the attack life cycle is completely different.

Another really good example would be WannaCry, which shared a lot... This was a worm that was pretty destructive. It looked like ransomware initially but was probably just a destructive worm. But the WannaCry shared code with a lot of espionage tools. And so on one hand that was a pretty, I don't want to say easy, but it was one of the indicators that WannaCry probably had North Korean origins, because of that code overlap, but it'd be different to say that because of that overlap WannaCry was being used by the exact same group that was carrying out espionage operations against say, US military or defense contractors in the US and the UK.

And so yeah, that's definitely created a lot of problems where there are different levels of public reporting that still kind of rely on that method, here's some malware similarities between these groups, so clearly they're all related. But we've gotten better. I'd like to think we've improved to the point, we've matured where we've become a lot more confident in how we split up these groups, not just based on the malware similarities but with the infrastructure that they're using or the specific TTPs that this specific group is using, and the targeting, and the timing of all of thee things, like the use of particular TTP or the use of particular tool at a specific time.

And then just to make things more complicated, so things have kind of branched off but then we see instances where things kind of go backwards. So a really good example of this would be, there's a tool which we call MonkeyCherry, right, which was linked to all the old TEMP.Hermit espionage stuff. And we said, "All right, so that's all over here." But very recently we saw this other North Korean group, which Kimsuki and we found them using that old tool and a very old version of it, but combining it with a much newer tool.

And so there's these instances of, or this overlap and then it becomes down to how does that square with how we've understood these groups have developed over time. And there's a lot of things that could explain it. It could be an organizational difference, here's one group and they like to use these tools. There's another group that uses these tools. Maybe one guy got reassigned from this group to another. Or it could just be practical, right. Ultimately, North Korea, again, it's not China-sized, it's not Russia-sized. It could just be one group needing a specific tool that has a particular function or capability and they just walked down the hall maybe and borrowed it from somebody else.

Luke McNamara:

It's the one thing with North Korean allies and North Korean cyber-operations, they always have to have in the back of your head is... And again, to kind of what we've been talking about is we have these assessments and understandings of how we assume certain types of North Korean behavior in a space like cyber-operations will look like, but because of how closed off

the country is, there are peculiarities in how they may assemble code or go about development that are very different then a Western context of how we would do that here.

You always, I think, are having to kind of balance against what the sort of current understanding of their operations and the nature of how they're going about doing things, but you're right, there's always a lot of explanations for why something that does not look incredibly practical or doesn't necessarily make sense to how we would consider other groups or other countries to operate in some of a similar manner.

Fred Plan:

Yeah. And another really good example to converting would be for say, China. China's also very prolific in cyberspace, but also China is... I don't know, this is going to be the weirdest analogy I've ever made, but it's a relatively understood country. There's Chinese scholars, there's Chinese websites that Westerners can publicly go to. You can go visit China and you can build this much bigger and wider understanding of what China is about in terms of not just a country, and it's history, and it's people but even for what we care about in the cyber-realm where we talk about what China's interests are as a state. What does the Chinese Communist Party have in mind in order to push forward it's goal and it's national priorities.

And that level of understanding is just completely lacking, or it's relatively harder to get when it comes to North Korea, right. We can't just go to North Korea and figure out what's going on. We can't just go to North Korea and have a better understanding of what the most pressing issues are with the regime and what the internal politics are like. And what are the struggles like within the Kim family? And what is Kim Jong Un thinking? They don't release the kind of... It's weird to say it in terms of an objective, strategic plan, or national priority, or national strategy in the same way China does. But yeah, relative to other countries, we just know a lot less about what's going on in North Korea.

And so, one thing that's unique about North Korea's cyber-operations, and this is kind of going full circle with what we had talked about earlier, is that if you consider North Korea to be this country that doesn't have many options left in terms of tools of statecraft. But it has this really powerful asymmetric cyber capability, right. So North Korea's in this position where they can use cyber-operations to affect other countries. But those same kind of operations will be relatively less effective against North Korea, right.

So North Korea has understood this to be this enormous asymmetrical advantage that they have in cyberspace. And they're definitely using it, right. I mean, they don't have any other options left. They can't conduct sanctions against another country. Their diplomatic relations effectively don't really exist in a way that's effective for them. But what North Korea does have is these cyber capabilities. They can directly go out and get money in a way that... I mean, it doesn't matter to them if it's allowed or not or it's legal or not, they just need it. Right. They can directly target summits or diplomatic meetings, including ones that they're not at the table for, right.

And so, in effect, the cyber-operations that North Korea's carrying out become kind of a window into what's going on in North Korea. They become our way of inferring and understanding the kind of priorities that North Korea has at that time.

So a really good example would be North Korea's recent shift to targeting the COVID-19 vaccine development effort, right. I mean, publicly North Korea is still saying they don't have any COVID-19 cases and of course their boarder with China shut down at the beginning of the pandemic. And yeah, publicly North Korea still continues to deny it but then at the same time, as of a couple months ago, North Korea shifted pretty much all of their cyber-operations to include looking at COVID-19 vaccine development, COVID-19 vaccine distribution. And you kind of wonder, why would they do that?

In the same way that earlier this year North Korea shifted over to targeting agricultural industry, which we previously had not seen them point their espionage operations against. So it gives us kind of a little window into what might be going on in terms of North Korea's priorities in a way that we might not be able to understand through other means, right.

It's because North Korea has this very one-dimensional capability, this is one of the few ways that North Korea has left to interact with the world. It is the one that North Korea has put a ton of investment into. And it's proven good results for North Korea to date, right. So what's the old saying, to the man who has a hammer, every problem looks like a nail. And that's exactly what it is for North Korea. Anything that concerns North Korea, it seems like cyber-operations is the way to go in terms of responding to it, in terms of addressing it. Because it's all that North Korea has left. It's the primary tool that they have.

And so when we see North Korea carrying out these operations the way they do against the countries that they do and against the different industries and verticals that they have been targeting, it's reflective of what's going on in the state, right.

I mean, going back, if we look at the timeline of things, North Korea's financially motivated activity really expanded and really blossomed, I guess, when we saw these sanctions first taking effect, right. When these sanctions really started hitting the inner circle, when they started becoming really pointed, that's when we saw APT38 carrying out the operations that they were.

We always saw the low-grade financially motivated activity, but the crypto-currency stuff, things like that, but to see that expand there's a strong correlation between the expansion of financially motivated activity and the prolonged effectiveness or pointedness of these sanctions against the Pyongyang regime. The same way it goes... I mean, there's the typical things that North Korea of course would be targeting, South Korea, the United States, defense, military, things like that. That is non-stop because that is a non-stop problem for North Korea. But when you see these things shift, I think it's really reflective of what's going on in the country. And North Korea's kind of, again, it's in this unique state that we believe the central regime has a lot of control over these different operations because of how they came about. But yeah, North

Korea's in this kind of unique position where they can tell, literally all of their groups, to do one thing and they'll all go and do it.

So if you think back to, was it... When we say this almost hard shift from widespread espionage operations targeting South Korea and the United States, especially the military and government, and we saw the hard shift... Was it 2017, 2018?

Luke McNamara:

2016, it may have been. Late, late 2016 maybe when it first started.

Fred Plan:

But you see this hard turn towards financially motivated activity. And all the groups did it. Pretty much every North Korean group that we saw did this. Even the ones that only targeted the military, even the ones that only targeted South Korea and the US, pretty much all of them in some way got involved in financially motivated targeting. And it was this hard shift that you just don't see with other countries.

Fred Plan:

Chinese groups, they wouldn't shift that hard. The Iranian groups wouldn't, the Russian groups wouldn't. But the North Korean groups, they did. They can and they did. And now you see that sort of same expansion where the really active North Korean groups that we're seeing now have then this other hard shift where Kimsuki activity and these UNCs that are related to TEMP.Hermit, which almost all really focus on defense and military targeting, geo-political targeting regarding the Korean peninsula, now they're targeting COVID stuff.

And it's just that level of authority that North Korea has over it's operations, is I think relatively unique to these North Korean groups. You can tell them to do something, even that's outside of their usual specialization or purview and they'll just shift and do it.

Luke McNamara:

And I think that's an interesting problem. Everything you've just described there is a great indicator of why North Korean cyber-espionage is a fantastic lagging indicator for North Korean analysts and watchers all over, in terms of getting that window into what are priorities for the regime and the government. From the standpoint of network defenders and organizations focused on it, who do I focus on, who within my threat model do I need to be most worried about?

This seems to be some of what is a challenge presented by these sort of operations. The last podcast we did was focused on Latin America. And we briefly brought up the example of the activity that we saw, I believe it was 38, maybe some TEMP.Hermit stuff as well. Again, as you

noted, a lot of them made a hard, fast pivot into financially motivated crime. But you had organizations throughout Latin America that never had to be concerned with or worry about and probably wasn't even on their radar, North Korean cyber-operators in different groups.

And so from this standpoint of where we've seen these fast shifts in targeting, sometimes accompanied by continued focus on their primary area of collection, kind of added this to their repertoire. Does that make it difficult for organizations that, again, the ones that want to focus on, all right, I've got limited resources, who are the top threat actors I should focus on based on the industry that I'm in, the region that I'm in? North Korea seems to break that mold a little bit.

Fred Plan:

A little bit, yeah. I mean, to some extent it still applies. If you're in South Korea or you're in the United States, you probably have a little bit more to worry about coming from North Korea than say Latin America. But yeah, there's those instances where you're not being targeted by North Korea until suddenly you are. And it just happens. And it's-

Luke McNamara:

And you don't have those indicators, as you noted, with other countries. We don't necessarily have the North Korea defense strategy that they come out with every year and they say, "Here are our top priorities. Here are the industries that we're focused on acquiring more technology from. And we're focused on building up internally." So you don't necessarily have those other indicators.

Fred Plan:

Yeah, and that makes it tough. And then, again, especially because of the nature of how North Korea, at least as we understand how it's politically structured, right. Ultimately it comes down to what's going on in Kim Jong Un's inner circle. And it's kind of this manifestation of what would a country look like if it was literally all subject to the whims of a specific individual. And North Korea is that. And it's as unpredictable because there's the lack of checks and balances and a stable political system that is predictable and well-understood by other countries. It just doesn't exist within North Korea. And then that makes it tougher for sure.

What's the answer from the network defender perspective? It's tough, man, it's tough. Because yeah, like we're saying, you're not targeted by North Korea until suddenly you are. But it comes down to the prioritization, right. So again, you can always condense it down to if you're doing business in Northeast Asia, if you're doing business in these regions or countries that historically have been targeted by North Korean operations, so Japan, South Korea, the United States, things like that. Or if you're in these industries of interest to North Korean operators like the defense industry or the financial industry. Then you can kind of compare and re-rank your priorities against what you believe to be the most likely threats.

But with the understanding that that can very quickly change. That can very rapidly evolve or devolve, depending on the whims of Kim Jong Un or whoever is calling the shots in North Korea at the time. So yeah, it's tough for sure and that is one of the things that sets North Korean operators apart from Chinese, Russian, or Iranian ones.

Luke McNamara:

Well that's a great segue way into my last question for you. And I think you started answering it a little bit when you brought up ransomware. I won't ask you to give any hard and fast predictions and hold you to them in terms of what we will see from what has historically been this very unpredictable set of threat actors. But for folks looking for potential indicators of where North Korean operations, be they espionage, destructive, or financially motivated, where they could go next from here from what we've seen this past year, what might be some guideposts to look out for?

Fred Plan:

Yeah, so one of the key ones, as I alluded to, is that expansion of financially motivated activity. So early this year we saw the first web skimming operations that we were able to link all the way back to North Korean operators.

So there's this shift towards increased financially motivated operations. And there was already a shift, but now that's gotten stronger and expansion of that financially motivated activity has taken place. So I think it would be very natural, if it isn't happening already, for those operations to expand to where the money is. And that's currently ransomware operations. Especially, given the world that we live in now.

I mean, the global economy in general is in bad shape. North Korea in particular is in probably really, really bad shape because their primary trading partner holds down the boarders first. And China has not been as close to North Korea, relatively speaking, as they historically have been. So surely that's impacted North Korea's financial situation.

In addition to that, there's this shift recently towards the agricultural industry and targeting, like I said, biotech, pharmaceuticals, things like that which we think is a response to a COVID-19 outbreak within North Korea. And so there's a good chance, I think, that that sort of health sector kind of targeting will be a bigger focus for these North Korean operations going forward, especially as we're just beginning to come to terms with what might be happening in North Korea. And they might be just coming to terms with what might be happening within their state. So that'll be something to watch out for.

The other kind of shift or trend with North Korean operators that we've seen this past year was a shift towards more using of social media in their operations. So doing things on LinkedIn, doing things via Skype or doing things via those sort of mediums in a way that we hadn't previously seen with North Korea.

Luke McNamara:

You're speaking specifically in the furtherance of cyber-espionage operations, right?

Fred Plan:

Yeah, yeah. Sorry. Yeah. So in terms of cyber-espionage operations. So this is kind of a shift in their TTPs from what we've previously seen.

We've certainly seen other countries doing this kind of thing, Iran for example or Russia, things like that. But North Korea has relatively recently gotten into that as well. And so we may see more development of their operations along that line.

Luke McNamara:

Yeah, that's an interesting one to point to. And again, you mentioned the case of Iran and how they've gone from utilizing that in cyber-espionage operations to increasingly what we witness and suspect to be sort of pro-Iranian disinformation campaigns, leveraging some of those same TTPs we saw initially used, right. Spoofing or pretending to be a journalist, setting up fake news websites.

Fred Plan:

The good old newscaster days.

Luke McNamara:

Good old newscaster, yes. This has all been tremendously interesting and I think both for individuals who are maybe familiar with some of historic activity around North Korean operations but then also some stuff that we've been seeing recently, I think a lot of people will find this of value. So we'll have to have you back on if any of these predictions come true.

Fred Plan:

I'll be on in 2021 and then we'll look back on it.

Luke McNamara:

Well as you noted, you left yourself a good bit of wiggle room by noting that they're very unpredictable set of actors. Who knows what we'll see from North Korea in the future. But, Fred, thanks again and take care.

Fred Plan:

For sure. Thanks a lot, Luke. Thanks for having me.