Eye on Security

The “Big Four”: Spotlight on North Korea

Transcript

Luke McNamara:

Welcome to another episode of the Eye on Security podcast.

Eye on Security 팟캐스트의 새로운 에피소드를 시작하겠습니다.

I'm your host, Luke McNamara.

저는 호스트인 Luke McNamara 입니다.

And joining me today, we have senior analyst on the cyber espionage team here at Mandiant, Fred Plan.

오늘 저와 함께 Mandiant 사이버 스파이 분석팀의 선임 애널리스트인 Fred Plan 와 함께 합니다.

Fred, how are you today.

안녕하세요, Fred. 반갑습니다.

Fred Plan:

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

안녕하세요. 초대해 주셔서 감사합니다.

Luke McNamara:

Definitely.

환영합니다.

So this'll be the first in a series that we're planning on doing.

앞으로도 자주 초대해서 모시게 될 텐데요.

Because I've now said that publicly, we're committed to this,

이제 공개적으로 청취자들에게 말씀드렸기 때문에 앞으로 자주 나와 주셔야 합니다.

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,

오늘 2021 년 첫 팟캐스트 에피소드로 시작으로 사이버 위협 그룹 중에 Big 4 라고 할 수 있는

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.

러시아, 이란, 중국, 북한이 있는데, 각각의 국가 차원의 공격 그룹에 대해 시리즈로 엮어서 하나씩 자세히 다뤄 볼까 합니다.

So who better than you to kickstart us here.

오늘은 북한에 대해 이야기를 자세히 나눠 보겠습니다.

Fred Plan:

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

네. 조선 민주주의 인민 공화국,

North Korea.

흔히 우리는 북한이라고 부르죠.

Luke McNamara:

That is the Korea that we are here to talk about, yes.

자, 그럼 이제 북한에 대해서 이야기를 시작해 보겠습니다.

I was thinking about this and we were talking about this a little bit beforehand of where do we actually start

어떤 이야기부터 시작을 하면 좋을지 시작하기 전에 잠시 이야기를 나눠봤고, 저도 나름대로 혼자 생각을 해봤었는데요.

if we're to talk through sort of North Korea's cyber capabilities,

북한의 사이버 공격 능력이나, 과거에서 최근까지 북한이 시도했던 공격 사례들,

what we've seen historically from North Korea and potentially some of the more recent activity,

또는 여러 기업이나 조직들에서는 북한의 사이버 공격을 어떻게 바라보고 있는 지,

but how organizations should think about North Korea and cyber operations.

이런 류의 이야기를 먼저 해 보면 어떻게 생각해 보았습니다.

But I guess for someone that's completely new to North Korean operations, to give us the cliff notes sort of history of what

청취자 중에 북한 공격 동향에 생소한 분이 있을 수도 있기 때문에

what we've seen from North Korea, what they've dabbled in when it's come to cyberspce activity, kick us off.

북한 공격 활동에 대해 우리가 알고 있는 내용을 간단히 알려드리면 어떨까 해요.

How would you frame that?

먼저 북한의 공격 특성을 어떻게 규정해 볼 수 있을까요?

Fred Plan:

Yeah. So that's a good question.

네, 제가 알고 이해하고 있는 내용을 설명해 드리겠습니다.

There's a lot of different ways to think about North Korea as a player in cyberspace.

사이버 공간 안에서 공격자로서의 북한 매우 다른 시각으로 각자 다르게 볼 수 있습니다.

But I always like to take it back to what the country fundamentally is about, right.

저는 근본적으로 먼저 그 국가 자체를 먼저 놓고 처한 상황을 고려해 볼 필요가 있다고 생각합니다.

North Korea, of course, is a relatively small nation state in Northeast Asia.

북한은 아시아 국가 중에서 상대적으로 작은 나라입니다.

Their primary geo-political concerns are vis-a-vis there relationships with their neighbors,

지리적으로 이웃 국가들로부터 받는 영향이 상당히 큰데요,

especially South Korea, China, Japan, as well as the allies of those countries.

특히 주변 국가 중에 한국, 중국 일본을 포함한 동맹국가들이 그 대상입니다.

So in the case of both South Korea and Japan, North Korea is extremely concerned with the United States.

한국과 일본의 경우도 마찬가지이지만, 북한은 미국과의 관계에 대해 매우 민감해 하고 있습니다.

Not going into too much detail,

지금 너무 자세하게 설명하지는 않겠지만,

but the other thing that North Korea's really known for is the level of control that the regime in Pyongyang

북한은 평양을 중심으로 펼치는 정권 세력이

has over pretty much all aspects of society, over the military, over the status of the country as a whole.

거의 모든 북한 사회를 포함해 군대, 국가 전체를 통제되고 있습니다.

So one thing to consider about North Korea, especially when looking at cyberspace is,

특히 사이버 공간에서의 북한을 볼 때에는 특정 지역을 포함하여 전 세계적으로 북한과의 관계가

how North Korea's relations, not just within the region but globally have steadily degraded over time.

어떻게 악화되어 왔는지를 알아야 합니다.

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,

그리고 북한의 사이버 공격이 양과 질적인 측면에서 지속적으로 증가하고 고도화될 수록

and how that is in contrast to how badly their relations with their neighbors have become.

주변 국가들과의 관계는 점점 악화되고 있어 부정적인 상관관계를 초래하는 것을 볼 수 있습니다.

And so North Korea's in this unusual position where here's a relatively small country that has steadily developed increasingly capable cyber operations

경제적인 제재나 외교 관계를 침식 시키면서도, 북한과 같이 작은 나라가

despite economic sanctions, despite steadily eroding diplomatic relations with it's neighbors.

꾸준히 사이버 공격 수준을 높여가는 것은 특이점으로 꼽을 수 있습니다.

But then at the same time, this is kind of the corner that the North Korea has painted itself into, right.

하지만, 이도 충분히 북한이 의도한 것으로 볼 수 있습니다.

So backing out a little bit. Trying to talk about the nation state example a little bit further,

일단 잠시 이 이야기는 뒤로 하고, 일반적인 국가들의 상황을 비교해서 들여다 보면,

The vast majority of nation states, of course, have different ways of relating to other countries

대부분의 국가들은 다양한 방법으로 다른 나라들과 교류하고,

or different tools of statecraft available to them, so diplomatic relations, economic ties, and things like that.

국정 운영이나, 외교 및 경제 활동도 마찬가지로 여러가지 방향으로 진행하고 있습니다.

North Korea is at the point where it doesn't have these things.

북한의 경우는 상황이 전혀 다르죠.

It's only remaining friend of significance, really, is China.

오직 중국만이 유일하게 북한과 친화적인 관계를 가지고 있는 나라입니다.

It's heavily burdened with economic sanctions,

경제 제재에 대한 부담이 큰데,

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.

북한의 군사력을 과시하는 연례 퍼레이드 행사만 빼면 사실상 눈에 띄는 국정 운영을 위한 별다른 방안은 보이지 않습니다.

And so North Korea just doesn't have many options left to it.

따라서 북한으로서는 선택의 여지가 그리 많지 않아요.

What the state does have however, is they've put a lot of investment into their cyber capabilities.

이 와중에 북한 정부는 사이버 기능에 많은 투자를 했습니다.

And this is kind of North Korea's only remaining tool of statecraft left.

그리고 이건 북한이 유일하게 가지고 있는 국가 차원의 주요 기능으로 볼 수 있죠.

And it has a huge impact on the kind of operations that we're seeing from the country.

이와 관련해서 북한이 행하는 일들을 보면 엄청난 영향을 미치고 있어요.

And conversely, I believe that it's reflective of the kind of concerns that North Korea has as a state.

또 반대로 해석하면, 북한이 우려하고 있는 부분을 알 수 있다고 생각해요.

Luke McNamara:

And that's one I think we'll definitely get into a little bit later, talking about some of the examples

좀 더 자세히 이야기를 나눠보면 좋을 것 같은데, 구체적인 사례를 들어서 말이죠.

that we've seen this year of North Korea and cyber-espionage in particular

사이버 스파이 활동 같이 올 해 북한이 벌인 사이버 위협 활동이나,

and what that potentially allows us in terms of a window into the things that are priority to the state, to the Kim regime.

김정은 정권이 우선순위로 꼽고 있는 것은 무엇으로 볼 수 있는지 말입니다.

One question I guess I have,

제가 궁금한 것은

when we think about the sort of expansion of activity, and North Korea would definitely be,

북한의 공격 활동이 늘어난 것을 보면,

I think fair to say, in the category of more emergent cyber-power in the last several years,

중국이나 러시아는 이미 강력한 사이버 공격력을 가지고 있었고,

five to seven years, than China or Russia that's been established for some time.

지난 5-7 년 동안 북한은 이들보다 더 활발히 활동하면서 새로운 신흥 주자로 떠올랐다고 볼 수 있죠.

Talk to us a little bit about I guess, what we used to see five, seven years ago

5-7 년 전은 어땠는지 좀 더 이야기 해 주세요.

from North Korean threat activity, in terms of the sort of regional focus.

좀 더 지역에 초점을 맞춘 북한의 위협 활동에 대해서요.

Wasn't a lot of it more focused around South Korea?

한국이 주로 타겟이 않았던가요?

You talk about this sort of regional, neighbors that it has different relationships or lack of relationships with.

서로 다른 관계를 가지고 있거나 교류가 부족한 나라나 이웃 국가들에 대해서 이야기 해 주세요.

A lot of that we've seen expand to different sectors and different industries,

다양한 분야와 산업으로 공격 활동이 확장되는 것을 보고 있죠.

but we've also seen expand away from where it originally began, in terms of South Korea.

그런데 한국의 입장에서도 들여다 볼 필요가 있을 것 같아요.

Fred Plan:

Yeah, for sure.

네, 맞습니다.

So as I mentioned, South Korea is absolutely North Korea's biggest concern.

앞에서 말했듯이, 한국의 절대적으로 북한의 가장 큰 관심사입니다.

They're right up there, they're the biggest rival regionally and in terms of everything that North Korea's trying to do.

지역적으로도 그렇고, 북한이 하려고 하는 모든 면에서 가장 큰 라이벌이죠.

And so the vast majority of the early cyber-operations that we observed were pointed from North Korea to South Korea.

그래서 우리가 관찰한 북한의 초기 사이버 공격의 대부분은 한국을 향하고 있었어요.

And this is kind of typical of what we see of emergent cyber-powers in general.

이건 우리가 일반적으로 볼 수 있는 신생되는 사이버 공격의 전형적인 형태입니다.

A lot of these started very basic, they were DDoS attacks, or website defacements, and things like that.

대부분 디도스(DDoS) 공격이나 웹사이트 침해 같은 베이직한 것들로 시작되요.

And these were, I mean they're comical now in comparison to what North Korea has grown to become.

지금 북한이 성장해 온 것에 비하면 이런 것들은 우습죠.

But yeah, these were really basic attacks, they were largely disruptive, almost all of them were pointed against South Korea,

하지만, 이런 기본적인 공격 활동들로 시작되었고, 거진 다 성공했어요.

different government offices, financial sector, Korean media, things like that.

그리고 여러 한국의 정부 기관, 금융 조직, 언론 등에서 거센 비난을 받았습니다.

And then over time these became progressively more complex, they became more capable,

그리고 시간이 흐르면서 이러한 것들은 점차적으로 더 복잡해졌고, 공격 기술이 고도화 되었고,

and North Korea gained more confidence in their ability to carry out these cyber-operations.

북한은 이런 사이버 작전을 수행할 수 있는 그들의 능력에 대해 더 큰 자신감을 갖게 되었어요.

Then the big coming out party for North Korea really was the Sony attack, right.

그 후, 소니(Sony) 영화사도 북한의 사이버 공격을 받게 되었죠.

At that point we had seen North Korea interested in targeting outside of the region.

그 당시 북한은 한국 이외의 다른 지역에 대한 공격도 노리고 있었어요.

They had targeted, for example, US forces that were in South Korea.

예를 들면, 한국에 주둔하고 있는 주한 미군이 표적이 되었습니다.

They had targeted other US government organizations, US military at that point.

미국 정부나, 미군 조직들도 공격 대상에 포함되었어요.

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.

그러다 거기서 그치지 않고 미국의 민간 기업을 공격하기 시작하면서 모든 사람의 주목을 끌게 된 거죠.

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.

북한은 기회를 놓치지 않았고, 스스로의 공격 능력을 전 세계에 보여주게 된 거죠.

And things have just ballooned from there.

그 후 그들의 공격은 점점 더 확대되어 가고 있습니다.

South Korea has become progressively more destructive,

한국은 점점 더 피해를 입게 되었고,

they have expanded their targeting beyond just South Korea and the United States.

북한은 한국, 미국에만 그치지 않고 공격 대상을 더 넓혀가고 있습니다.

They're activities have expanded beyond just espionage operations.

그들은 더 이상 첩보 활동에만 집중하고 있지 않아요.

Now they're doing a lot of financially motivated activity.

이제는 재정적 동기를 가진 공격을 활발히 시행하고 있습니다.

Their espionage operations now target a lot of other countries.

지금은 많은 수의 국가를 대상으로 스파이 활동을 벌이고 있죠.

So not just within Northeast Asia but also financial industry or financial institutions in Southeast Asia, in Latin America.

동북 아시아 뿐만 아니라, 동남 아시아, 남미 금융 산업이나 여러 금융 기관도 그들의 표적이 되고 있습니다.

And yeah, it's escalated very, very quickly from there and North Korea's now a global player

그들이 가진 사이버 능력이 없었다면 불가능했을 일들을 현재 굉장히 빠르게 확대하고 있으며,

in a way that it previously would not have been without this cyber capability.

이제는 빼 놓을 수 없는 세계적인 공격 능력을 보유한 국가가 되었습니다.

Luke McNamara:

Yes. And for sure, no longer an emergent player, but a player that has emerged into the space.

그렇군요, 이제는 더 이상 신생 공격자로 볼 수 없고, 전 세계를 대상으로 위협적인 존재가 되었네요.

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.

우리가 북한의 공격 그룹을 제대로 파악하지 못하면, 그들의 특성과 구조에 대해서는 논할 수 없을 것 같아요.

And that's always, I guess, the discussion about any of these different countries we talk about is

그리고 제가 보기에는 이런 국가들에 대한 정보들은 우리가 관심있게 지켜보고 있는 공격 그룹들의

the sort of nature of how organizations such as ours group threat actors and separate out kind of the different clusters of threat activity.

특성을 이해하고 공격 활동이 누구의 소행인지 식별하는 데 중요한 단서가 되는 거 같습니다.

And in the years have changed and morphed.

사이버 공격 활동을 바라보는 시각에 있어 여러 해 동안 많은 변화가 있었어요.

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.

우리가 추적하고 있는 주요 공격 그룹이나, 북한의 위협 활동, 관심 대상 등이 말입니다.

Fred Plan:

Yeah, I mean, so kind of getting back to what we were just talking about historically, how this has grown.

맞습니다. 우리가 과거에 얘기했던 것을 되짚어 보면, 지금은 어떻게 달라졌는지 알 수가 있어요.

I mean, again, North Korea's a relatively small country and it's central control is very strong.

다시 말하지만, 북한은 작은 나라이고 그들의 중앙 집권 체제는 매우 견고합니다.

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,

초기에는 북한 밖에서 일어나는 모든 사이버 공격 작전은 상호 연결되어 있다고 생각할 수 밖에 없었어요.

it was all a relatively small subset of activity that was interconnected.

모두 특정 활동에서 파생되어 서로 얽혀있는 활동들로 봤으니까요.

But over time it became very clear that there are multiple, distinct groups

그러나 시간이 지나면서 여러 다른 공격 그룹이 북한 내에 존재하고 있고,

that are operating out of North Korea and each of these groups have different specializations and different focuses.

북한 외부에서 작전을 수행하고, 다른 전문 분야와 목적을 가지고 있다는 것을 알 수 있었습니다.

So, yeah, just very quickly off the top so some of these groups are very focused on, for example, financially motivated operations.

예를 들면, 재정적인 목적을 가진 공격 그룹이라던가 말이죠.

APT38 is the best example of this I can give.

APT38 이 좋은 예가 될 수 있겠네요.

This is an operation that was very focused on carrying out longterm, extended deep dive bank heists against global targets.

전 세계 금융기관을 대상으로 장기간 계획하여 정교하게 공격을 가하고 있습니다.

And that's really the main focus of what APT38 does.

APT38 은 북한의 금융 전문 해커 조직이죠.

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.

사이버 스파이 활동같이 중요한 전략적 정보를 빼내는 류의 활동을 하는 여러 ATP 그룹들도 있어요.

So groups like that include APT37, as well as groups that are publicly referred to as Kimsuki is another one of these operations,

ATP37 나 잘 알려져 있는 김수키라는 그룹이 있고,

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.

여러 UNC 그룹이나, 공격 조직들이 서로 연결되어 활동하는 경우 TEMP.Hermit 으로 통칭하고 있습니다.

A lot of times the TEMP.Hermit ones especially, are called out publicly as Lazarus.

TEMP.Hermit 도 있지만 라자루스라고 불리는 그룹도 있어요.

Largely based on malware overlaps, linked all the way back to the Sony stuff.

서로 멀웨어를 공유해서 사용하고 있구요, 라자루스의 경우 소니 해킹 사건에도 연류되어 있어요.

But if you look at how those groups split up and the kind of activities that they're doing,

이 집단들이 어떻게 구분되고 어떤 활동들을 하는지를 보면,

it's pretty clear that there's multiple subsets of activity that are all doing different things.

각자 여러 하부 조직들을 양성하여 다양한 여러 활동들을 동시에 펼치고 있습니다.

Some espionage stuff, some financially motivated stuff, some of that activity is very focused on targeting the US military and defense sector for example.

한 그룹은 간첩 활동을 하고 또 다른 그룹은 재정적인 목적을 가진 공격을 진행한다던지, 또는 미군이나 국가 안보와 관련된 조직을 해킹 하는 등 말이죠.

Whereas, there's other UNCs that almost exclusively do financially motivated activity,

반면에, 재정적 이득을 취하기 위한 목적을 위해서만 움직이는 UNC 집단도 있는데,

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.

예를 들어, 최근 북한의 암호 화폐를 노린 공격이나 메이지카트나 웹 스키밍 공격이 증가하고 있습니다.

And then outside of those clusters that I've mentioned, the TEMP.Hermit stuff, the APT38 stuff, there's the Kimsuki espionage stuff.

이런 집단 외에도, 제가 말씀드린 바와 같이 TEMP.Hermit 이나 APT38, 또 김수키라는 조직들이 있죠.

There's another cluster that's kind of off to the side and that's the clusters that typically get reported as Andariel.

안다리엘(Andariel)이라고 불리는 또 다른 하부 조직이 있는데요,

And this is another espionage operator that we see going way back, very focused on the South Korea espionage campaigns early on.

사이버 첩보 활동을 하고 있는 조직으로, 이전에는 한국을 대상으로 첩보 활동을 주로 벌였어요.

And then over time those also started targeting more globally, especially against the United States.

그리고 시간이 흐르면서 이들은 특히 미국을 대상으로 하지만, 전 세계를 타겟으로 삼고 있습니다.

So there are several, I don't know if you want to call it mega-clusters, but I guess it depends on how...

이들을 거물급으로 볼 수도 있겠지만, 글쎄요, 어떻게 보느냐에 따라 관점이 다르겠지만,

What are your units of analysis, right?

분석에 사용되는 정보나 정보의 범위에 따라 다르겠죠?

What units of analysis, at the country level or at the operational level, or at the tactical level?

국가로 분류를 한다던지, 아니면 활동 수준을 관점으로 삼거나, 공격 기술 수준으로 볼 수도 있구요.

But for sure, these groups are distinct in their tool sets and how they do what they do and the targeting that they have.

하지만 분명한 건, 이들 공격 그룹들이 각자 가진 기술이나, 기법, 그리고 어떤 목적을 가지고 누구를 노리느냐에 따라 구분 지울 수 있습니다.

Again, North Korea's a relatively small country.

다시 말하지만, 북한은 작은 나라입니다.

There's a ton of sharing between these groups, especially in terms of malware.

북한의 공격 그룹들은 특히 멀웨어를 서로 주고 받으면서 공유하고 있어요.

There's a ton of overlap in terms of their targeting, especially against either South Korea or the United States.

공격이 한국이나 미국을 향하고 있다는 공통점도 가지고 있죠.

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.

특히 북한의 경우 각각의 공격 그룹을 뚜렷하게 식별해 내는 것은 매우 어려운 일입니다.

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.

네, 그래서 이번 팟캐스트 시리즈는 북한에 대한 이야기로 먼저 시작하고 싶었던 이유에요.

Because I think there's some interesting aspects of what makes attribution and the separation of different clusters somewhat difficult,

왜냐하면 북한의 공격 그룹이나 그들의 하위 집단들을 식별하기 어렵게 만드는 흥미로운 무언가가 있을 거라고 생각했구요,

and I think highlights how messy sometimes attribution can be.

이들의 특성들이 또 매우 복잡하게 얽혀 있을 거라고도 생각되었습니다.

Or rather, the difficulties of attribution with really messy clusters like what we see coming from the North Korean groups.

이것이 오히려 북한 공격 그룹이 가진 특성으로 볼 수도 있죠.

What I think, in particular I guess, two things to pull on a little bit more,

저는 두 가지 정도 더 자세히 들여다 봤으면 하는데요,

you mentioned the financially motivated activity that we see.

말씀하신 재정적인 목적을 가진 공격 그룹이 있었죠.

That's interesting to me, when we see...

좀 흥미로운 부분이 있는데요,

In some cases, you could make maybe the case for increasingly different types of, what historically we've thought of as cyber-espionage clusters

경우에 따라서는 사이버 첩보 활동만 주로 하던 공격 집단들이,

that have engaged in some activity that looks financially adjacent, shall we say.

금융 공격을 동시에 하게 경우도 있는데, 좀 더 다양하게 이들을 분류하여 정의해 볼 수가 있을 것 같습니다.

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

예를 들어, APT41 에 대해 분석된 내용과 이들의 재정적인 목적을 가진 공격을 접근하는 방식이나,

and kind of how we frame and think about that is different as we perceive them to kind of be contractors

우리가 정의하고 있는 내용을 볼 때, 일시적으로 가담하는 것이라고 인지하고 있는 것과 차이가 있습니다.

than how we frame groups from North Korea like TEMP.Hermit or APT38.

북한의 TEMP.Hermit 이나 ATP38 에 대한 정의도 다시 생각해 볼 수 있는 거죠.

Fred Plan:

Yeah.

네, 맞습니다.

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,

제 생각에는 처음에 지적하신 내용들로 돌아가 보면, 우리가 북한이라는 나라 자체를 놓고

to go back to some of your points at the very beginning about this.

어떻게 보는 지에 대해서도 영향을 미칠 거라고 봐요.

But maybe walk us through that a little bit of why kind of we've reached those analytic conclusions

다른 나라들과는 상황이 매우 다른데, 이들 공격 그룹을 재정적인 목적을 띄거나

in terms of the financially motivated or cyber-crime activity of some of these groups,

또 특정 사이버 범죄를 목적으로 움직이고 있다고

that it looks different than what we've seen from other countries.

정의를 내리게 되었는지 더 이야기 해 보면 좋을 것 같습니다.

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.

네, 언급하셨듯이, 최초에 이들의 공격이 어떻게 발생되었는 지를 분석하면서 일부 판단되는 부분이 있습니다.

So for example, in the case of APT41, which is just Chinese operation that conducts both the financially motivated cybercrime, as well as cyber-espionage.

예를 들면 금융 거래를 공격하면서 동시에 스파이 활동을 펼치는 중국의 공격 그룹인 ATP41 의 경우,

We believe that much of the cyber capability in China had kind of grew up on its own in a way.

중국의 사이버 능력은 그들의 방식으로 스스로 성장시켰다고 판단하고 있습니다.

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.

홍커라고 부르는 레드햇 해커와 같이 암흑에서 공격 그룹들을 매우 적극적으로 양성 시키고 있어요.

And APT41 is a natural extension of that.

APT41 도 그렇게 탄생되었죠.

Here's some guys who are doing financially motivated activity and then decided to become contractors

주로 재정적인 목적의 공격을 하면서, 외주를 받아 잠시 첩보 활동을 동시에 하다가,

and continue on with both types of activity, espionage and cyber-crime.

두 종류의 공격 활동을 자연스럽게 하게 되는 경우들이 많습니다.

Fred Plan:

North Korea's is really different because in North Korea everything is controlled by the state, right.

북한의 경우 모든 것이 중앙 통제되고 있기 때문에 상황이 좀 달라요.

You don't get to go online and become your own hacker in North Korea.

스스로 해커가 되고 싶다고 해서 될 수 있지 않습니다.

And so most of the capability developed because the central authority put some number of military units through training,

대다수가 북한 중앙 당국에서 선택된 후 훈련을 통해 만들어 졌어요.

they organized a pipeline effectively of specialized trainees would be carefully selected

북한 정부는 세밀하게 파이프라인을 계획하여,

based on their loyalty or their different skillsets, or how they performed in training.

충성도나 보유하고 있는 스킬셋, 훈련 때 보여 준 능력 등을 고려해서 신중하게 해커들을 선택합니다.

And they would be set up to be part of these specialized units that really were decided from the top on down.

그렇게 조직화된 여러 공격 집단이 만들어 지게 되는 거죠.

As you guys will now be the cyber special forces

특정 목적을 가지고 공격 활동을 하거나,

or you will be the specialized cyber units that will be carrying out the will of the regime,

북한의 정치 체제를 위한 활동을 한다던지, 또는 김정은 독재 체제나 정권의 계획을 실행시킨다던지,

you will be carrying out the will of the Kim family and Pyongyang in cyberspace.

각자 주어진 임무를 수행하는 공격 그룹의 일원으로 움직이게 됩니다.

And so it's a very top down sort of capability that was built up.

그리고 매우 탑다운 방식으로 양성되고 있습니다.

It comes down to the level of control that North Korean state has over the people.

북한 정부가 국민 개개인을 다 컨트롤 하고 있는 거죠.

Not everyone can access the internet, not everyone can access these sort of training or these skills.

북한 주민들 모두가 인터넷을 사용할 수 있는 것도 아니고, 모든 사람들이 자유롭게 이런 종류의 훈련을 받거나 기술을 배울 기회가 없습니다.

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,

북한과 관련된 거의 모든 공격 활동들은 모두 북한 군부와 연결되어 있습니다.

even when we find that they're linked to different cell companies in different countries, or they're operating in a way

다른 국가들의 기업을 타겟으로 공격하는 것 조차도 말이죠.

that it's clear that they're conducting cybercrime activity and making money, it's still ultimately for the North Korean state.

모든 사이버 범죄 행위나, 금전 탈취를 위한 금융 공격 조차도 다 북한 정부를 위한 일입니다.

It's still ultimately for the regime.

궁극적으로 여전히 북한 정권을 위해 모든 일이 행해지고,

And everything that these operations are doing are in the interests of the regime.

공격 활동에 있어 일어나는 모든 일들은 북한 정권의 이익을 위해 일어나는 것들입니다.

And again, that's very different from say, Chinese cyber-crime actors who are making money on the side for themselves

다시 말씀드리지만, 돈을 벌기 위한 수단으로 해킹을 하는 중국의 사이버 공격 그룹이나,

or Russian actors where there's very clearly espionage operators that are acting on behalf of the state

국가를 대신하여 첩보 활동을 벌이는 러시아 공격 그룹과는 분명한 차이가 있습니다.

but then there's this enormous body of different underground forums and crime groups and carters

국가를 대신하는 첩보 활동도 하고 있지만, 여러 언더그라운드 포럼, 범죄 집단이 있고,

and all this assorted cyber-crime activity that's completely beyond what the nation state would be actively supporting in Russia.

러시아 보다 북한 정부에서 다양한 목적을 띈 더 많은 공격 활동들을 지원하고 있습니다.

And so it's a very different structure and that's what shapes how these North Korean groups operate

북한의 공격 그룹은 구조적으로 매우 다른데, 어떤 방식으로 공격 활동을 진행하고,

and the way they relate to each other in terms of tool sharing and operational similarities,

공격 툴을 공유하는 방식이나 공격 활동의 유사점 등이 각각의 공격 그룹의 정체성을 형성하고 있습니다.

but also in terms of what they're pointed against in terms of North Korean problem sets, right.

또한 북한이 가진 문제점들도 투영되어 고려되야 합니다.

So what are the things... Maybe this is going to be me preempting your question...

제가 미리 질문에 앞서 답을 하는 걸 지도 모르겠지만,

But it's the case where a lot of these North Korean groups, you could kind of see them as a proxy for the things that,

많은 북한 공격 그룹들이 일종의 프록시 역할을 하는 경우가 있는데,

you can see their operations as a proxy for the things that are most concerning to North Korea's interests at that moment.

활동 당시에 북한의 가장 큰 관심사에 따라 공격 활동이 이루어 진다는 것입니다.

Luke McNamara:

Well, I guess this is a preempting of my question.

제가 하려고 했던 질문은 말이죠.

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,

그런 관점에서, 북한이 결국 점점 더 해를 거듭할 수록 보다 많은 기술들로 무장하여

which as you noted has become more capable over the years,

공격력이 강해지는 것은 당연한 것으로 볼 수도 있는 가였습니다.

they've dabbled in a little bit of everything, the disruptive activity, the espionage,

침해나 스파이 활동 등을 조금씩 가리지 하고 닥치는 대로 시도해 오고 있고,

but they now have this resource that, particularly against the backdrop of over the years increasing sanctions...

점점 더 제재를 강화시키면서도 이런 인력들을 양성하고 있습니다.

And then you think about the other thing that in Opensource, they're well documented and known for

그리고 기록이 잘 되어 있고 알려진 오픈소스들로

is having extensive operations related to money laundering and counterfeiting currency.

돈세탁이나 화폐 위조와 관련된 공격 활동에 대해서도 많이 사용되고 있습니다.

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,

어쩌면 암호화폐와 같이 그들이 이득을 취할 수 있는 것은 북한의 입장에서는 당연하게 목표물로 삼아 공격을 벌이는 거죠.

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,

초기에 보안의 틈이 있었던 한국의 거래소를 공격의 목표물로 삼은

to what we've seen in terms of the big bank heists that we've seen with respect to APT38?

APT38 그룹의 은행 해킹과 같은 사건들은 피하기 어려웠을 겁니다.

Is that somewhat of an inevitability when looking back on that?

이러한 상황들은 불가피할 수 밖에 없었을 겁니다.

Fred Plan:

Yeah. Was it inevitable?

네, 그랬겠죠?

I don't know if you can say that, but for sure it was the path of least resistance.

이렇게 표현을 해도 되는지 모르겠지만, 그건 그들만의 힘을 가지기 위한 최소한의 방법이었을 거에요.

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.

북한은 이미 위조 의약품이나 필로폰을 제조하는 기술을 가지고 있고, 이를 가지고 돈세탁도 일삼고 있습니다.

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.

궁극적으로 북한은 여전히 한 나라이기 때문에, 하나의 국가로써 할 수 있는 많은 일들이 많습니다.

They had this capability when they were plugged into these financial networks.

금융 네트워크를 활용하여 돈세탁을 하고 있는데,

And so, it was kind of a natural extension of what North Korea was already doing.

이건 이미 북한이 벌이고 있는 악의적인 행위들로부터 자연스러운 확장하는 형태라고 볼 수 있습니다.

And when these different cyber-operations delve deeper into the world of cybercrime,

그리고, 다양한 공격 활동을 벌려 그들의 사이버 범죄 활동을 더 활발히 전개하면서,

the world of crypto currency targeting, which again, it's very natural

자연스럽게 암호화폐에도 발을 들이게 될 수 밖에 없었는데,

because their primary rivals, South Korea and Japan were quite early on the crypto currency game.

그 이유로는 주요 경쟁국인 한국과 일본이 암호화폐 시장에 꽤 선두주자로 있기 때문입니다.

So it was natural that North Korea would target that.

북한이 그걸 목표물로 삼는 건 매우 자연스러운 일인거죠.

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.

북한은 이미 이런 사이버 범죄 활동을 하고 있었기 때문에 또 다른 종류의 사이버 범죄로 이어질 수 있었던 것은 당연한 일입니다.

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.

자금 세탁을 할 수 있는 능력과 숙련된 첩보 활동을 기반으로 ATP38 과 같은 공격 그룹이 장기간 동안 금융 공격을 쉽게 지속할 수 있었습니다.

And then by extension, you see an expansion in the kind of financially motivated activity that North Korea's now doing.

그리고 그 연장선상에서 북한은 현재 금전 탈취를 목적으로 한 다양한 공격 활동으로 확장되고 있는 걸 볼 수 있죠.

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.

예를 들면, 바로 올해 초, 우리는 금전 탈취를 목적으로 하는 UNC 그룹들의 웹 스키밍의 사건이 있었는데요.

And that was something that we haven't seen before.

이건 이전에 한번도 보지 못했던 최초 사례였어요.

And then related to that, maybe this is me preempting another question,

이와 관련해서, 또 다른 궁금증이 있을 수 있는데요,

but it would not be a shocker to me if North Korea pivoted over to conducting ransomware.

북한이 랜섬웨어 공격 쪽으로 방향을 틀었다고 해도 별로 놀라운 일은 아니에요.

They already clearly have the capability, they've deployed it before,

명백히 그들은 이미 그럴 능력이 충분이 확보되어 있고, 경험도 있죠.

but mostly for disruptive of detraction, destructive reasons or to distract incident responders.

하지만 대부분은 공격 대상의 주의를 다른 곳으로 돌리기 위한 목적으로 사용되었습니다.

But it would be really natural for North Korea to go where the money is and ransomware is that thing now.

지금은 금전 갈취를 위한 용도로도 충분히 사용할 수 있을 겁니다.

They clearly have the capability to process that incoming revenue,

공격으로 갈취한 자금을 현금화하기 위한 처리 능력이 있고,

they definitely need it given the continued sanctions.

현재 지속되는 제재 상황을 고려할 때 공격을 지속할 수 밖에 없을 거에요.

And it would be a very natural extension of the kind of things that North Korea's already doing.

그리고 그런 공격들은 현재 진행 중인 활동들에서 좀 더 고도화하거나 발전시켜 확장하는 형태가 될 것입니다.

Luke McNamara:

Yeah, that's a good point.

네, 좋은 지적이에요.

And we'll definitely get into some of the stuff we've seen this year.

올해 일어난 일들을 몇가지 짚어보도록 하죠.

I had forgotten about the web skimming activity,

저는 웹 스키밍 공격을 잠시 잊고 있었던 것 같네요.

because that was the beginning of this year which now feels like an eternity ago.

올해 초에 일어난 일이기도 하고, 지금은 매우 옛날 일처럼 느껴지기도 하거든요.

Fred Plan:

Right.

맞습니다.

Luke McNamara:

That feels so long...

너무 길게 느껴지는데,

So I wanted to return to one of the points you were making.

그래서 저는 말씀하신 것 중에 한가지 포인트로 되돌아가서 더 이야기를 나누고 싶습니다.

And this goes back to the sort of grouping,

어떻게 공격 그룹을 구분하는 가인데,

how we think about grouping different threat actors, particularly North Korea

특히 북한의 경우 여러 공격 그룹을 어떻게 분류해 볼 수 있을까 입니다.

and looking at not just the malware families and the lineage of the malware,

멀웨어 패밀리와 멀웨어의 기원을 또 한번 살펴 보고,

if you will, but looking at operationally how was it used, what are the TTPs around the spearfishing campaign, the infrastructure.

이걸 공격에 어떻게 사용했는지, 스피어피싱 공격이나 공격 인프라는 어떤지에 대해서도 궁금합니다.

What are some things when we look at that...

이걸 이야기 할 때에는요,

And again, paint with very, very broad brush strokes because individual campaigns and even clusters can vary a lot.

공격 활동들 각각은 매우 특징적으로 다르기 때문에 큼 범위에서 이야기를 하면 좋을 것 같구요,

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.

멀웨어 측면에서 생각해 보면, 북한의 경우 멀웨어 코드를 다른 여러가지의 목적으로 다시 재사용 하는 경우가 많았습니다.

In some ways makes it difficult to do some of these groupings

어떤 면에서는 공격 그룹을 분류하기가 까다롭고

and maybe in part why we have such sort of messy clustering in this space, in this industry with respect to North Korea.

또 어떤 면에서는 북한 공격 그룹이 복잡해 보이는 것도 이 때문일 수 있을 것 같습니다.

Talk about that a little bit.

이거에 대해서 조금 이야기해 보시죠.

Fred Plan:

Yeah, so that's a key characteristic of a lot of North Korean activity is this very widespread sharing of code.

네, 코드를 널리 공유해서 사용하는 것이 북한 공격 활동의 매우 중요한 핵심 특징입니다.

So there are certain tools that will have specific characteristics

특정 기능을 하는 툴을 사용하구요,

and for lack of a better way of explaining it, it's just widespread copy/pasting of this code.

다르게 표현할 방법이 없는데, 그냥 복사해서 붙여넣기 식으로 코드를 사용하는 거에요.

And then over time, you can track who copied which section of code from which malware at what times

그리고 시간이 지남에 따라, 어떤 악성코드의 어떤 부분을 언제 카피해서 사용했는지,

and how those have kind of branched out.

어떻게 파생시켜 사용했는지 등을 추적해 볼 수 있습니다.

And so, initially, in the wild, early days of cyber espionage attribution,

초기 사이버 스파이 공격의 특징들을 보면,

a lot of times when we saw code similarities or similarities in between two pieces of malware

다른 멀웨어에서 코드의 유사점들을 발견할 수가 있었는데,

that look like a clear copy/paste, you could kind of assume, hey, here's two groups that are sharing resources.

명확하게 복사하고 붙여넣은 것처럼 보였고, 여기서는 두 개의 다른 그룹에서 코드를 공유해서 사용한다고 의심할 수도 있습니다.

They're probably the same groups

아마도 같은 그룹일 수도 있구요,

or it was the same code master or same programmer that built these tools.

코드 마스터가 같거나, 동일한 프로그래머가 툴을 만들었을 수도 있죠.

But then it became clear over time, especially as these tool evolved and they were being used in different ways,

시간이 지나서 보면, 이런 공격 툴이 변화되고, 다른 방식으로 사용되는 걸 보면서

that these were not the same operations at all.

전혀 다른 공격 활동이었다는 걸 알 수가 있었습니다.

So a really good example would be groups like APT38 and the TEMP.Hermit espionage stuff.

APT38 과 TEMP.Hermit 이 좋은 예시입니다.

There's a lot of overlap in those tools, especially in the code that's included,

특히 사용된 코드를 보면 이들의 공격 툴들은 중복되는 점들이 매우 많습니다.

but the way those tools are used and their role in the attack life cycle is completely different.

그렇지만, 각자 툴을 사용하는 방식이나, 공격 라이프사이클 내 수행 방식이 전혀 다르거든요.

Another really good example would be WannaCry, which shared a lot...

또 다른 좋은 예시로는 많이 알려진 워너크라이(WannaCry)입니다.

This was a worm that was pretty destructive.

꽤 파괴력이 높았던 웜(worm)이었습니다.

It looked like ransomware initially but was probably just a destructive worm.

처음에는 랜섬웨어처럼 보이긴 했지만, 아마도 그냥 파괴성이 높았던 웜이었을 겁니다,

But the WannaCry shared code with a lot of espionage tools.

워너크라이는 많은 스파이 공격 툴과 코드를 공유되었습니다.

And so on one hand that was a pretty, I don't want to say easy,

그리고 한편으로는 쉽게 단정짓고 싶지 않지만,

but it was one of the indicators that WannaCry probably had North Korean origins, because of that code overlap,

북한이 출처일 거라는 단서가 있었는데, 그게 바로 중복 사용된 코드 때문이었습니다.

but it'd be different to say that because of that overlap WannaCry was being used by the exact same group

하지만, 워너크라이와 중복되는 코드가 있는 툴을 사용했다고 해서,

that was carrying out espionage operations against say, US military or defense contractors in the US and the UK.

예를 들어, 미군이나 미국 또는 영국의 방위 업체를 대상으로 스파이 공격을 행한 그룹이 동일하다고는 볼 수 없을 겁니다.

And so yeah, that's definitely created a lot of problems

명백하게 이건 많은 오해의 소지가 있는데,

where there are different levels of public reporting that still kind of rely on that method,

여전히 많은 리포트에서는 멀워어에 유사점이 있으니,

here's some malware similarities between these groups, so clearly they're all related.

명백히 연관성이 있다는 식으로 분석하고 있는 리포트가 아직 많습니다.

But we've gotten better.

그렇지만, 점차 개선이 되고 있는 상황입니다.

I'd like to think we've improved to the point, we've matured

지금은 좀 더 개선된 방법으로 분석되고 있다고 생각하고 있구요,

where we've become a lot more confident in how we split up these groups,

여러 공격 그룹들을 구분해서 분리하는 방법도 보다 정확해 졌습니다.

not just based on the malware similarities but with the infrastructure that they're using

멀웨어 유사점에만 초점을 두지 않고, 공격 그룹이 사용하는 인프라나

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.

TTP 특징, 공격 대상, 특정 툴의 사용 시기 등의 정보를 기반으로 분석하고 있습니다.

And then just to make things more complicated,

좀 더 상황이 복잡하지는 경우가 있는데요,

so things have kind of branched off but then we see instances where things kind of go backwards.

여러가지 요소들이 파생되어 원점으로 되돌아 가서 생각해 봐야 되는 경우가 있습니다.

So a really good example of this would be,

여기에 대한 좋은 예시가 있는데요,

there's a tool which we call MonkeyCherry, right,

몽키 체리(MonkeyCherry)라고 부르는 도구가 있었는데,

which was linked to all the old TEMP.Hermit espionage stuff. And we said, "All right, so that's all over here."

예전 TEMP.Hermit 와 연관성이 있었고, 다른 가능성에 대해서는 검토해 보지 않았죠.

But very recently we saw this other North Korean group,

그러나 아주 최근에 새로운 북한 그룹이 있었는데,

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.

김수키라는 조직이었고, 아주 오래된 툴의 옛날 버전을 최신 공격 툴과 결합해서 사용한 걸 발견했습니다.

And so there's these instances of, or this overlap

이런 유사한 사례들은 여럿 있었고,

and then it becomes down to how does that square with how we've understood these groups have developed over time.

시간이 지남에 따라 이런 공격 그룹들이 어떻게 발전해 왔는지에 대해 파악해 봐야 합니다.

And there's a lot of things that could explain it.

그리고 이걸 설명할 수 있는 방법은 여러가지가 있습니다.

It could be an organizational difference,

조직의 특성에 대한 부분일 수도 있구요,

here's one group and they like to use these tools.

어떤 공격 그룹은 특정 공격 툴을 주로 사용하고,

There's another group that uses these tools. Maybe one guy got reassigned from this group to another.

또 다른 그룹이 같은 툴을 사용하는 경우에, 이전 그룹에서 다른 그룹으로 재배치가 되었을 수 있는 거죠.

Or it could just be practical, right.

아니면 그냥 단순히 실용적이라 같은 툴을 사용하게 되는 경우일 수도 있고요.

Ultimately, North Korea, again, it's not China-sized, it's not Russia-sized.

궁극적으로, 북한은, 다시 말하지만, 중국이나 러시아와 규모 면에서 전혀 다릅니다.

It could just be one group needing a specific tool that has a particular function or capability

그냥 단순히 한 공격 그룹에서 특정 툴을 사용하는 것은 그 툴의 기능이나 특징 때문에 사용할 수도 있고,

and they just walked down the hall maybe and borrowed it from somebody else.

단순히 다른 사람한테서 빌려서 사용할 수도 있습니다.

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...

북한의 동맹국들과 북한의 사이버 작전에 대해 항상 기억하고 있어야 할 것이 있습니다.

And again, to kind of what we've been talking about is we have these assessments and understandings of

특정 북한 공격 그룹의 특성을 잘 파악하고 이해하고 있으므로서,

how we assume certain types of North Korean behavior in a space like cyber-operations will look like,

사이버 공간에서 이들이 행하는 공격 활동들을 예측해 볼 수 있어야 하는 것입니다.

but because of how closed off the country is, there are peculiarities in how they may assemble code

북한이 패쇄적인 나라이기 때문에, 서양 문화권과 비교했을 때,

or go about development that are very different then a Western context of how we would do that here.

코드를 조합하는 방식이나, 발전시키는 방법이 다르고, 매우 특이해 보일 수 있습니다.

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,

항상 북한 공격에 대한 현황을 이해하고 그들의 활동 방식을 고려해 종합적으로 판단할 수 있어야 합니다.

but you're right, there's always a lot of explanations for why something that does not look incredibly practical

하지만 말씀하신대로 매우 현실적으로 보이지 않는 특정 사건이나, 다른 공격 그룹이나 국가들이

or doesn't necessarily make sense to how we would consider other groups or other countries to operate in some of a similar manner.

이들과 유사한 방식으로 진행하는 공격 활동에 대해서 다양하게 해석될 수 있습니다.

Fred Plan:

Yeah. And another really good example to converting would be for say, China.

네, 중국을 또 좋은 예시로 들 수가 있어요.

China's also very prolific in cyberspace,

중국도 사이버 상에서 매우 활발한 활동을 하는 집단이지만,

but also China is... I don't know, this is going to be the weirdest analogy I've ever made,

중국은, 글쎄요, 지금까지 제가 했던 비유들 중에 가장 이상할 수도 있을 것 같아요.

but it's a relatively understood country.

하지만, 비교적 파악하기 쉬운 나라입니다.

There's Chinese scholars, there's Chinese websites that Westerners can publicly go to.

중국 학자들도 있고, 서양권에서 정상적으로 방문할 수 있는 웹사이트도 있습니다.

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

중국을 방문할 수도 있고, 국가 차원에서 뿐 역사와 사람들에 대해서도 좀 더 폭 넓게 파악할 수 있습니다.

but even for what we care about in the cyber-realm where we talk about what China's interests are as a state.

또한 중국 공산주의 정당이 추구하는 이익을 실현시키기 위한 어떤 목표를 가지고 있는지에 대해서도

What does the Chinese Communist Party have in mind in order to push forward it's goal and it's national priorities.

어떤 목표를 가지고 있는지에 대해서도 사이버 공간을 통해 알아낼 수가 있죠.

And that level of understanding is just completely lacking, or it's relatively harder to get when it comes to North Korea, right.

북한이 경우에는 이런 수준의 정보를 얻기도 쉽지가 않습니다.

We can't just go to North Korea and figure out what's going on.

쉽게 북한을 갈 수도 없고, 무슨 일이 일어나는 지 볼 수도 없어요.

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.

북한 정권의 최대 관심사나 정치 구조를 알아보러 북한에 가 볼 수도 없죠.

And what are the struggles like within the Kim family? And what is Kim Jong Un thinking?

지금 김정은 정권의 가장 시급한 현안이 무엇인지, 지금 무슨 생각을 하고 있는 지 등,

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.

대게 중국이 가지고 있는 전략적인 계획이나, 목표, 국가적 우선순위 등은 북한에서는 볼 수 없어요.

But yeah, relative to other countries, we just know a lot less about what's going on in North Korea.

다른 나라들에 비해, 북한에 대해 파악하는 일은 상대적으로 어렵습니다.

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,

북한의 사이버 공격에서는 특이점이 하나 있는데요, 좀 전에 이야기 한 내용을 충분히 설명해 줄 것 같습니다.

is that if you consider North Korea to be this country that doesn't have many options left in terms of tools of statecraft.

북한이 국가 경영을 위해 할 수 있는 일이 거의 없이, 선택권이 많지 않은 상태에

But it has this really powerful asymmetric cyber capability, right.

비교적 매우 강력한 사이버 공격 기술을 보유하고 있다고 생각해 보세요.

So North Korea's in this position where they can use cyber-operations to affect other countries.

북한은 사이버 기술을 이용해 다른 나라들에게 영향을 충분히 줄 수가 있습니다.

But those same kind of operations will be relatively less effective against North Korea, right.

하지만 반대로 북한을 대상으로는 그리 효과적이지 않을 것입니다.

So North Korea has understood this to be this enormous asymmetrical advantage that they have in cyberspace.

따라서 이는 북한의 입장에서는 상대적으로 큰 이점을 가지고 있다고 볼 수 있어요.

And they're definitely using it, right. I mean, they don't have any other options left.

그래서, 달리 방법이 없기 때문에 이런 상황을 적극적으로 활용을 하게 되는 것이죠.

They can't conduct sanctions against another country.

북한은 다른 나라를 대상으로 제재를 가할 수 있는 입장이 아닙니다.

Their diplomatic relations effectively don't really exist in a way that's effective for them.

북한의 이익에 부합하는 외교관계는 사실상 존재하기 힘듭니다.

But what North Korea does have is these cyber capabilities. They can directly go out and get money in a way that...

따라서 보유하고 있는 사이버 기술로 직접적으로 자금을 확보하는 길을 모색하는 것이구요,

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.

합법적인지 불법적인지는 더 이상 북한의 입장에서는 중요하지 않습니다.

They can directly target summits or diplomatic meetings, including ones that they're not at the table for, right.

정상회담이나 외교 미팅을 가리지 않고 원하는 목표를 대상으로 공격을 가할 수 있습니다.

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.

사실상, 이러한 북한의 공격을 통해 북한에서 일어나고 있는 일들을 짐작할 수 있게 하는 수단이 되기도 합니다.

They become our way of inferring and understanding the kind of priorities that North Korea has at that time.

우리의 입장에서는 공격 사건 당시 북한이 가지고 있는 국가 차원의 우선순위를 유추해 볼 수 있게 됩니다.

So a really good example would be North Korea's recent shift to targeting the COVID-19 vaccine development effort, right.

그래서 이에 대한 또 좋은 예로 최근 북한이 COVID-19 백신을 목표로 삼는 걸 보면요,

I mean, publicly North Korea is still saying they don't have any COVID-19 cases

중국간 국경은 코로나 팬데믹 초기 당시 이미 폐쇄가 되기도 했지만

and of course their boarder with China shut down at the beginning of the pandemic.

공개적으로 북한은 코로나 감염자가 없다고 발표했잖아요.

And yeah, publicly North Korea still continues to deny it but then at the same time,

여전히 코로나 감염 사례는 없다고 부인하고 있지만,

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.

북한의 대부분의 사이버 공격 활동은 코로나 백신 개발과 보급으로 초점이 맞춰져 있습니다.

And you kind of wonder, why would they do that?

이유가 무엇인지 짐작이 가시죠?

In the same way that earlier this year North Korea shifted over to targeting agricultural industry,

올해 초 북한이 농식품 산업으로 공격 활동을 전환한 것과 같은 방식으로,

which we previously had not seen them point their espionage operations against.

북한의 공격 활동이 각기 다른 방향으로 진행되는 경우는 없었습니다.

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.

따라서, 이런 공격 패턴으로 인해 북한에서 염두에 두고 진행하는 우선순위의 일들이 무엇인지를 짐작해 볼 수 있는 계기가 되고 있는 것입니다.

It's because North Korea has this very one-dimensional capability,

북한을 매우 1 차원적으로 볼 수도 있고,

this is one of the few ways that North Korea has left to interact with the world.

이렇게 다른 나라들과 교류하는 몇 안 되는 교류 방식이기 때문입니다.

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.

북한이 이에 엄청난 투자를 하기도 했고, 또 원하는 결과를 내기도 했죠.

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.

북한의 입장에서는 문제를 해결하는 수단으로 볼 수 있고, 그들만의 방식인 거죠.

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.

북한은 어떤 문제가 있을 때 마다, 사이버 공격을 수단으로 대응하여 해결하려고 하는 것 같습니다.

Because it's all that North Korea has left. It's the primary tool that they have.

달리 방법이 없어서 일 수도 있고, 그들 입장에서의 해결하기 위한 중요한 수단이기 때문이죠.

And so when we see North Korea carrying out these operations the way they do

북한의 사이버 공격을 보면,

against the countries that they do and against the different industries and verticals

표적하는 국가나 산업들을 살펴보면,

that they have been targeting, it's reflective of what's going on in the state, right.

북한에서 어떤 일이 일어나고 있는 지를 짐작하게 됩니다.

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,

다시 뒤돌아 보면, 북한의 금융 공격이 확대되고 활발했던 시점에

when we saw these sanctions first taking effect, right.

대북제재가 처음 발표되었어요.

When these sanctions really started hitting the inner circle, when they started becoming really pointed,

대북제재가 실제 시작되고, 이를 매우 민감하게 받아들였는데,

that's when we saw APT38 carrying out the operations that they were.

그 당시 APT38 의 공격이 일어났었죠.

We always saw the low-grade financially motivated activity, but the crypto-currency stuff, things like that,

늘 보아오던 금융 공격 활동이 최근 암호화폐도 타겟으로 삼고 있는데,

but to see that expand there's a strong correlation between the expansion of financially motivated activity

이러한 북한의 금융 공격의 확대는, 대북 제재 이후 북한 정권의 대응 방식과

and the prolonged effectiveness or pointedness of these sanctions against the Pyongyang regime.

매우 큰 상관관계가 있는 것으로 해석됩니다.

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.

한국이나, 미국, 군사 조직 등의 일반적인 북한의 공격 타겟도 같은 방식으로 진행하고 있습니다.

That is non-stop because that is a non-stop problem for North Korea.

북한의 입장에서는 영원한 문제이기 때문입니다.

But when you see these things shift, I think it's really reflective of what's going on in the country.

하지만 상황이 변할 때에는 반듯이 북한 내 변화가 있기 때문으로 볼 수가 있어요.

And North Korea's kind of, again, it's in this unique state

아시겠지만, 북한은 일반적인 나라들과 상황이 많이 다르고,

that we believe the central regime has a lot of control over these different operations because of how they came about.

북한의 중앙 정권이 사이버 공격도 전부 통제하고 있을 것으로 보고 있습니다.

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.

이러한 북한 특성으로 보아, 공격 집단은 위에서 시키는 대로 무조건 할 수 밖에 없을 겁니다.

So if you think back to, was it...

과거에 어떤 사례가 하나 있었는데요,

When we say this almost hard shift from widespread espionage operations targeting South Korea and the United States,

한국이나 미국으로 향한 북한의 공격 목표가 쉽게 변할 수 없을 건데,

especially the military and government, and we saw the hard shift...

특히 군사 조직이나, 정부 기관을 대상으로 하는 첩보 활동 들인데요,

Was it 2017, 2018?

2017 년인가, 2018 년인가 일어났을 거에요.

Luke McNamara:

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

2016 년인 것 같아요. 2016 년 말에 아마 처음 시작되었을 걸요.

Fred Plan:

But you see this hard turn towards financially motivated activity.

북한은 금전 탈취를 목적으로 하는 공격은 쉽게 그만두지 못할 것인데,

And all the groups did it. Pretty much every North Korean group that we saw did this.

모든 북한의 공격 그룹이 이 때 동시에 움직였던 사건인데,

Even the ones that only targeted the military, even the ones that only targeted South Korea and the US,

군사 조직, 한국, 미국을 공격하던 그룹들 조차

pretty much all of them in some way got involved in financially motivated targeting.

모든 그룹이 금융 공격을 같이 진행했습니다.

And it was this hard shift that you just don't see with other countries.

이건 다른 나라에서는 볼 수 없는 사례죠.

Fred Plan:

Chinese groups, they wouldn't shift that hard.

중국의 공격 그룹도 그렇지는 않아요.

The Iranian groups wouldn't, the Russian groups wouldn't.

이란이나 러시아도 마찬가지죠.

But the North Korean groups, they did. They can and they did.

북한에서만 볼 수 있는 특징이죠.

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

이런 유사한 상황을 지금도 북한 공격 그룹에서 볼 수가 있는데요,

where Kimsuki activity and these UNCs that are related to TEMP.Hermit,

김수키나, TEMP.Hermit 과 관련된 UNC 그룹이

which almost all really focus on defense and military targeting, geo-political targeting regarding the Korean peninsula,

거의 군사 및 정치를 포함한 한국의 정세에 대한 정보를 빼내기 위한 해킹 활동을 했는데,

now they're targeting COVID stuff.

최근에는 코로나 관련 공격을 시도하고 있습니다.

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.

정부가 이런 공격 활동을 통제하고 있는 경우는 북한을 제외하고는 볼 수가 없습니다.

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.

주로 전문적으로 활동하는 분야에서 정부에서 시키면 그만두고 금방 다른 분야로 갈아타는 거죠.

Luke McNamara:

And I think that's an interesting problem.

좀 재미있는 사실이네요.

Everything you've just described there is a great indicator of why North Korean cyber-espionage is

방금 말씀하신 내용으로 보면, 북한 전문 애널리스트나 관찰자들이

a fantastic lagging indicator for North Korean analysts and watchers all over,

북한의 정권이나 정부에 대한 정보를 파악하는데 있어

in terms of getting that window into what are priorities for the regime and the government.

왜 어려울 수 밖에 없는지 알 수 있는 대목이네요.

From the standpoint of network defenders and organizations focused on it,

네트워크 보안 담당자나 관련 조직 입장에서

who do I focus on, who within my threat model do I need to be most worried about?

어떤 공격 그룹이나 위협 활동을 조심해야 할 지도 파악하고 있어야 합니다.

This seems to be some of what is a challenge presented by these sort of operations.

이것도 해결해야 하는 현안 중에 하나입니다.

The last podcast we did was focused on Latin America.

지난 팟캐스트에서는 남미에 대서 이야기를 나눴었는데요,

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.

몇 가시 예시로 언급했던 것 중에 APT38 과 TEMP.Hermit 에 대한 내용이 있었습니다.

Again, as you noted, a lot of them made a hard, fast pivot into financially motivated crime.

대부분이 금융 공격으로 방향을 빠르게 틀었었죠.

But you had organizations throughout Latin America that never had to be concerned with or worry about

하지만 남미 전역의 조직들 중에 이를 주의하거나 우려하고 있는 곳은 없었고,

and probably wasn't even on their radar, North Korean cyber-operators in different groups.

여러 북한의 사이버 공격 그룹 활동 들을 전혀 인지하지 못하고 있었습니다.

And so from this standpoint of where we've seen these fast shifts in targeting,

이렇게 공격 방향을 급하게 변경하는 경우에는

sometimes accompanied by continued focus on their primary area of collection, kind of added this to their repertoire.

때로는 그들의 전문 분야의 공격을 진행하면서, 추가로 동시에 새로운 공격 활동을 강행하는 경우가 있습니다.

Does that make it difficult for organizations that, again, the ones that want to focus on, all right, I've got limited resources,

그렇다면 다시 말해, 여러 조직들은 제한된 리소스로 스스로를 보호해야 할 때,

who are the top threat actors I should focus on based on the industry that I'm in, the region that I'm in?

지금 내가 속해 있는 산업, 지역을 고려해서 어떤 공격자가 가장 나에게 위협이 되는 지 파악하기는 과연 어려울까요?

North Korea seems to break that mold a little bit.

북한은 그 틀을 조금 깨는 것 같습니다.

Fred Plan:

A little bit, yeah. I mean, to some extent it still applies.

어느 정도는 그럴 수 있을 거에요.

If you're in South Korea or you're in the United States,

한국이나 미국의 경우에는,

you probably have a little bit more to worry about coming from North Korea than say Latin America.

남미보다는 북한 공격에 좀 더 주의를 기울이고 있어야겠죠 .

But yeah, there's those instances where you're not being targeted by North Korea until suddenly you are.

하지만, 갑자기 북한의 공격을 받지 않는다고 안심할 수는 없습니다.

And it just happens. And it's-

어느 순간 갑자기 일어나게 되는 것이죠.

Luke McNamara:

And you don't have those indicators, as you noted, with other countries.

다른 나라들에서는 대비가 잘 안 되어 있는 경우들이 많아요.

We don't necessarily have the North Korea defense strategy that they come out with every year and they say,

북한에 대비한 안보 전략 수립을 매년 할 필요가 없는 거죠.

"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."

우선순위나, 성장시켜야 집중해야 할 기술을 포함한 산업 군들에 대해

So you don't necessarily have those other indicators.

공격의 표적이 되고 있는 지를 모를 수가 있어요.

Fred Plan:

Yeah, and that makes it tough.

네, 그건 알기 힘들죠.

And then, again, especially because of the nature of how North Korea, at least as we understand how it's politically structured, right.

북한의 정치 구조와 같이 북한이라는 나라의 본질에 대해서도 알아야 합니다.

Ultimately it comes down to what's going on in Kim Jong Un's inner circle.

결국에는 김정은 정권과 깊은 연관성이 있는 거에요.

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.

한 인물에 의해 한 나라가 좌지우지 된다는 건데, 바로 북한이 그렇습니다.

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.

외부 다른 나라에서도 쉽게 예측할 수 있고 이해하기 쉽게 정부 시스템 잘 정립되어 있지 않아 매우 파악하기 어려울 수 밖에 없는 거죠.

It just doesn't exist within North Korea.

북한에서 그런 시스템이 있지도 않구요,

And then that makes it tougher for sure.

그래서 더 예측하기 어려운 상황이 만들어 지는 것입니다.

What's the answer from the network defender perspective?

네트워크 보안 관점에서 어떻게 해야 할까요?

It's tough, man, it's tough. Because yeah, like we're saying, you're not targeted by North Korea until suddenly you are.

굉장히 힘들텐데, 아무렇지도 않다가 어느 날 갑자기 북한의 공격 대상이 될 수도 있기 때문이에요.

But it comes down to the prioritization, right.

하지만 우선순위를 따져보면,

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

동북아시아권에서 사업을 하고 있는 나라들이 북한의 주요 공격 대상이었습니다.

that historically have been targeted by North Korean operations, so Japan, South Korea, the United States, things like that.

일본, 한국, 미국 같은 나라들이 주요 타겟으로 피해를 입었죠.

Or if you're in these industries of interest to North Korean operators like the defense industry or the financial industry.

북한이 높은 관심을 가지고 있는 방위 산업이나 금융 산업도 북한의 목표물이 되죠.

Then you can kind of compare and re-rank your priorities against what you believe to be the most likely threats.

자, 이제 서로 비교해 보고, 우선순위를 다시 따져서, 공격을 한번 예측을 해 볼 수 있을 겁니다.

But with the understanding that that can very quickly change.

하지만 경우에 따라 상황이 빠르게 변할 수 있다는 걸 인지해야 합니다.

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.

김정은 정권의 움직임이나 북한의 고위급 인사의 결정으로 인해 상황이 갑자기 바뀔 수도 있는 일이죠.

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.

그리고 이건 중국, 러시아, 이란의 공격자들과는 확연하게 북한 공격자들의 특성이 까다로운 원인입니다.

Luke McNamara:
Well that's a great segue way into my last question for you.

이제는 마지막 질문을 드려야 겠네요.

And I think you started answering it a little bit when you brought up ransomware.

랜섬웨어 얘기를 꺼냈을 때 일부 답변이 좀 되긴 했는데요,

I won't ask you to give any hard and fast predictions and hold you to them

과거의 사례를 비추어 보아 매우 예측하기 어려운 공격 그룹에 대해

in terms of what we will see from what has historically been this very unpredictable set of threat actors.

특별히 어려운 질문을 드리거나, 당장 앞으로 어떻게 예측되는 지를 알려달라는 것은 아닙니다.

But for folks looking for potential indicators of where North Korean operations, be they espionage, destructive, or financially motivated,

스파이 활동, 해킹, 금융 공격 등의 북한 공격을 미리 예측해서 대비하고 싶어하는 사람들에게

where they could go next from here from what we've seen this past year, what might be some guideposts to look out for?

지금까지 파악된 정보를 기반으로 앞으로 어떻게 예측을 해 보면 좋을까요?

Fred Plan:

Yeah, so one of the key ones, as I alluded to, is that expansion of financially motivated activity.

네, 제가 언급했던 내용 중에 핵심적인 것 중 하나는, 어떻게 북한의 금융 공격 활동이 확장되었는가 입니다.

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.

올해 초 처음 발생한 웹 스키밍 공격을 추적해 보니 북한을 향해 있었습니다.

So there's this shift towards increased financially motivated operations. And there was already a shift,

북한의 금융 공격이 증가하게 된 시발점이 되었구요, 이미 진행이 많이 되었습니다.

but now that's gotten stronger and expansion of that financially motivated activity has taken place.

현재는 금전 탈취를 목적으로 하는 공격 활동이 더 활발해 지고 확대되어 가고 있습니다.

So I think it would be very natural, if it isn't happening already, for those operations to expand to where the money is.

그렇지 않았더라도, 자연스럽게 금융권을 타겟으로 한 북한의 공격은 점차 확대되어 갔을 것입니다.

And that's currently ransomware operations.

그리고 현재 랜섬웨어 공격을 보면 그렇죠.

Especially, given the world that we live in now.

지금의 상황을 보면 더욱 그렇습니다.

I mean, the global economy in general is in bad shape.

현재 글로벌 경제가 그리 좋지 않은 상태죠.

North Korea in particular is in probably really, really bad shape

북한의 경우 더 상황이 심각한데요,

because their primary trading partner holds down the boarders first.

북한의 주요 주요 교역 상대국의 국경이 닫혔구요,

And China has not been as close to North Korea, relatively speaking, as they historically have been.

중국은 과거에 그랬던 것처럼 상대적으로 보면 북한과 가깝지 않고,

So surely that's impacted North Korea's financial situation.

북한에 대한 경제 제재도 큰 영향을 끼쳤습니다.

In addition to that, there's this shift recently towards the agricultural industry

더불어 최근 농식품 산업을 타겟으로 삼아 공격을 하고 있고,

and targeting, like I said, biotech, pharmaceuticals, things like that which we think is a response to a COVID-19 outbreak within North Korea.

바이오테크, 제약 부문과 같은 산업도 공격을 시도하고 있는 것으로 보아 북한에서도 코로나 상황이 심각할 것으로 예측됩니다.

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,

그래서 이런 의료 산업을 표적으로 북한의 공격이 더 거세질 것으로 보고 있구요,

especially as we're just beginning to come to terms with what might be happening in North Korea.

특히 이 점은 북한에서 곧 일어나고 있는 일들을 예측해 볼 수 있는 정보가 되기도 하고,

And they might be just coming to terms with what might be happening within their state.

앞으로 일어날 일들을 미리 예측해 볼 수 있는 정보가 되기도 합니다.

So that'll be something to watch out for.

그래서 주의깊게 북한의 동태를 파악해 봐야 됩니다.

The other kind of shift or trend with North Korean operators that we've seen this past year

또 다른 북한의 공격 트렌드로는

was a shift towards more using of social media in their operations.

소셜 미디어를 최근 적극적으로 활용하고 있습니다.

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.

링크드인(LinkedIn)이나 스카이프(Skype)을 활용하는 것을 발견할 수 있었는데 이것은 과거에는 사용하지 않았던 방식입니다.

Luke McNamara:

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

스파이 공격 활동에 대한 부분인거죠?

Fred Plan:

Yeah, yeah. Sorry. Yeah. So in terms of cyber-espionage operations.

네, 맞습니다. 사이버 스파이 활동에 대해서요.

So this is kind of a shift in their TTPs from what we've previously seen.

이전의 TTP 가 변화했다고 볼 수 있습니다.

We've certainly seen other countries doing this kind of thing, Iran for example or Russia, things like that.

이란이나 러시아의 공격자들에서 최근 본 방식인데,

But North Korea has relatively recently gotten into that as well.

북한도 최근 같은 양상을 보이고 있습니다.

And so we may see more development of their operations along that line.

따라서 북한의 공격 방식도 점차 발전하고 진화하고 있다는 것을 알 수 있습니다.

Luke McNamara:

Yeah, that's an interesting one to point to.

네, 흥미로운 지적입니다.

And again, you mentioned the case of Iran and how they've gone from utilizing that in cyber-espionage operations

말씀하신 이란의 경우처럼, 허위 정보를 유포하는 용도로 사용하거나,

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.

예전에 사용했던 동일한 TTP 를 활용한 점을 볼 수가 있었습니다.

Spoofing or pretending to be a journalist, setting up fake news websites.

기자인 것처럼 위장을 하거나 가짜 뉴스 사이트를 구축해서 배포하는 것처럼요.

Fred Plan:

The good old newscaster days.

예전 뉴스 보도 방식이긴 하네요.

Luke McNamara:

Good old newscaster, yes.

네, 옛날 일이죠.

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

북한 공격 그룹의 과거의 행적 뿐만 아니라,

but then also some stuff that we've been seeing recently, I think a lot of people will find this of value.

최근에 나온 사례들도 까지 매우 중요한 정보로 함께 놓고 들여다 봐야 합니다.

So we'll have to have you back on if any of these predictions come true.

다시 초대해서 앞으로의 북한 공격의 행적에 대해 더 이야기를 나눠 보면 좋을 것 같아요.

Fred Plan:

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

2021 년에 돌아와서 더 많은 이야기를 나누도록 하겠습니다.

Luke McNamara:

Well as you noted, you left yourself a good bit of wiggle room

말씀하셨듯이, 이들이 매우 예측하기 어려운 공격자임이 분명하고,

by noting that they're very unpredictable set of actors.

앞으로 할 이야기들이 많이 남아 있을 거라고 생각해요.

Who knows what we'll see from North Korea in the future.

북한이 앞으로 어떤 일을 더 벌일지 누가 알겠어요.

But, Fred, thanks again and take care.

다시 한번 나와 주셔서 감사드리고, 잘 지내시길 바랍니다.

Fred Plan:

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

네, 오늘 초대해 주셔서 감사합니다.