Eye on Security

Pandemic Impacts to the Cyber Threat Landscape

Transcript

Luke McNamara:

Welcome to another episode of the Eye on Security Podcast. I'm your host, Luke McNamara. And with me today is returning guest, Jens Monrad, Head of Mandiant Threat Intelligence, EMEA. Jens, it's great to have you back.

Jens Monrad:

Yeah. Thank you for having me, Luke.

Luke McNamara:

I think what we're going to discuss today is some of the impacts and changes in the cyber threat landscape, where that might progress and how that might evolve as we are now over a year into the pandemic, how that's going to impact the threat landscape. I think just to kick us off, some of the things that we've seen over this past year, a lot of which may be of no surprise in comparison to other sort of historical trends in the threat landscape, but certainly seeing COVID-19 get utilized as a phishing lure.

Of course, as we've moved into the vaccine development phase, some of the threat activity around targeting of that research that we saw even kind of early on from groups like APT 32, interest in what governments are doing, public health officials are doing in response to this pandemic. And then as the vaccines have gone into full swing, seeing that become valuable research to be targeted by different APT groups. Of course, we've had the impact from ransomware impact the healthcare system. And then also, as we're now entering the sort of distribution phase, seeing some of those networks of coordinated inauthentic behavior, disinformation focused around some of the different vaccines and trying to use that to drive wedges in certain communities. So with all that, what's kind of your sense of where we're at right now, and what are some things that we should be thinking about of how the threat landscape may be changing?

Jens Monrad:

Yeah, I think that's a really good review of the events happening in the past year, not just globally, but certainly also what we see in my region, which is the EMEA region, or Europe, Middle East, and Africa. And it might be worth mentioning that when you look at the EMEA region, it is 116 countries and we're a population of more than two billion people. So certainly when you look at that, in that aspect from a threat perspective, and what a healthcare crisis due to a global pandemic has caused, we have seen significant changes in I would say in how we're working and that obviously introduces new opportunities from a cybercriminal perspective. But interestingly, we also have forced local industries in different countries to rethink how they're doing business and how they can continue to facilitate the different services and opportunities to their customers.

I think in that aspect, one of the biggest changes we've seen is really that everybody's working from home. Nobody is going to any office and that has certainly raised an interesting and complex threat landscape

because now everybody is sort of their own CSO. In a way, companies are relying on a lot of unknown factors in terms of how do they secure remote equipment. Can they even enforce some sort of security control on privately-owned equipment? Certainly, that has been some of the discussion points that I've seen especially out of the European region. But on the same page, we've seen from a cyber threat perspective, we have seen some events, both were activities most likely motivated by financial gain, trying to steal credentials, or trying to monetize intrusions. And certainly also from an espionage perspective, seeing targeted industries to obtain some sort of intellectual property, I guess, both in vaccine development, but certainly also in the political space with the different political aspects going on.

But I think one of the biggest changes is really how we're working today and how that might influence the cyber threat landscape as a whole. And then obviously as we are hopefully progressing to a past pandemic stage with the improvements of a vaccine and those kinds of elements, what we might also see and one of the things that I'm personally concerned about is what will be the effect of job losses versus potential enrichment of the cybercriminal ecosystem. That is something that I'm concerned about.

Luke McNamara:

So that's an interesting point when you think about obviously a lot of these threats that we're focused on and that we're tracking, they're global in nature often in terms of the organizations that they can impact, but often the local drivers, the regional drivers can play a significant role in making something a greater threat or increasing the likelihood that you see threat actors entering a particular space. So it seems to me that one of the things I know you're thinking about is from the cybercrime ecosystem, you could have individuals who have been negatively impacted economically by this that are more susceptible to entering that space. And it's not just individuals that necessarily have a very technical skillset that can be used for things like malware development, right? There's all of these different functions that exist within the criminal ecosystem where people may be susceptible, interested in or pressured to take part. What are some of those things that you're thinking through in ways which individuals that could be at risk could enter this space?

Jens Monrad:

I think it all depends on the different regions. Within my territory certainly, there are some countries in Europe that have a higher population of youth that don't necessarily have a job either because the country's locked down, and some of the positions that they used to have is no longer available because nothing is open, right? But when you look at it from an ecosystem perspective with cybercriminal activities, you're absolutely right, it is certainly beyond being capable of producing or writing malicious code. When we dive into the cybercriminal ecosystem, there's a variety of different services being offered and also a rise of different roles to be played from a criminal perspective. You have people that potentially could be insiders that have access to sensitive information. You have people that are facilitating local services to money laundering services, or potentially providing some sort of assistance in how to transact stolen credit card details and how to take that money out of a digital system into the physical world. So there's a lot of different varieties.

And while I won't say necessarily, we have seen an increase in the ecosystem certainly, throughout the past two years, we have seen different people in Europe and in other places of the world try and offer their services or their access to that cybercriminal system. And obviously, if you are out of a job and you don't have any income anymore and maybe you're part of a family that you need to secure as well, my fear is that there might be an incentive to actually take some part in that ecosystem in order to have some sort of income to support your family or to support yourself for the near future.

Luke McNamara:

Do you see certain types of threat activity in this ecosystem being more attractive than others? I guess I'm thinking more around things that could be perceived as lower-risk threats. So for example, maybe someone doesn't have the technical aptitudes to be involved in deploying malware, like ransomware on a victim network, or they're concerned with the sort of law enforcement blowback from that, but maybe they would see it being advantageous to install a crypto miner, something that's maybe a little bit more surreptitious and less likely to get maybe a law enforcement response. Do you see certain types of activity being more attractive than others?

Jens Monrad:

Yeah, I think so. And then I guess that also comes down to the individual technical skills that people might have. But if operating out of some moral code, I guess people that don't necessarily feel comfortable, obviously compromising infrastructure or deploying ransomware or running some sort of extortion schemes against their victims, well, they might necessarily not feel too bad if they're just maybe facilitating their own bank account to money laundering, for example, or where they might facilitate their physical address to receive certain goods with the promise of delivering them to another address, for example. So those kinds of elements is I think perhaps somewhere in the gray area for some people because it doesn't necessarily feel that you are potentially affecting any victims, right? You don't get a sense of the victim that you're actually affecting because it's not as visual as ransomware and you're not in direct engagement with any sort of victims either.

So, those kinds of things, I think if I would label them, some of the lighter elements of the cybercriminal ecosystem, that could be potentially where we might see people offering their services. And it is really a vital part of the ecosystem as well. As you and I were talking, we were also talking on the back of takedown of Emotet where there was arrests happening in Ukraine. And certainly, the arrests that happened in Ukraine, for example, well, while it is speculated that they were part of driving that Emotet operation, certainly, they were not the full operation, right? So that could just be the people that are doing, in lack of better terms, the dirty work, whereas the people that are making the most of the money, they are not affected by the arrest. They might retire, or they might move to a different operation. And those kinds of services is always needed in the ecosystem. So it might be more attractive to actually pursue that path if you suddenly are out of a job, for example.

Luke McNamara:

Right. And I think what you're highlighting there is the resiliency of some of the aspects of this ecosystem, where we've seen law enforcement response and arrests that have been made against different portions of criminal groups and activity. Some of those have had very short-lived impacts on that threat activity or on parts of that activity. I guess one other question I have is now that we're thinking through, okay, these are some areas where we could see potential more interests and attraction of individuals getting involved in aspects of cybercrime, what might be some early indicators that we are seeing that trend, right? So if we have this as a hypothesis, what might be some ways that we would test this? Would we start seeing potentially an uptick in individuals on easier-to-access forums, the underground posting, hey, I've accessed the system, I'm looking to monetize it in some way, individuals that are offering money muling services? What might be some indicators that we're starting to see this shift?

Jens Monrad:

Yeah. And this is certainly part of a lot of what we do at Mandiant Intelligence, and certainly, within my region where we probably have the majority of our research and collection efforts, the reasons why we have that is to keep track on those kind of changes or whenever there is a slight change in the ecosystem. So some of the ways that we might be looking into this and we have been looking into this previously is if we suddenly see an increase in localized activity that we haven't seen before, so suddenly we might see an increase of individuals that are offering either their services or some sort of capability to the ecosystem in a localized language that we haven't necessarily seen a significant amount of activity in before. And that would certainly be one of the areas that we are looking into.

And I think when we talk about it in relation to COVID and then compared to the cybercriminal ecosystem as a whole, I think doing the initial lockdown that we experienced especially in Europe, I think the total amount of, for example, phishing emails related to COVID-19, or coronavirus, or any other type of activity that you could compare that with, I think we were peaking maybe at 10% of malicious emails that we are seeing totally. And what that also means is that there is an ongoing ecosystem that is focusing on making money on various legal activities, and they will do that regardless of COVID-19 pandemic and the healthcare crisis. So I think the incentive there is also that if you can get more resources by people offering their services, that system can keep growing right.

Luke McNamara:

So we've talked a lot here about the cybercrime aspect of this when it comes to the nation stateside, what we see from ABT actors. Obviously, a lot of those have standing intelligence collection requirements, but they're also going to move onto things of immediate or temporary interest for the requirements for the sponsors that they're collecting for. We saw that, for example, with North Korea and some of the swift pivoting that we saw towards a vaccine targeting. Are there any particular aspects of the pandemic as we stretch on into the second year that you see in EMEA shaping APT activity beyond what we've already seen?

Jens Monrad:

I think a lot of it that we will see in this year will be around different political aspects. So in Europe, obviously you have the EU council meetings, you have certain political and country group organizations. For example, in the Middle East, you have the GCC and so on. Those kinds of political decisions that will be made on the back of a global healthcare crisis and also a global pandemic will most likely also be a target of other adversaries or other nation-states that might have an interest in either in learning about changes in political development, or potentially upcoming sanctions, or other types of political discussions. And we are still seeing those kinds of frictions across my region, where obviously with that many countries, certainly not all of them are really good friends and some of them are also in global or regional conflicts or part of EU, or US, or global sanctions.

So I think a lot of the targeting that we will see this year will be based on what sort of political outcome there might be and discussions coming out of let's say EU, for example, or any other significant changes coming out of, for example, NATO, or those type of political developments. While we have seen obviously a continuous targeting from what we would call espionage campaigns, obviously focusing to a degree on vaccine development and so on, I think a lot of it will be on the political aspect because we also have to factor in that some of the meetings that will take place this year is how, for example, the EU region, what should be their stance on let's see Russia, for example, and there will also be other developments like for example, the North Korean 2 gas pipeline. And those elements I think will be a driver for espionage activities because obviously, it's a very good place if you want to learn about potential political outcomes or

negotiation standpoints that we might see.

Luke McNamara:

And of course, the other politically motivated arena, or at least one other politically motivated arena that we see cyber threat activity around is disinformation. And we've seen this to some extent already, as I mentioned, with respect to some of the messaging around specific vaccines, or even I think in the early stages around this time or a little bit later last year, even sort of the origins of the pandemic, where it came from, and that being used by some of the different networks that we track to spread fabricated content around that to drive a wedge in certain countries or within different political blocks. Do you see that either because of the response of different countries or the national origins of different vaccines as we're seeing those come to market, do you see that playing a role as well in what we might see in EMEA?

Jens Monrad:

Yeah, certainly. And one thing that I think is also worth paying attention to is that I think for at least nation-states that are considering maybe participating or building up capacity when it comes to information operations, which stretches far beyond what we have previously seen, obviously, when we talk about influence operations or information of recent campaigns, we always talk about US elections, right? I think certainly there has been a lot of learning points for different countries and maybe also countries in my region where it might become attractive to try and control the narrative in the media or on social media, right? So certainly, that could be an aspect that we could potentially see more of. Again, also depending a bit on an issue of political outcome that might be happening regional-based in EMEA or politically-based on some of the different political groups that we have, like the EU or GCC, for example.

Luke McNamara:

So bringing this back around to the cybercrime aspect of this, you have this potential risk as a driver of the economic conditions in EMEA, what are some ways that you think we can minimize that risk? And that could be either whole of government, whole of society approach to this down to how individual organizations are working to minimize the sort of insider risks that you talked about. What are some ways that we can minimize that?

Jens Monrad:

It's a good question. I'm already seeing some improvements at least personally what I would like to see. And obviously, when we see these kinds of joint collaborations between law enforcement in different countries in Europe and maybe even extending to US, for example, I think that has a significant effect on making the ecosystem less attractive to work on. I think on a longer scale, we also eventually need to have a discussion around how we can address this on a political level. While crime is a global challenge, I don't think that there is a country in the world that doesn't have or face some sort of risk based on cybercrime.

What we also are seeing is that certain countries, they don't necessarily play an active role in either facilitating international arrests or maybe not even considering arresting people that are in the country as long as they're not making their illegal activities in the country, right? And that is something that we need to address if we are to minimize the threats on a global scale. And equally by becoming much more vocal about it, whenever there is takedowns or whenever there is arrests, certainly that will also help. And then lastly, governments play a huge part in informing the citizens in terms of what are some of the downfalls of

participating in cybercriminal activities. And I think there is really much to learn from different countries. That will fall down to the different maturity levels of each individual country in my region.

Luke McNamara:

Do you see that any particular regions within EMEA that you see that being more at risk for this sort of activity, or that are also good examples of ways in which they've worked to address some of the cybercrime ecosystem components we've discussed here?

Jens Monrad:

I think I don't necessarily want to call out one particular country. But in the discussion related to let's say job losses, for example, obviously, my concern here is that certainly countries that have a higher percentage of the younger generations that don't necessarily have a job or cannot find a job, you would also assume that they have a bit more abilities working with computers, understanding the different aspects of the internet, and those kinds of elements, which makes it maybe easier for them to participate in some sort of cybercriminal activity.

The other thing is obviously in countries where there is still either a distrust when it comes to governments, or where there might be a high increase when it comes to corruption, for example, certainly they could also be a contributing factor to the cybercriminal ecosystem because it is perceived as a natural way of making business either because you don't necessarily trust your government or because the government in some way or fashion has behaved in a way that you would assess to be participating in some sort of corruption scheme. Right? So, those are some of the elements that I think will be a contributing factor to the ecosystem with the pandemic or without the pandemic.

Luke McNamara:

That's an excellent point. Any final thoughts on anything that we've not discussed here that pertains to what we might see as drivers shaping this, particularly with what you're looking at or expecting to see in EMEA?

Jens Monrad:

I think this is probably something that or at least it's something that I have said before when I talked to executives and senior leaderships in different organizations across Europe and the Middle East is that with the global pandemic happening and obviously, there's a healthcare crisis in many countries and you don't necessarily know or understand how we are supposed to work next quarter. It could be we're still in lockdown, or it could be that certain countries are opening up. Organizations really need to pay attention to the ongoing threat activity that will always happen regardless of the current situation that we're in.

That's something that I think is worth just repeating and reminding the listeners on is that while it is certainly a driver when we talk about cyber threat activities, it is probably let's say 10% of the cyber threat activities that we see. So for any organization out there that are still protecting or defending against threats or making strategic decisions on how they can defend against the ever-changing threat landscape, they still need to have a plan for the 90% of cyber threat activities that will always happen regardless of the current situation that we are in. So I think that's very important also when we move forward.

Luke McNamara:

That's a great point to end it on. Jens, as always, great to talk to you and have you on, and we'll have to have you back maybe a little bit later in the year to see how some of these predictions may play out.

Jens Monrad:

Thank you very much.

Luke McNamara:

Take care.

Jens Monrad:

You too.