Eye on Security

The “Big Four”: Spotlight on Iran

Transcript

Luke McNamara:

Welcome to another episode of the Eye on Security podcast. My name is Luke McNamara, your host here for the second part in a series that we are doing, Looking at the Big Four. Today, we are tackling Iran and joining me to help do that are, Sarah Hawley principal analyst on the cyber espionage team, here at Mandiant intelligence and Lee Foster, Senior Manager of information operations analysis, and returning guest. Sarah and Lee, thanks for joining me today.

Sarah Hawley:

Hi Luke, thanks for having me.

Lee Foster:

Great to be here again Luke.

Luke McNamara:

So I think kind of how we kicked off our last discussion around North Korea, we'll do something similar and we have both of you here to break down, not just the cyber espionage and cyber attack activity that we've historically seen from Iran, but also some of the information operations and what they've been building out in that space. But I think, and maybe Sarah, we'll start with you. Maybe just start with framing some of the high level goals that we've seen over the years with Iran and the issue of cyber to carry out different operations. What have we seen from them and typically what has that activity been characterized by?

Sarah Hawley:

Sure. So Iran has these long standing overarching goals related to basically their geopolitical ambitions to become a regional power, countering the West and regional rivals like Israel and Saudi Arabia, as well as national security and domestic concerns, basically to protect the regime. And on the cyber front, typically the activity we've seen is characterized by espionage related operations, like waves of spear phishing campaigns, or credential theft operations and

intelligence collection aimed at gaining access to strategic or commercial information from government or private companies from a variety of industries like government, telecoms, energy, for instance, that would benefit Iran's interest in some way. As well as internal targeting against the Iranian dissident community or individuals outside its borders.

We've also seen offensive tools use like wipers, which have been used against critical industries in the region like energy and oil and gas for retaliation or competition, or to undermine a rival. And interestingly, while these goals play a role in the intent behind area and cyber operations, in the last year, the effects of the coronavirus pandemic related to the level of unrest in the country, mistrust of the government because of their poor response to COVID and the effects it's had on public health and the economy, as well as reimpose sanctions, these are all probably additional factors that currently shape activity we see today.

Luke McNamara:

Iran is certainly kind of similar to North Korea as state sponsor of cyber espionage and cyber threat activity in general, that I guess a lot of people think about as more of an emerging power or emerging player in this space, but they've had a capability or have been building up a capability in various forms in terms of offensive cyber activity for some years, right? So this is not a new thing for them, even as we've seen it matured and grown, and increase in capability. It's certainly not a new thing for them to utilize cyber for the purposes of, disruptive attacks or a lot of what we see, which is separate espionage, right?

Sarah Hawley:

Yeah, so Iran has a history of using offensive activity, mostly in the form of DDoS and web defacements at the hands of Iranian hackers or the hacktivist community. Especially during the earlier years, like from 2010 to 2014-ish time period, some more notable events during that time would have been operation Ababil, which was an extended DDoS attack against the US financial sector, likely to get back at the US for Stuxnet and related sanctions at that time. There was also the destructive attack on the Sands Casino for a comment the CEO made about Iran.

And also the first, probably more notable wiper attack was the Shamoon incident against the Saudi Arabian oil industry. And since then, we have continued to identify other wipers with links to Iran like other Shamoon variants, Dustman Zero clear and Deadwood are probably some of the most recent ones. And since then too actors who were part of these activist groups were also starting to perform espionage or some form of Intel or information collection either in response to government taskings or on their own likely for profit.

We've seen a steady increase here regarding espionage as well in terms of tool development and evolving techniques and improvements to their operations and targeted campaigns. So things have definitely been evolving since then becoming more professional and organized.

Luke McNamara:

Yeah. I definitely want to get into a little bit later talking about some of these different groups, either organizations or the entities that we track them as, as APT or UNC groups, but Lee, I want to bring you in here as well, because certainly the story around Iranian cyber threat capability and how it's grown and expanded over the years, you can't tell that story without also looking at information operations and that as another tool that they've been establishing in their arsenal.

And certainly one where I think when most people think about disinformation and online influence operations, they may think of the capabilities that we've seen from Russia, but Iran has been building the capability in this space as well. Right? Talk us a little bit through some of the things that are kind of noteworthy in that space.

Lee Foster:

Yeah. What's interesting about Iran's foray into the whole kind of online driven information operations is just how rapidly they've been expanding the capabilities here and how aggressive they'd be getting, even in just the past couple of years. Now, primarily if you were to kind of identify the overarching motivation behind these activity in the IO space was really focused on undermining Iranian adversaries. Both near and abroad, particularly Israel, Saudi Arabia, but further afield as well, including the US. And even in just the past, too in some years, we've seen this rapidly increasing volume of activity and also aggressiveness behind the activity.

We've talked previously on a prior episode about the Liberty Front Press IUVM network of fabricated news sites, that we uncovered in 2018, which really broke over the whole insight into Iranian IO. That quickly progressed to other instances like endless mayfly and a campaign we called Distinguished Impersonator in which Iranian actors were actively impersonating US political candidates on social media during the 2018 midterms. But then if we look now, even at the just past 2020 election, has been a number of revelations about Iranian actors aggressively trying to influence US election directly.

The US government attributed to Iran, some activity that involved emails purportedly being sent by the members of the Proud Boys to voters in the US effectively threatened if they didn't vote for our former US president Trump. They were clearly taking advantage of the very unique social dynamics here in the US, knew that audience and knew exactly the type of messaging to push. And then even more recently, the US government also revealed that Iranian actors were responsible for a campaign referred to as Enemies of the People in which they stood up a website that revealed private information regarding US officials and other individuals that were involved in the US election in 2020. Effectively claiming that these individuals responsible for stealing the election, the rigging the election, and basically trying to stir up a further or amongst those audiences domestically within the US that believe that the election was rigged.

And so this is a much more direct influence campaign, actively seeking to influence very specific audiences that is just far more aggressive than even we were seeing two years ago from them.

Luke McNamara:

Is that something that, and this is, I think also for you Sarah, but as we think about the willingness to carry out certain activity, certainly it seems like in the information operations space and with respect to the activity we saw in 2020, but also maybe even in 2018, some of the stuff in the US election then, that maybe there was a greater willingness or greater interest in involvement in targeting those sorts of democratic processes. But I guess in some of these other areas too, maybe it's targeting of critical infrastructure, have we seen kind of a shift over the years across all different types of cyber threat activity, where that willingness to engage in increasingly antagonistic operations has been apparent or what might be some things that we could look at that showcase how we should think about maybe changes in attitudes towards usage of some of these tools?

Sarah Hawley:

Well, on the espionage side, I think we can look at more concerted efforts or like pivots to target critical industries and changes to the geopolitical scene and the energy and oil and gas market, that might drive some sort of additional activity there. Also, we can look for changes to their operational TTPs, like advances in social engineering, malware or using new techniques, as well as the registration of infrastructure or domains or patterns there that may use certain naming conventions that could signal potential intent to target a particular organization or sector.

On the other side of that, typically the wipers or the more offensive activity used have contained some sort of political messaging associated with them, whether it's through a string or an image. So changes to their use of wipers, possibly, maybe related to veering away from the critical infrastructure targets they usually are used against, or a lack of a political message would point to questions like if the use of these tools are going to be more associated with less political attacks, or maybe those tools are being shared with other actors with other motivations. Or if the operator is doing something on the side.

Along those same lines too, there have been some public reports of ransomware associated with Iranian actors, which also brings to light similar questions surrounding the possible use of ransomware, or if there's some sort of tool sharing going on here, or there's something going on, on the side.

Luke McNamara:

Yeah. And that's one of the things I think in each of these episodes, focusing on Iran, North Korea, China, and Russia, looking at the sort of nexus or connection and interplay between

assets and resources that are used for what appear to be clearly nation state purposes, but then also the criminal underground and how that looks different in each of these different contexts.

Luke McNamara:

So I wonder if you could talk a little bit about, you referenced a little bit earlier that the hacker communities and how this has been something that Iran has leveraged over the years as they've built up their capability. Describe for us a little bit of what that looks like and what those sort of relationships look like.

Sarah Hawley:

Yeah. So the hacker community has played a role in Iranian cyber scene from the early years to now going from being a member or being associated with hacktivists or hacking forums in some way, to becoming a contractor or forming a company. But this also creates some difficulty in terms of attribution and tracking because these individuals can jump from job to job or possibly be doing things on their own. But we do have some indications through our own data collection information released through US indictments and sanctions, as well as series of leaks that gives us some insight into those relationships and the range of activity taking place.

For instance, on one side, you have individuals with ties to the hacker community, essentially conducting information theft on their own and turning that around, pricing it and selling it to the highest bidder. And then you have entities conducting espionage in attack operations likely on the behalf of the IRGC or the Islamic Revolutionary Guard Corps, to front companies set up by the MOIS or the Ministry of Intelligence Security to conduct operations.

Interestingly, a recent leak alleged that a front company called Ronna, which was called out by the US as being set up by the MOIS, had used stolen identities and personal information to set up cryptocurrency accounts, to buy infrastructure and tools. Information on one of those leaked documents have been previously identified as being associated with APT39, which is in Iranian APT that's best known for their surveillance and monitoring and counter intel operations. So these things kind of taken together gives us some indication of a possible relationship there between APT39, MOIS and Ronna. And also gives some insight into how 39 possibly funds its operations through some sort of criminal activity.

Luke McNamara:

So since they're opened this store around attribution, and we'll definitely get into this a little bit more maybe talking about some of the activity from these different APT groups, but Lee, I'm curious from your standpoint, I know kind of the approach that we take to attribution and assessment analysis of activity, the disinformation space is a little bit different. So often I know we're looking at things like the message that's being spread, but can you talk a little bit about what that looks like when it gets to, we're saying we suspect this account, this network of

activity we're observing is in support of Iran, but what's getting us to that point, that call?

Lee Foster:

Yeah, and that really varies depending on the particular campaign we're looking at. In our public reporting around some of the Liberty Front Press Network in 2018, we highlighted as you alluded to certain behaviors, the type of content being pushed, but then looking at that in combination with other indicators, such as the fact that social media accounts were registered using phone numbers from Iran or that certain domains, email addresses and so on, had been previously affiliated with particular Iranian individuals or organizations.

And so we're kind of compiling all of that together to come up with an assessment around attribution. Obviously, and importantly, very carefully outlining what you don't know and communicating the uncertainty behind that. What's been interesting in some of the more recent operations is these actors kind of get more competent for lack of a better term. Some use the term sophisticated, although there's always debates around what that actually means, but we're definitely seeing an improvement in OPSEC in some of these campaigns. So sometimes getting hold of those technical indicators can be a lot more difficult.

And really where a lot of the attribution is coming from now is these kinds of combined insights from different organizations. Looking at what each other is saying, comparing the evidence and then marrying that up together. So for example, on our side, we might be looking at behavioral and content based indicators. We can clearly identify, for example, that say a network of social media accounts is inauthentic and clearly demonstrate that they're coordinating and then looking at what they're pushing, who they're pushing it to, we may come up with a low competence assessment. That this is being conducted in supportive of Iranian interests, not necessarily even that it's Iranian government conducting it, but the motivation behind it is to, in some way benefit Iran.

But then, other organizations, say social media platforms, maybe have other backend data. I may look at that activity and then they can come out and say, yes, we've actually seen these emanating from Iran. And that's been a frequent occurrence with a lot of takedowns and the social media companies have done where they've highlighted that third party researchers, including us in some instances, have identified the suspicious behavior and then they've gone and looked on the backend at the activity on that platforms and can see direct ties to Iran in some manner.

Some of these other attributions, there's still not much out there in the public domain. I mentioned a couple of US government attributions to Iran around the 2020 US election, but there's not a lot of specific details around that for obvious reasons as to how the US government was able to attribute that activity to Iran. So it really does vary on a case-by-case basis.

Luke McNamara:

And in terms of when we think about some of the immediate drivers or longstanding themes that drive and shape activity, both in the IO space, but also with respect to what they choose to carry out disruptive operations against, what they choose to collect against, standing intel collection requirements, what are some of the things that we typically see?

I know it seems like we've seen a targeting of kind of InLight kind entities when they've, for example, been hit with sanctions. Sarah, you mentioned the operational Ababil earlier, that was the targeting of the financial sector in response to sanctions. We've seen activity around elections. So maybe Lee, starting with you, what are some of the specific themes or messages that we've seen activity really galvanize around?

Lee Foster:

Yeah, this is going to sound obvious, but in the IO space, in particular, this is in many ways reactive to the contemporary geopolitical environment. So there's going to be ebbs and flows of activity, depending on Iran's relationships with other countries with its adversaries. And you asked earlier about intent and Iran's clearly it has the intent to engage in aggressive operations when it perceives it to be in its best interest to do so. But that doesn't necessarily mean it will continue at that level of aggressiveness for example, if relations with particularly adversaries improve in some manner. So it really does ebb and flow with kind of the broader geopolitical context.

Certainly when there are incidents or events that in some way directly impact Iran, there is a defensive reaction and kind of a counter effort with some of these campaigns effectively to push back or retaliate against particular, whether it be incidents or developments in relationships, whatever it may be. So really it is driven and can be driven by specific incidents and events on the geopolitical stage.

Luke McNamara:

That's both a mixture of sort of pro Iran content, as well as anti Israel, anti the West anti US.

Lee Foster:

Yeah, I'd say if you had to choose one of those, it certainly falls more on the side of undermining Iranian adversaries. And when it comes to the pro Iran kind of stuff, it's very much from a defensive posture. It's in response to something to try and counter narratives around Iran, or to try and bring up sections of Iran backup. It's not so much activity, just going out projecting this image Iran is great, right? Which is the kind of typical state propaganda you see from other actors.

A lot of it comes from this kind of perception of defending Iran's image in the world.

Luke McNamara:

And Sarah on the cyber espionage side and what we've seen there, certainly as you noted, some of the recent activity been shaped around COVID economic concerns, you mentioned, I think earlier some of the internal targeting. I know we've seen targeting of dissidents. What are some of those things that seem to be priorities for Iranian intel collection?

Sarah Hawley:

Yeah, similar to what Lee was saying in terms of targeting the geopolitical landscape shapes Iran's targeting and their priorities in the volume of that changes and it seems to come in waves. So along with those big overarching goals, I mentioned earlier, the effects of COVID on the public and the rising levels of dissatisfaction, essentially going on in the economy as part of that and sanctions, these are all probably big issues for the government today. While we probably won't see all the internal targeting going on, we have also observed other targeting shifts related to the pandemic and public health. Like targeting of the pharmaceutical industry and global health organizations.

Related to their economic problems and the reimposed sanctions, we've seen targeting of Western policy think tanks. And because they use shipping as a way to continue to export oil, we have also seen instances of targeting geospatial entities in the shipping and satellite tracking industries. Probably to collect and monitor customer or shipping related data or imagery to try to keep off the radar.

Luke McNamara:

I know you're primarily looking at this obviously from a cyber espionage standpoint, but some of those same skillsets and intrusion capabilities being utilized to gain a foothold for operations we see targeting cyber physical systems and activity kind of in the destructive space. What have we seen in terms of the growth and capability there from Iran? You referenced earlier, for example, wiper malware, obviously one of the big target sectors or areas that Iran's going to have interest in, are just from, I think, an espionage collection standpoint, but the energy space, right? And we've seen sort of interest there in going after those sorts of targets, whether it's oil and gas, other sorts of extractive sectors, where they seem to be putting an emphasis on building up a capability to go after those sorts of targets.

Sarah Hawley:

We've definitely seen a parallel interest on the espionage side and for destructive activity going after industrial targets in the oil and gas sector. APT 33, 34 and TEMP.Zagros which are all campaigns that we track for instance, have all shown interest in this space and have used a range of techniques to target organizations in this space. Ranging from password spraying, to spear phishing operations. 33, for instance, has been linked to destructive activity before, and has also used spear phishing and password spraying, which is a type of brute force attack

where you spray commonly used passwords across a large number of accounts.

34 has used social engineering platforms and job themed Dolores as part of phishing campaigns to target victims as well. TEMP.Zagros too uses really targeted a spear phishing and is also really good at leveraging access from a secondary target, to target its primary target. Basically pivoting from a compromised email, for instance, to draft a phishing email that looks like it's coming from a trusted person or source to target similar industries.

Luke McNamara:

One of the things you referenced earlier too, is sort of political nature of some of these destructive operations. I think it was Shamoon, correct me if I'm wrong, that utilize some of the imagery and language in the course of the operations that clearly has some political intent. Have we seen, and Lee, I'm curious to your thoughts on this because I know in some of the other areas around the world where we've seen the expansion of information operations that are levering intrusion capabilities, right? Whether it's compromising a news outlet and then posting fabricated content there. Have we seen that sort of pairing in the context of Iranian activity or suspected Iranian activity?

Lee Foster:

Less so compared to other States, although some recent suspected endless mayfly activity appears to have also utilized some compromises of new sights as well as social media accounts. Again, for the purpose of spreading false narratives, fabricated news articles and so on. So there may be a bit of that going on. As always with all of these things, it comes down to visibility. We'll be going on an extensively and nobody's catching it, that's always a possibility. But the broader discussion here really does raise this interesting point because sometimes it can be very difficult to clearly define what is an information operation versus what is a destructive attack versus what is espionage intrusion.

And often there are strong overlaps with these, not necessarily in Iranian context, but certainly in other actors where something can start off as an espionage operation, kind of the valuable data is extracted, the stuff of any intelligence value is retained and then the rest is leaked to have that added effect. It could be argued on the incidents like Ababil, like Shamoon can also be conceptualized as info ops because of the political motivation. And they're using these tools to send a signal, right, to influence a behavior. So that could also be considered some regards and influence operation.

So we haven't seen as much evidence of Iran utilizing these tactics compared to other state actors, but we are seeing some indications of the use of what I like to just call traditional cyber threat activity to support what are primarily influence operations.

Luke McNamara:

No, I think that's a very important nuance point there with respect to these aren't necessarily as neatly categorized types of activity, as sometimes we think our conceptualization of them are. I want to get both of your takes on how we should think about Iran amongst the cadre of different adversaries that we're talking about here in the series, but also across the board.

There's obviously a lot of different threat actors that are out there that have the capabilities or more so that we've seen around demonstrate, but in terms of their intent, their willingness to use it in those capabilities, as we understand them today, this is going to obviously probably vary a little bit by sector and region too, but how should we think about Iran and their capability and willingness to use cyber threat activity? Sarah, we'll probably start with you.

Sarah Hawley:

Yeah. I mean, I definitely wouldn't count them out. They have this history and willingness to attack when they think it's necessary. Those operations have proved to be pretty destructive and have had real effects on their victims and targets. Their espionage operations too, are becoming more evolved. Even though we see similar themes like recruitment and jobs and the use of spear phishing and credential theft operations, but these things still work and they're getting better at tricking victims with really well-crafted social engineering, using social media to build rapport, performing reconnaissance, and being able to pivot from target to target. Their use of TTPs, like legitimate links and legitimate tools and campaigns and exploding VPN vulnerabilities that really let them get around being detected. They really don't seem to be deterred too much by public disclosures either.

So I think all these factors taken together, I think they definitely place Iran on the radar and make them stand out.

Luke McNamara:

Lee, any thoughts from you on that?

Lee Foster:

Yes. So from a IO perspective, Iran absolutely should be taken seriously as a prolific threat actor in the IO space. It's clearly demonstrated intent to pursue aggressive operations when it perceives it to be in its interest to do so. It does not have any qualms it seems about directly trying to influence audiences in adversary countries and so on. So from an intent standpoint, from a demonstrated history standpoint and from just a sheer volume of activity standpoint, Iran absolutely should be taken seriously as a threat actor in the IO space.

I think the capability questions of sophistication and so on, just maybe are a little less important in this context, compared to others, such as the espionage context. I've said this many times, we've spoken about this before that operations don't necessarily need to be particularly sophisticated to have that desired effect, to infiltrate a particular community or to shape

attitudes among a particular audience. Certainly it doesn't require much in the way of technical capability to pull off some of these operations.

I think we have to think broadly when we're talking about this concept of capability in the IO space, because it really doesn't take much from a technical perspective. Certainly matters less than it does say an espionage operation where technical proficiency, technical sophistication is going to be correlated with sophistication of the actual operations themselves and thus success.

Luke McNamara:

So you both kind of already touched on this, but I'm curious any sort of final thoughts or predictions of what we might see this year from Iranian threat actors. This time last year, we were all hands on deck preparing for potential activity in the wake of the Soleimani killing. Fortunately, we didn't really see that emerge, I think we saw a sort of ebb and flow throughout last year in different quarters in terms of how much activity we saw from Iran. Sarah, as you noted, some of that was kind of shaped around COVID. Any sort of final thoughts or predictions on what we might see this coming year?

Sarah Hawley:

So the geopolitical landscapes basically what's going on today and the shifts in diplomatic relationships and the oil market, I think are definitely going to continue to kind of shape how they use cyber internally and in the middle East and beyond that to the US. And we'll probably see an increase in activity as it relates to more current needs, like with a pandemic and the economic situation. So we can more than likely expect some continuation of strategic targeting related to US foreign policy or the new administration, as well as continued targeting in the middle East against government and commercial organizations, telecommunications, and energy, possibly finance.

It will be interesting to see too how COVID and the unknowns related to the financial situation in Iran also play into their more strategic needs and targeting over the next year and also how that may affect operational units in terms of resources and turning to other ways to make money.

Lee Foster:

From the IO perspective I think that, as we talked about earlier, we're likely to see Iran's IO threat activity, kind of track with as particular geopolitical relationships of what is going on in the world. So I imagine right now there's a lot of contemplation and observation around what the new US administration is going to do with regards to Iran policy, and that could well influence what types of activity Iran chooses to engage in and what level of aggressiveness it chooses to engage in.

So I think that the answer to your question is really dependent on what else is going to play out more broadly from a geopolitical perspective.

Luke McNamara:

A good analyst answers like that. It depends. Well, all good thoughts. Thank you both for coming on here and helping us make sense of Iranian activity in both the respective areas that you guys are tracking, what we've seen historically and what we might see to come. Thank you both and have a great day.

Sarah Hawley:

Thanks, Luke.

Lee Foster:

Thanks very much.

Luke McNamara:

Take care.