The not-so-Charming Kitten working for Iran

By Dina Temple-Raston

Published: 2023-01-09 · Archived: 2026-04-05 20:42:26 UTC

The protests that have swept Iran over the past four weeks have become the biggest challenge to the ruling regime since 2009. Demonstrators took to the streets after 22-year-old Mahsa Amini, a Kurdish woman who was arrested for allegedly violating Iran's hijab policy, died in police custody.

Protesters Click Here podcast spoke with last week say Iranian authorities have throttled the internet and are trying to knock demonstrators offline. But the authorities' cyber offensive goes beyond Iran's borders, and its roots were in place long before protests overtook the country last month.

We spoke with Sherrod DeGrippo, vice president of threat research and detection at Proofpoint, about Iran's efforts to target the Iranian diaspora. The interview was edited for length and clarity.

Click Here: Are you seeing any change in the way Iranian authorities are using digital tools to silence people outside the country?

Sherrod DeGrippo: We haven't seen a change, and that actually tracks with what we've seen from Iran in the past. In January 2020, the United States sent a drone strike to kill Iranian General [Qassim] Suleimani. And the question was, now that we've seen this kinetic warfare attack against an Iranian general, will we now see cyber espionage to match it? And the reality was, we did not see a change in the operations, projects, and targets that Iran cyber espionage groups had already been pursuing. They have their targets, they have their focus, and they tend to remain on track regardless of what's happening out in the world.

CH: Can you tell us about some of those hacking groups coming out of Iran like TA453 or — our favorite name — Charming Kitten?

SD: So what we refer to as Threat Actor 453 is often referred to in the intelligence community as Charming Kitten. And the reason for that designation, which is incredibly adorable, is it refers to Persian cats.

We see this group operating in support of the IRGC or Iran's Islamic Revolutionary Guard Corps, so you can think of them as sort of a quasi-military cyber espionage organization. Their main targets are diplomats, academics, human rights workers, journalists, and government agencies.

They pretend to be someone looking into issues around the Middle East, and a lot of times they offer to get on a Zoom call. There's almost this idea that they're associates or they're in the same industry or they're working on similar projects.

Now, you might think, why would a cyber espionage actor out of Iran be able to easily get on a Zoom? Well, generally they don't actually follow through with the call. They offer it and then send some kind of credential harvesting link, an attempt to get the username and password of their target.

CH: So are they actually getting their targets to download malware?

SD: For these credential harvestings, typically you click the link and it looks like a login to Zoom. But in fact it's a login to a threat actor's landing page.

CH: Given the depths of the protests rocking Iran now, are you seeing Charming Kitten branch out and attack more targets?

SD: So I think what's going on in Iran now in terms of the social unrest, the civil demonstrations, all of those things will *not* necessarily impact changes into the operations. But the previously obtained access that this threat actor has could easily be leveraged in service of the state's agenda *today* because of those things.

If these attacks have worked in the past, they already have access into, say, someone's email inbox that might be covering this. [Someone] that might have sources on the ground that are part of the demonstrations. The Iranian government, if they've been successful with these attacks against others in the past, they're able to see all that. And of course they will leverage that for their own agenda.

CH: How has the government used this cyber surveillance to push back against the demonstrations that are happening now?

SD: Iran has put a lot of work into making sure that their telecom systems are controlled by the state. They have reportedly turned on and off 5G cell service, so you're only able to make phone calls, only able to call for emergency services. So we've seen reports of that.

Something that's interesting to remember is Iran has one of the most well-developed and visible citizen hacker capabilities that we've seen. We're hearing a lot of talk about it with the Ukraine IT Army. Iran is the OG when it comes to citizens doing hacking on behalf of the government, both outwardly and inwardly.

CH: The IT army in Ukraine is focused specifically on Russia in response to the war, but you're saying that there are Iranian hackers who are ordinary people who are dispatched by the Iranian government to do their bidding?

SD: I would clarify that they're not necessarily dispatched by the Iranian government. They feel an alignment and an allegiance to the Iranian government, and they're a bit rogue, but they say, *I'm Iranian. I have allegiance to my country, and I know that my country hates Israel, Saudi Arabia, the United States, and I'm gonna go after them as my own choice.* And Iran's government isn't going to prosecute them.

CH: So it is just like Russia, where there's been very little punishment for its homegrown ransomware actors, as long as they were outward facing…

SD: I would completely agree with that, and I would even take it a little further and say, not only is there no punishment, there might be some aspect of reward. Iran takes those citizen activists and recruits them as a pipeline into official IRGC roles or other Iranian cyber espionage group roles. It's almost like a feeder path: Do it for fun, do it for yourself, do it for belief in your country and patriotism. And, hey, in the future, we may have a job for you.

[Dina Temple-Raston]

is the Host and Managing Editor of the Click Here podcast as well as a senior correspondent at Recorded Future News. She previously served on NPR's Investigations team focusing on breaking news stories and national security, technology, and social justice and hosted and created the award-winning Audible Podcast "What Were You Thinking."
