DOWN ON THEIR LUCK

Iran's Cyber Army Is Under Attack From All Sides

Iran's scrappy hacking crew is most effective when flying under the radar. Unfortunately for them, now everybody's paying attention.

Kevin Poulsen
Sr. National Security Correspondent
Published 06.21.19 4:46AM ET

Photo Illustration by Kelly Caminero/The Daily Beast/Getty

Iran's state-sponsored computer hackers have been under a steady and unusually public bombardment in recent months, with details of their secret operations bared to the world and portions of their online infrastructure stolen away. That unwanted attention has left Iran's cyberwarriors battered and

READ THIS LIST

Biden Runs Scared From the Press—Until He Slips Up
SAM STEIN, MAXWELL TANI

How Deadly Were the UK's Secret Nazi Concentration Camps?
NICK SCHAGER

Longtime Wacko Marianne Williamson Is Now a Dangerous Wacko
JAY MICHAELSON

The Evil Robots of the Ancient World
CANDIDA MOSS

After Last Week, the Dem Debates Now Have a Theme: Race
ADAM HOWARD
BEAST INSIDE

JOIN
EXCLUSIVE CONTENT
MY ACCOUNT
LOG OUT

If you're looking for a way to inflict pain on America and its allies without killing American troops or citizens, cyber seems like a domain that's ripe for mischief. Fortunately for Tehran, it's also a domain where they've demonstrated some notable skill. Security researchers have tracked a number of hacking gangs linked to Iran, each with its own flavor. Oil Rig, Iran's version of Russia's Fancy Bear, infiltrates networks far and wide through phishing attacks. The group dubbed Newscaster specializes in running fake personas on social engineering platforms to get close to a target. Elfin, or APT33, performs offensive, destructive attacks, like a November incursion into an Italian company with a presence in Saudi Arabia.

"They wiped a bunch of their computers," said Ben Read, senior manager for cyber espionage analysis at FireEye. "So it's something they've done recently."

Thus far, there's been no reporting of an uptick in Iranian cyberthreats over the past two months but cybersecurity firms are on guard. "They have been probing critical infrastructure

Hultquist, director of intelligence analysis at FireEye, told The Daily Beast. “We are concerned that similar incidents are imminent."

But Iran’s hackers have been having a run of bad luck, beginning last November when security companies discovered one of their covert hacking campaigns.

Dubbed DNSpionage by Cisco’s Talos, the campaign was both brazen and cunning. Instead of directly trying to penetrate a target network, the hackers were hijacking the controls for their target’s internet domain names. That allowed them to redirect incoming traffic wherever they chose. It was roughly the electronic equivalent of a thief filling out a bogus change-of-address card to forward a victim’s mail to his own address.

“They’re not good at overpowering the most defended spot,

finding the one place on your network that isn't well defended."

That sort of out-of-the-box thinking is typical of Iranian-linked hacking groups, said Read—they lack the resources of their counterparts in the U.S., China and Russia, but show unusual craftiness in their attacks. "They're not good at overpowering the most defended spot, but they're much better at finding the one place on your network that isn't well defended," Read said. "They're sort of the guy who can use the pump fake at just the right time to get a shot off."

FireEye publicly attributed the DNSpionage attacks, with "moderate confidence," to the Iranian government. And though the hacks mostly targeted the Middle East, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency chose

ordering other agencies to take specific defensive measures against DNS hijacking, and putting Iran's cyber capabilities under a microscope.

It was the start of a series of public disclosures that have bathed Iran's cyber ops in the kind of high-intensity light anathema to any covert organization.

In February, federal prosecutors unsealed espionage charges against Monica Witt, a former U.S. Air Force intelligence officer who defected to Iran. The indictment went beyond laying out the charges, and detailed how Witt allegedly helped cyber spies in Iran's Islamic Revolutionary Guard Corps target her former military colleagues on social media, using impersonation, fake profiles and inside-information provided by Witt to infiltrate a target's social circles. Four Iranians were charged as well.

The next month, Microsoft hit Oil Rig in another soft spot—the web addresses it uses in its phishing attacks. Repeating a tactic the company has been using against

Russia's Fancy Bear, Microsoft lawyers sued Oil Rig in federal

using to trick victims into giving up their passwords.

Things went from bad to worse for Iran's cyber spies a few months later, when a mysterious Telegram channel opened up called "Lab Dookhtegan"—"sewn lips" in Farsi.

> "Things went from bad to worse for Iran's cyber spies a few months later"

"We are exposing here the hacking and penetration capabilities that the malicious Iranian ministry of intelligence uses for its evil goals," the channel announced. "These capabilities include specializing in databases, Internet service providers, programming languages, hacking implants, social engineering, etc. This damn ministry uses these capabilities to spy on innocent compatriots… The time has come to crash them."

Lab Dookhtegan have meted out a wealth of inside information about Oil Rig's tactics, tools, and targeting, including the private source code for the group's malware, a long list of the systems they've hacked from Thailand to Qatar, the alleged names and biographical details of some of the individual hackers, and the blueprints for their command-and-control infrastructure, right down to the IP addresses of their rented servers.

"Exposures like that impose a cost," said Read. "When infrastructure gets burned, they have to find a way to get money out of Iran covertly to replace it. It wouldn't surprise me if, as a consequence of that, they had to kind of slow down."

The leaks have proven a bonanza for some of the security experts tracking Iran's hackers, who got the see the original source code for malware they've been encountering at crime scenes for years. Whoever is running the Telegram channels remains a mystery, but there's no shortage of suspects—spy agencies in Israel,

the United Arab Emirates, and the U.S. are all possibilities.

nobody doubts that they retain the ability to do serious damage. And Read notes that it's usually impossible to distinguish a routine espionage hack from a destructive attack until it's too late.

"They're good enough to get in lots of places and mess things up," said Read. "With what's going on geopolitically, we're taking them very seriously."

Kevin Poulsen
Sr. National Security Correspondent
@kpoulsen
Kevin.Poulsen@thedailybeast.com

Got a tip? Send it to The Daily Beast here.

President Joe Biden spoke to national media reporters in nearly a week of campaigning was to address a mini political crisis of his own making.

On Wednesday evening, hours after Sen. Cory Booker (D-N.J.) had admonished him for fondly recalling the collegiality of segregationist senators of the '70s, the former vice president was asked if he would apologize.

"Apologize for what? Cory should apologize, he knows better," Biden responded, standing outside an SUV on his way into a fundraiser. "There's not a racist bone in my body, I've been involved with civil rights my whole career. Period. Period. Period."

The moment marked a new level of aggression in a still-nascent Democratic primary. It also put the spotlight on what Democratic officials say is a risky and often confusing campaign blueprint being deployed by the party's presidential frontrunner. Increasingly, Biden seems to speak publicly or talk with

reporters only when he is under duress.

Biden as the top communications adviser on the 2008 campaign and in the Obama White House. "His message is that he's the guy who can beat Donald Trump and he is viewed as the least risky choice. Over time, if the only interactions he has is around these screw ups and gaffes, then he is going to start losing that message."

Over the past few weeks, Biden has been forced to grapple with a number of mini-controversies and self-inflicted wounds. His nostalgia for former Sens. James O. Eastland (D-MS) and Herman E. Talmadge (D-GA) was preceded by a 24-hour flip-flop on a law banning federal funds from funding abortion (Biden went from supporting the Hyde amendment to opposing it). Those two instances came after Biden

was criticized for not offering a full apology to Anita Hill and for

space.

Virtually every candidate running for president has to clean up the messes he or she makes. That's especially true for the frontrunners and those who, like Biden, have a proclivity for speaking with limited filters. But what makes Biden's current approach so confusing for other Democrats is that much of his public-facing campaigning has involved doing only that.

Elsewhere, the former vice president has kept a notably low profile, taking little opportunity to push his larger campaign message or make proactive defenses of his political baggage.

Biden hasn't appeared on national television since the day after he officially declared his run for president. Since then, the campaign has repeatedly declined invitations from television and cable news outlets. One network source told The Daily Beast that over the past several months, Biden has been offered a number of appearances on MSNBC, including telephone interviews.

And a CNN insider said the network reached out to the former

would be interested in participating in upcoming town hall events.

In addition to missing many of the forums packed with 2020 Democratic prospects, Biden was the only 2020 Democratic presidential candidate to decline an interview by *The New York Times* as part of the paper's major package released this week comparing the various candidates (and wouldn't respond to questions when asked why he didn't participate).

"I think that it is never a good idea to sit on a lead. That rarely works out well, and that's what they're doing," said Axelrod.

Though while in South Carolina this weekend, Biden worked the rope line well into the evening, mingling with press and voters, his campaign has previously restricted press access, running the vice president's press availabilities in a vastly different manner from the rest of the candidates. Biden's campaign has at points sealed off the press at events, only allowing a single reporter to represent the campaign press pool at Biden fundraising events.

In South Carolina, Voters Blame Media For Biden's Missteps

Biden's Way Rankles, but It May Be the Only Way

Joe Biden Misses a Major Opportunity on Iran

Occasionally, the Biden campaign has even seemed to forget or reverse course on planned media appearances. Earlier this month, the former vice president's staff told campaign reporters that he was going to be holding a press gaggle following an event in New Hampshire. But reporters were left hanging when Biden left the event and got into a waiting SUV without taking questions.

For communications specialists, the reticence seems not just at odds with the realities of modern media, but also unwise, leaving the impression that Biden—who has a reputation for joviality—is almost afraid of the scrutiny.

"If you are only interacting with the press when there is an issue of concern, you reinforce that perception that there are only problems," said longtime

Democratic strategist Chris Kofinis, who runs Park Street

Biden's defenders argue that the reason that he appears to interact with the press during times of duress is largely because those episodes are over-emphasized by the media itself. They point to polling data showing his consistent lead in the primary as evidence that the national press corps has fundamentally different priorities than the Democratic electorate.

The campaign has created its media strategy around that theory as well. Instead of doing national interviews, they have focused the vast majority of their attention on smaller local news outlets in the early primary states. Since jumping into the race in April, Biden has sat down for at least a dozen interviews with local TV and radio stations in Iowa and New Hampshire.

Biden hasn't been entirely closed off from national outlets. His campaign is the only one in the primary that allows a print pooler into his fundraising events. And on Thursday, senior Biden adviser Symone Sanders told CNN that

the former VP would be sitting down for an interview this

down with host Al Sharpton at an event for 2020 presidential contenders in South Carolina that MSNBC has exclusive rights to broadcast.

Nevertheless, Biden's caution when dealing with the press has stood out in a field of candidates where many others seem willing to accept any media request or live-streaming opportunity. Former Rep. Beto O'Rourke (D-TX) has been comfortable enough with campaign reporters to invite them on jogging outings, while South Bend Mayor Pete Buttigieg is so willing to sit for interviews he took questions while drinking brown-bagged beer in a park in New York City.

Campaign veterans say it would be unwise for Biden to go to those extremes, and not just because of his history of saying things that cause him political headaches. According to their logic, the former VP is already well known to the public and instead of re-introducing himself to voters, he can afford to spend that time on other campaign functions.

The question now being asked of the Biden campaign is not just

media landscape if he tried.

"You are not in the Hyde amendment era in the Democratic Party, and you are not in the James O. Eastland era of the party," said James Carville, a longtime Democratic operative. "How can you have the give and take [with the press] when your instinct is to get on the wrong side of two great issues of the modern Democratic Party, and that's abortion and racial relations? The world has changed."