NSA technical director: Iran-linked operations are about espionage, not destruction - CyberScoop

- Government
- Transportation
- Healthcare
- Technology
- Financial
- Watch
- Listen
- Attend
- Content Studio

government

A picture of Tehran, Iran. Iranian hackers are trying to conducting espionage missions against the U.S., according to the NSA. (Getty)

Written by Shannon Vavra

Jun 21, 2019 | CYBERSCOOP

Even as geopolitical tensions spike between Iran and the U.S. following an Iranian takedown of a U.S. drone, Iran-linked cyber-operations continue to focus on espionage and not destructive activities, a senior U.S. intelligence official says.

David Hogue, the technical director for the National Security Agency’s Threat Operations Center, tells CyberScoop Iranian-linked hacking groups are focused on traditional intelligence gathering.

“I think they’re trying to get more insights onto what U.S. policymakers are either knowledgeable of or think of them,” Hogue said in an interview with CyberScoop on Friday.

The past year has enflamed geopolitical tensions between Iran and the U.S. following the Trump administration’s withdrawal from the Iran nuclear deal. In April, the Trump administration took the unprecedented step of declaring a branch of Iran’s military to be a terrorist organization. Just last week, the administration blamed Tehran for attacks on two oil tankers in the Gulf of Oman. The Pentagon subsequently announced increased troop deployments to the region.

The attack against the unmanned, unarmed drone left the Pentagon poised to launch retaliatory strikes against three targets Thursday, although President Trump called off the strikes Thursday evening.

Hogue would not go so far as to use the names private cybersecurity firms have assigned several Iranian hacking groups, but indicated he is watching APT 33 and APT 34, which have commonly been associated with Iran.

By brute force

As an example of what the hacking groups are doing, Hogue said they have been trying to crack into military accounts through password spraying, a brute-force technique that continuously feeds passwords into login sites until one happens to work.

“Due to the commonality of shared passwords it can be successful if all of a sudden you get one,” Hogue said. “Detecting that is very hard because obviously people mistype their passwords all the time.”

When asked about the efforts, the Department of Defense told CyberScoop it “does not discuss cyberspace operations, intelligence or planning” as a matter of policy.

Iran-linked actors have been using password spraying techniques for years, according to Ben Read, FireEye’s senior manager for cyber espionage analysis.

The U.S. government, for its part, has been warning against these brute-force attacks. Last year, following an indictment of nine Iranian nationals, the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency issued a security alert on the matter.

In general over the last year, Iran-linked groups have been enhancing their game across the board, Hogue says.

They have “become a much more sophisticated adversary than we are used to dealing with,” Hogue says. “One of the most concerning trends for us over the last year has just been the rise in Iranian volume and sophistication.”

Broader attacks

Beyond password spraying, three prominent cybersecurity companies — CrowdStrike, Dragos and FireEye — told Wired that Iranian-linked actors were sending spearphishing emails in attempts to gain access to U.S. government agencies and private sector entities.

The cybersecurity firms stressed it is unclear if these attempts are intended to monitor for information or if there are destructive goals at stake.

“It’s probably more intelligence focused,” Hogue said of the spearphishing. “Their destructive activity seems to be mainly focused at their Middle East operations.”

The vast majority of Iranian-linked actors’ cyber activity has historically been focused on gathering information, Read points out.

“We see dozens and dozens of Iranian incursions in any given year and there’s usually one, maybe zero, destructive events,” Read, a former member of the White House’s National Security Council, said.

Hogue stressed that Iran could easily change its goals and turn to more destructive or disruptive behavior.

“We have a pretty good idea of their capabilities and intentions but you know with cyber, things can change rapidly,” Hogue said. “We’re not resting on our laurels.”

Iran-linked groups have launched destructive attacks in the past. The 2012 attack against Saudi Aramco, known as Shamoon, has broadly been attributed to Iran. As recently as last year an attack against an Italian oil firm and its networks resembled Shamoon.

For now though, Hogue suspects Iran-linked groups are just trying to gather intel on U.S. policymakers.

“They obviously don’t know what the U.S. positions are and so they’re trying to figure that out,” he said.

Former senior counsel of the House Intelligence Committee, Jamil Jaffer, says given the relationship’s volatility, Tehran is bound to try seeking more information on what policymakers in the U.S. are thinking.

“At the current time, there is obviously heightened tension between Iran and the U.S., so that might be why they better want to understand where we are, what we’re thinking, and to really understand how far we’re willing let them to push the envelope,” Jaffer told CyberScoop.

Dan Hoffman, a former chief of the CIA’s Middle East department, tells CyberScoop he has doubts about whether Iran has the capacity to gather this kind of strategic intelligence on the U.S.

“I certainly doubt the efficacy of that,” Hoffman said. “They don’t have that capacity on their own. They’ve got good cyber capabilities — they’ll go rob banks and shut down Saudi Aramco — but they’re going to ask the Russians for that sort of strategic intelligence.”

Hogue said he doesn’t believe the Iran-linked actors have been successful in learning what Pentagon personnel are thinking.

government
(U.S. Customs and Border Protection / Flickr)
Written by Jeff Stone
Jul 3, 2019 | CYBERSCOOP

U.S. Customs and Border Protection officials suspended Perceptics, the provider of license-plate scanners and other surveillance technology, from federal contracting following a data breach that exposed travelers’ information, according to federal records first obtained by the Washington Post.

CBP last month said one of its subcontractors, later identified as Perceptics, was breached in a “malicious cyberattack” that resulted in images of travelers’ faces, license plates, contracting documents and other data being made publicly available on the internet. Now, the Post reports, CBP has taken the rare step of punishing a federal contractor, citing “evidence of conduct indicating a lack of business honesty or integrity.”

As a result, Perceptics is prohibited from doing business with the government, a punishment that could last for years if the company is placed on a government blacklist.

CBP said on June 12 that a subcontractor had violated government policy by transferring images of license plates and traveler’s to the subcontractor’s corporate network. Then, hackers infiltrated that network in a breach that affected fewer than 100,000 people who entered and exited the U.S. in a vehicle through a specific lane at one border stop over a nearly two-month period.

“If the government collects sensitive information about Americans, it is responsible for protecting it – and that’s just as true if it contracts with a private company,” Sen. Ron Wyden, D-Ore., said at the time.

Customs and Border officials were collecting facial scans as part of an expansion of facial recognition at border checkpoints.