Iran Ups its Traditional Cyber Espionage Tradecraft

By Kelly Jackson Higgins

Published: 2019-01-30 · Archived: 2026-04-05 16:39:27 UTC

Iran's nation-state hacking machine mostly is known for its destructive cyberattacks: first with Web defacements, then crippling distributed-denial-of-service (DDoS) attacks, and most recently, data-wiping. But Iran increasingly is increasingly honing its operations in pure intelligence-gathering cyber espionage.

Cyber spying is nothing new, but over the past few years it has evolved into more of a step one for sophisticated nation-state hackers to know their targets, burrow in them, and ultimately wage more damaging attacks, such as ransomware, financial crime, data leaks/doxing, intellectual property theft - and in the case of some Iranian hacking teams such as the one behind Shamoon, data-wiping.

FireEye's research group this week officially christened one Iranian hacking team it has been tracking for more than four years, as APT39 - the same group of hackers that Symantec already calls Chafer and CrowdStrike calls Helix Kitten. The hacking group operates as an old-fashioned cyber espionage operation, but with advanced stealthy tactics and tools to meet its intel-gathering objectives.

Benjamin Read, senior manager of cyber espionage analysis at FireEye, says his team spotted APT39 in December of last year waging attacks against the telecommunications, travel, and technology services sectors, in campaigns aimed at gathering information and records on individuals. The attackers likely were rooting around for details on phone calls of specific individuals, as well as their travel plans and patterns in support of a broad Iranian government espionage operation, he says.

APT39, unlike its counterparts in Iran that wage influence-peddling, disruption, or destructive cyberattacks, focuses specifically on the theft of personal information for use in monitoring, tracking, and surveillance operations by the nation. "They're generally stealing data ... in bulk and then processing it" for usefulness and use, he says, adding that FireEye does not have insight into the types of individuals APT39 is after.

"They're gaining information on the very target itself," Jon DiMaggio, senior threat intelligence analyst at Symantec, says of APT39/Chafer. "It appears they do have some cooperation with other groups" in the Middle East region, he says. "That region's groups really play together often, which is one of the big differences in attacks" there, he notes.

Symantec by policy doesn't identify nation-state hacking teams by country, but rather, by general region.

US Intel Community Calls Out Iran

Meanwhile, US intelligence officials see Iran as one of the biggest cyber threats to the US in the next year. Daniel Coats, US director of national intelligence, in a report yesterday said Iran is among the main hacking adversaries to target the US in 2019, along with Russia, China, and North Korea. "The use of cyber attacks as a foreign policy tool outside of military conflict has been mostly limited to sporadic lower-level attacks. Russia, Iran, and North

Korea, however, are testing more aggressive cyber attacks that pose growing threats to the United States and US partners," according his statement in the Worldwide Threat Assessment of the US Intelligence Community, which was given to Congress yesterday.

Iran will "continue working to penetrate US and Allied networks for espionage and to position itself for potential future cyber attacks, although its intelligence services primarily focus on Middle Eastern adversaries — especially Saudi Arabia and Israel. Tehran probably views cyberattacks as a versatile tool to respond to perceived provocations, despite Iran's recent restraint from conducting cyber attacks on the United States or Western allies," the report said.

And like many nation-state groups, APT39/Chafer uses legitimate hacking tools such as Mimikatz and Microsoft apps like Windows Credential Editor, which makes the group difficult to detect. The key to catching them using legit tools is monitoring and looking of unusual behavioral trends and usage, DiMaggio notes. "Anyone can download and use Mimikatz," he says. "A lot comes down to behaviors, targets, the patterns and sequence of operations, how they get onto the network ... Attribution is getting harder, not easier" with these types of tools in use, he says.

If a tool is used at an odd time of day, or if a file gets dropped onto the network that hasn't been seen before, that could indicate an attacker is behind the tool, he says.

Other Iranian APTs

FireEye also closely follows other Iranian nation-stage hacking groups - APT33, APT34, and APT35. APT33 typically targets the defense industrial base, and has waged data-wiping attacks on victims; APT34 (aka OilRig), which may be related to APT39, conducts traditional cyber espionage, but mainly against foreign affairs ministries, Read notes. APT35 also targets the defense industrial base sector, but isn't known for the typical spear phishing attack in its initial step, for example.

What sets APT39 apart from its Iranian counterparts is its more "personal" touch of getting information on individuals. The group mostly uses the Seaweed and CacheMoney Trojan backdoors, as well as a variant of the Powbat backdoor, FireEye found. The attackers also employ relatively strong operational security to avoid detection; they were spotted running an altered version of Mimikatz that bypasses anti-malware tools, as well as conducting credential harvesting outside the victim's network.

"They are a bit stealthier and more careful than other Iranian groups," FireEye's Read says.

However, so far, he says, Iran hasn't retaliated cyber-wise against the US for withdrawing from the Joint Comprehensive Plan of Action (JCPOA) nuclear agreement, however.

Related Content:

About the Author

Editor-in-Chief, Dark Reading

Kelly Jackson Higgins is the Editor-in-Chief of Dark Reading and VP, cybersecurity editorial at Informa TechTarget, where she leads editorial strategy for the company's three cybersecurity media brands: Dark Reading, SearchSecurity and Cybersecurity Dive. She is an award-winning veteran technology and business journalist with three decades of experience in reporting and editing for various technology and business publications and major media properties. Jackson Higgins was selected three consecutive times as one of the Top 10 Cybersecurity Journalists in the U.S., and was named as one of Folio's 2019 Top Women in Media. She has been with Dark Reading since its launch in 2006.
