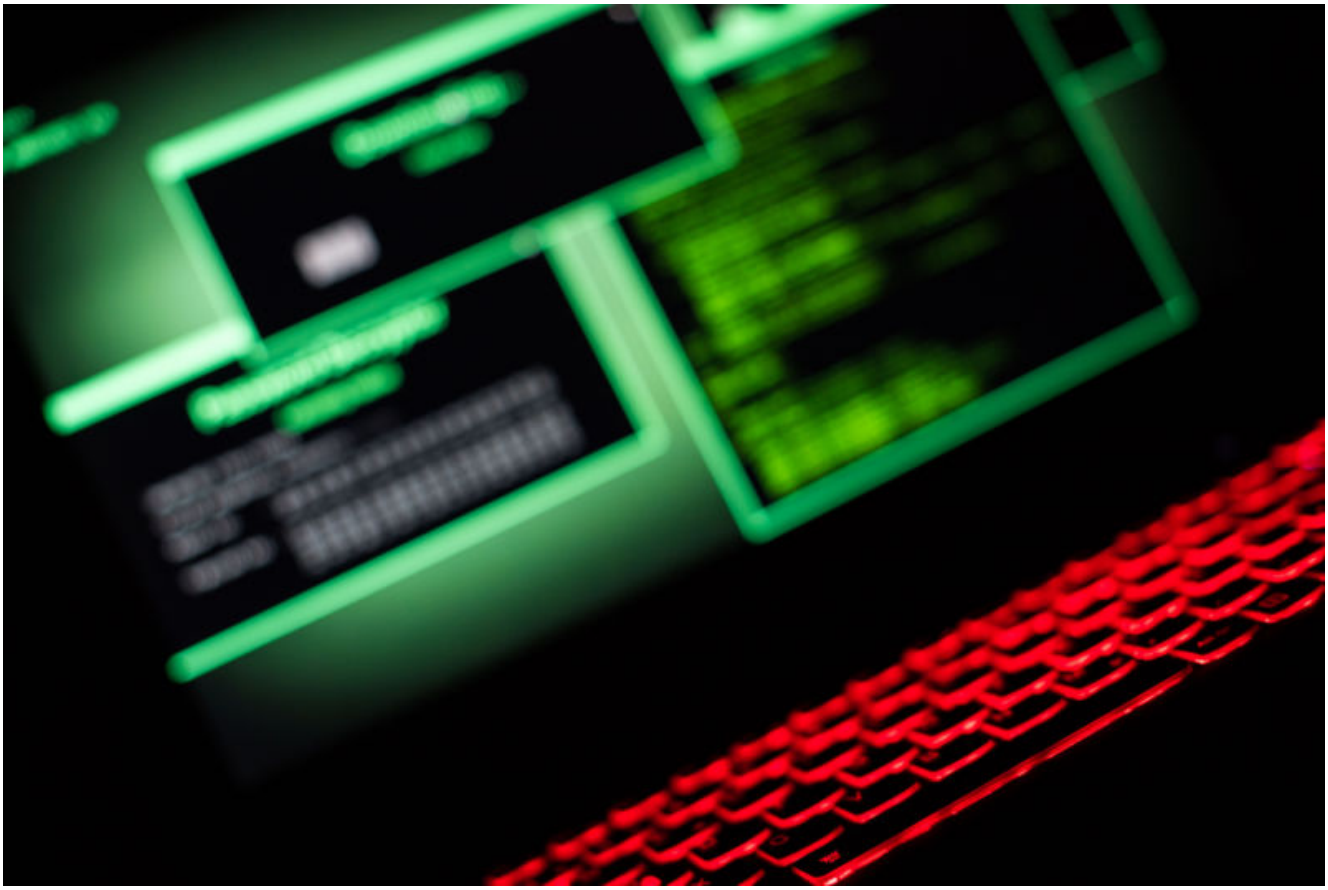
A mystery agent is doxing Iran’s hackers and dumping their code



reader comments

34 with 22 posters participating

Share this story

Nearly three years after the mysterious group called the Shadow Brokers began disemboweling the NSA’s hackers and leaking their hacking tools onto the open Web, Iran’s hackers are getting their own taste of that unnerving experience. For the last month, a mystery person or group has been targeting a top Iranian hacker team, dumping its secret data, tools, and even identities onto a public Telegram channel—and the leak

shows no signs of stopping.

Since March 25, a Telegram channel called Read My Lips or Lab Dookhtegan—which translates from Farsi as "sewn lips"—has been systematically spilling the secrets of a hacker group known as APT34 or OilRig, which researchers have long believed to be working in service of the Iranian government. So far, the leaker or leakers have published a collection of the hackers' tools, evidence of their intrusion points for 66 victim organizations across the world, the IP addresses of servers used by Iranian intelligence, and even the identities and photographs of alleged hackers working with the OilRig group.

"We are exposing here the cyber tools (APT34 / OILRIG) that the ruthless Iranian Ministry of Intelligence has been using against Iran's neighboring countries, including names of the cruel managers, and information about the activities and the goals of these cyber-attacks," read the original message posted to Telegram by the hackers in late March. "We hope that other Iranian citizens will act for exposing this regime's real ugly face!"

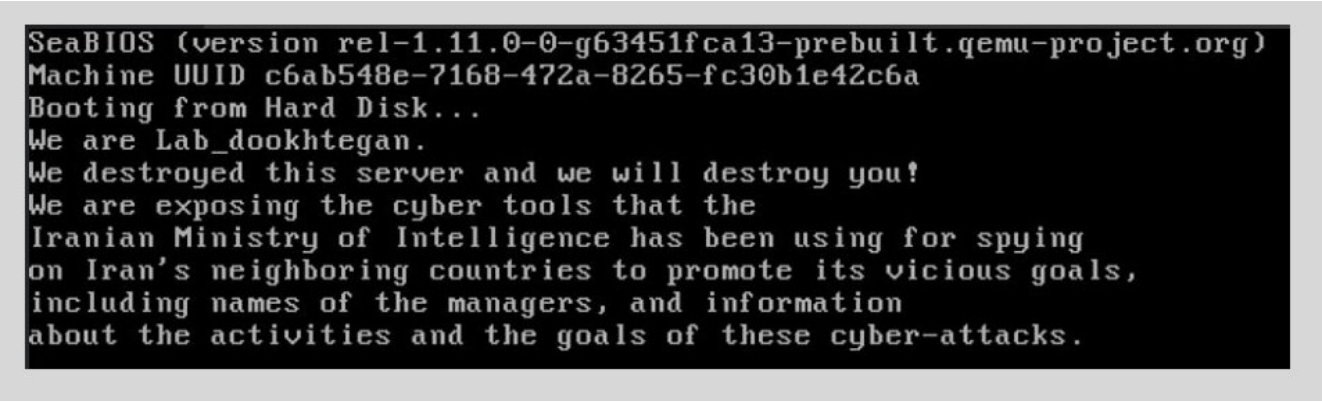
WIRED

The exact nature of the leaking operation and the person or people behind it are anything but clear. But the leak seems intended to embarrass the Iranian hackers, expose their tools—forcing them to build new ones to avoid detection—and even compromise the security and safety of APT34/OilRig's individual members. "It looks like either a disgruntled insider is leaking tools from APT34 operators, or it's a Shadow Brokers—esque sort of entity interested in disrupting operations for this particular group," says Brandon Levene, head of applied intelligence at the security firm Chronicle, which has been analyzing the leak. "They do seem to have something out for these guys. They're naming and shaming, not just dropping tools."

As of Thursday morning, the Read My Lips leakers continued to post names, photos, and even contact details of alleged OilRig members to Telegram, though WIRED couldn't confirm that any of the identified men were actually connected to the Iranian hacker group. "From now on, we will expose every few days the personal information of one of the cursed staff and secret information from the vicious Ministry of Intelligence so to destroy this betraying ministry," a message posted by the leakers on Thursday read.

Chronicle's analysts confirm that at least the hacking tools released are in fact OilRig's hacking tools, as the leakers claimed. They include, for instance, programs called Hypershell and TwoFace, designed to give the hackers a foothold on hacked Web servers. Another pair of tools called PoisonFrog and Glimpse appear to be different versions of a remote-access Trojan called BondUpdater, which researchers at Palo Alto Networks have observed OilRig using since last August.

Beyond leaking those tools, the Read My Lips leaker also claims to have wiped the contents of Iranian intelligence servers and posted screenshots of the message it says it left behind, like the one shown below.



Lab Dookhtegan/Read My Lips

When the Shadow Brokers spilled their collection of secret NSA hacking tools over the course of 2016 and 2017, the results were disastrous: the leaked NSA hacking tools EternalBlue and EternalRomance, for instance, were used in some of the most

destructive and costly cyberattacks in history, including the WannaCry and NotPetya worms. But Chronicle's Levene says that the dumped OilRig tools aren't nearly as unique or dangerous, and the leaked versions of the webshell tools in particular are missing elements that would allow them to be easily repurposed. "It's not really cut and paste," Levene says. "Re-weaponizing of these tools isn't likely to happen."

Another tool included in the leak is described as "DNSpionage" malware and described as "code used for [man-in-the-middle] to extract authentication details" and "code for managing the DNS hijacking." The DNSpionage name and description match an operation that security firms uncovered late last year and have since attributed to Iran. The operation targeted dozens of organizations across the Middle East by altering their DNS registries to redirect all their incoming Internet traffic to a different server where the hackers could silently intercept it and steal any usernames and passwords it included.

But Chronicle's Levene says that, despite appearances, Chronicle doesn't believe the DNSpionage malware in the leak matches the malware used in that previously identified campaign. The two DNS hijacking tools do, however, appear to have similar functionality, and the two hacking campaigns at least shared some victims. The Read My Lips leak includes details of server compromises that OilRig established in a broad array of Middle Eastern networks, from Abu Dhabi's airports to Etihad Airways to the National Security Agency of Bahrain, to the Solidarity Saudi Takaful Company, a Saudi Arabian insurance firm. According to Chronicle's analysis of the leaked victim data, OilRig's targets are as diverse as a South Korean gaming company and a Mexican government agency. But most of the hackers' dozens of victims are clustered in the Middle East, and some were also hit by DNSpionage, Levene says. "We don't see any link with DNSpionage, but there is victim overlap," he says. "If they're not the same, at least their interests are mutual."

For OilRig, the ongoing leak represents an embarrassing setback and operational security breach. But for the security research community, it also offers a rare view into the internals of a state-sponsored hacking group, Levene says. “We don’t often get a look into state-sponsored groups and how they operate,” he says. “This gives us some idea of the scope and scale of this group’s capabilities.”

Even as the Read My Lips leaker reveals the Iranians’ secrets, however, the source of those leaks remains a mystery. And judging by its Telegram claims, it’s only getting started. “We have more secret information about the crimes of the Iranian Ministry of Intelligence and its managers,” reads a message from the group posted last week. “We are determined to continue to expose them. Follow us and share!”

This story originally appeared on WIRED.com.

https://arstechnica.com/?p=1494015