New Iranian hacking tool leaked on Telegram

By Catalin Cimpanu

Published: 2019-06-03 · Archived: 2026-04-06 01:00:58 UTC

A new hacking tool believed to have been in the arsenal of Iranian state hackers has been published today online, in a Telegram channel.

Responsible for this leak is the same individual who, in April, leaked the source code of six other Iranian hacking tools, along with information on past hacked victims, and the real-world identities of members of Iranian government hackers.

This new tool is named Jason and was published online earlier today in the same Telegram channel where the leaker -- going by the name of Lab Dookhtegan -- dumped the six other previous hacking tools.

According to security researcher Omri Segev Moyal, the Jason tool is a GUI utility for brute-forcing Microsoft Exchange email servers using pre-compiled lists of username and password combos.

Jason folder content

Jason hacking tool

Moyal says the tool has been compiled way back in 2015, meaning Iranian hackers have used it for at least four years for their operations.

The six tools that have been previously leaked in April all belonged to an Iranian cyber-espionage group known under codenames such as APT34, Oilrig, or HelixKitten -- believed to be composed of members of the Iranian Ministry of Intelligence (MOIS).

But while the tools leaked in April had been seen in previous attacks before, the Jason tool that was shared today is completely new, at least for the security researchers who analyzed it today.

As for what Lab Dookhtegan has been up to since April, the leaker has been doxxing Iranian intelligence agents, sharing their real names, social media profiles, phone numbers, or personal photos, on an almost daily basis.

While initially it was believed that Lab Dookhtegan was a former insider, the new consensus is that this is the online persona of a foreign intelligence agency who is trying to expose Iranian hacking efforts in attempts to damage the country's cyber-espionage operations, as long as its political connections with neighbors and allies.

But Lab Dookhtegan wasn't the only leaker. In May, another leaker also shared details about another Iranian hacking unit named MuddyWater. The leaker linked MuddyWater operations to an Iranian organization known as the Rana Institute.

Related cybersecurity coverage:

- I2P network proposed as the next hiding spot for criminal operations
- Chinese military to replace Windows OS amid fears of US hacking
- New attack creates ghost taps on modern Android smartphones
- Russian military moves closer to replacing Windows with Astra Linux
- CI build logs continue to expose company secrets
- Wave of SIM swapping attacks hit US cryptocurrency users
- How WannaCry is still launching 3,500 successful attacks per hour **TechRepublic**
- The best identity theft monitoring services for 2019 **CNET**

Editorial standards
