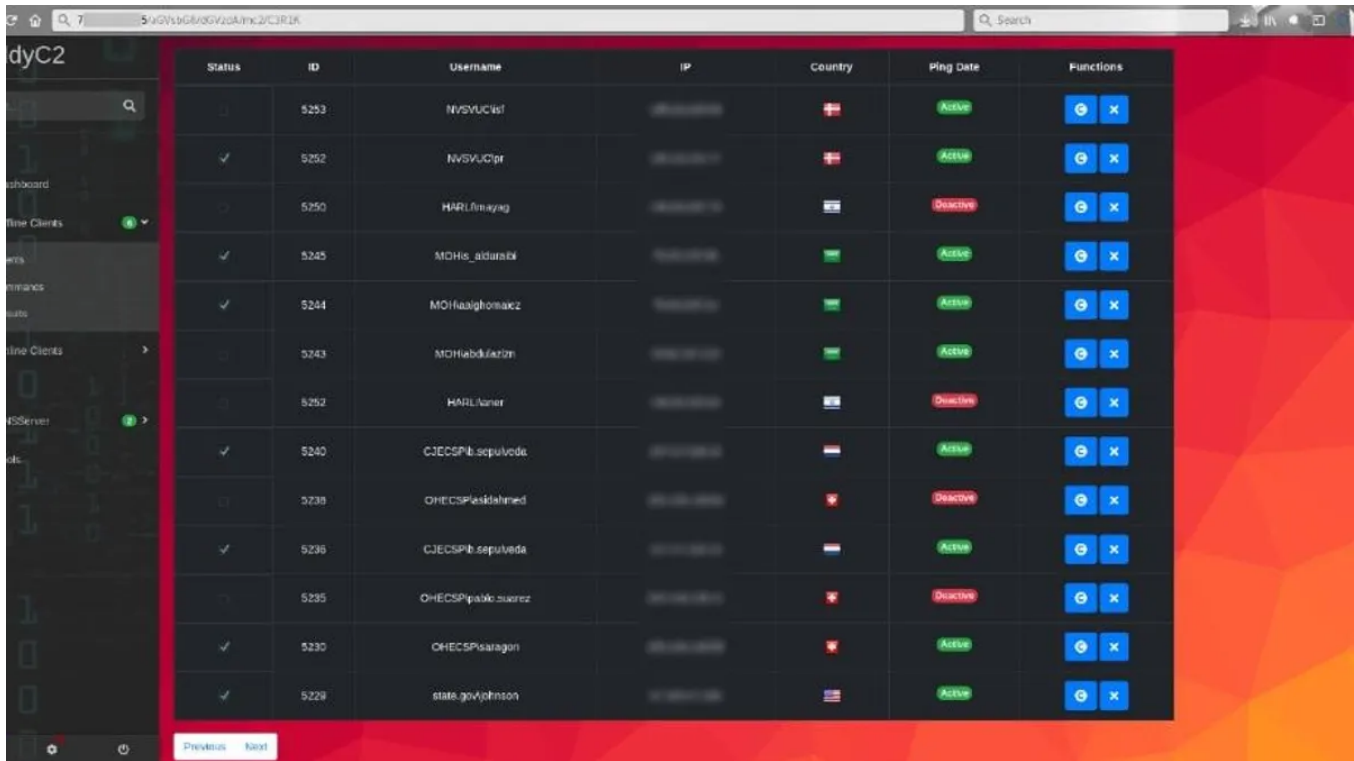


New leaks of Iranian cyber-espionage operations hit Telegram and the Dark Web

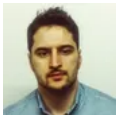
zdnet.com/article/new-leaks-of-iranian-cyber-espionage-operations-hit-telegram-and-the-dark-web/



Status	ID	Username	IP	Country	Ping Date	Functions
✓	5253	NVSVUCIst	[REDACTED]	Denmark	Active	[+] [X]
✓	5252	NVSVUCIpr	[REDACTED]	Denmark	Active	[+] [X]
✓	5250	HARU/finmayag	[REDACTED]	Denmark	Deactive	[+] [X]
✓	5245	MOHis_aidarabli	[REDACTED]	Iran	Active	[+] [X]
✓	5244	MOHaaighomaez	[REDACTED]	Iran	Active	[+] [X]
✓	5243	MOHabdulkarim	[REDACTED]	Iran	Active	[+] [X]
✓	5252	HARU/nanar	[REDACTED]	Denmark	Deactive	[+] [X]
✓	5240	CJECSPH.sepuveda	[REDACTED]	Iran	Active	[+] [X]
✓	5238	OHECSPHesklahmed	[REDACTED]	Iran	Deactive	[+] [X]
✓	5236	CJECSPH.sepuveda	[REDACTED]	Iran	Active	[+] [X]
✓	5235	OHECSPHalic.suarez	[REDACTED]	Iran	Deactive	[+] [X]
✓	5230	OHECSPHsaragon	[REDACTED]	Iran	Active	[+] [X]
✓	5229	state.gov/johnson	[REDACTED]	USA	Active	[+] [X]

Home Innovation Security

This time no hacking tools were released, but the leakers exposed a previously unknown Iranian APT group.



Written by [Catalin Cimpanu](#), Contributor on May 8, 2019

-
-
-
-
-



Two new leaks exposing Iranian cyber-espionage operations have been published online, via Telegram channels and websites on the Dark Web and the public Internet.

See als

[10 dangerous app vulnerabilities to watch out for \(free PDF\)](#)

One leak claims to contain operational data from the MuddyWater hacking group, while the second leak reveals information about a new group identified in official Iranian government documents as the Rana Institute --and currently not linked to any known Iranian cyber-espionage group.

A first leak happened last month

These two leaks come after last month, a mysterious figure using the Lab Dookhtegam pseudonym [dumped on a Telegram channel](#) the source code of several malware strains associated with APT34 (Oilrig), an Iranian government-backed cyber-espionage group.

These two new leaks are different from the first. None of them include source code for malware. Instead, they contain images of source code of unknown origins, images of command and control server backends, and images listing past hacked victims.

Multiple cyber-security firms, such as Chronicle, FireEye, and [Palo Alto Networks](#), confirmed the authenticity of this first leak. Security researchers from ClearSky Security and [Minerva Labs](#) have confirmed this last batch.

With two additional leaks hitting the airwaves, the theory that we are witnessing a well-orchestrated campaign to expose Iran's hacking operations looks now more valid than ever.

The perpetrators may be hoping that the political fallout from exposing Iran's hacks would damage the country's relations with neighbors, foreign political allies, and private sector companies that may rethink their operations and relations with the Iranian government.

MuddyWater leak

This was the second leak to emerge in the public eye after the Lab Dookhtegam leak that occurred on Telegram last month. A group calling themselves the Green Leakers took responsibility.

The group still operates two Telegram channels and two different Dark Web portals where they are selling data they claim is from the operations of the MuddyWater APT (APT = advanced persistent threat, a name used to describe government-backed hacking groups).

 Iran MuddyWaters dark web

Image: ZDNet

Image: ZDNet

Because this data was put up for sale, the leakers did not release any tools for free, like Lab Dookhtegam in the first leak. Instead, they posted:

- images showing the source code of a command and control (C&C) server used by the MuddyWater APT'
- images of MuddyWater C&C server backends --which also included unredacted IP addresses of some of MuddyWater's victims.

Image: ZDNet

Because the leakers have revealed only a small sample of data in the form of screenshots, the jury is still out on the authenticity of this leak; however, it cannot be discounted for the time being.

Both *ZDNet* and Minerva Labs have been keeping an eye on this leak for new developments, but besides having the Telegram channels suspended and having to create new ones, nothing new has been shared for a few days now.

Rana Institute leak

The third leak involving data of Iranian cyber-operations, which *ZDNet* has been tracking for almost a week, occurred on a website on the public Internet written in Persian and on a Telegram channel.

The leakers dumped small snippets from documents labeled "secret" that appeared to have originated with the Iranian Ministry of Intelligence and which described the Rana Institute, a contractor hired for cyber-espionage operations.

Unlike the alleged MuddyWater leak, this one has been verified by security researchers with ClearSky Security, some of the leading experts in Iranian hacking operations.

The leaked documents are a treasure trove of threat intelligence for APT researchers, and expose the activities of a new group whose activities have never been described or even spotted until today, despite being active since 2015.

"These documents contain lists of victims, cyber-attack strategies, alleged areas of access, a list of employees, and screenshots from internal websites relevant to espionage systems," ClearSky said in a [report](#) published a few hours ago.

"The documents shed light on some aspects of the group's activity, notably: tracking Iranians, tracking Iranian citizens outside of Iran, and the group's members."


 Iran Rana leak on the clear web

Image: ZDNet

The website where most of the Rana leak was published contained the personal details of Rana Institute members, along with a slew of information about past campaigns --most of which focused on hacking airlines to retrieve passenger manifests, and hacking travel booking sites to retrieve reservations and payment card numbers.

But in addition to airlines and booking sites, the group also targeted insurance, IT, and telecom firms, as well as government agencies and departments from all over the world.

 Iran Rana target countries

Image: ClearSky Security

Per the leaked documents, the Rana hackers were also asked to develop malware, with the most notable project that was assigned to their team being of developing malware capable of damaging SCADA industrial control systems --similar to Stuxnet or Shamoon.

"The project was unsuccessful and did not achieve its goals despite a large budget," ClearSky researchers said.

Achieving their goals

By exposing the Rana group, it appears that the leakers --whoever they are-- are achieving their goal of sabotaging Iran's cyber-espionage operations.

With hacking tools out in the open and with past campaigns exposed to the whole world, Iran's hacking groups will have to re-tool and focus on new campaigns going forward, potentially delaying any current or planned hacking efforts --exactly what the leakers may have wanted.

Data leaks: The most common sources

Related cybersecurity coverage:
