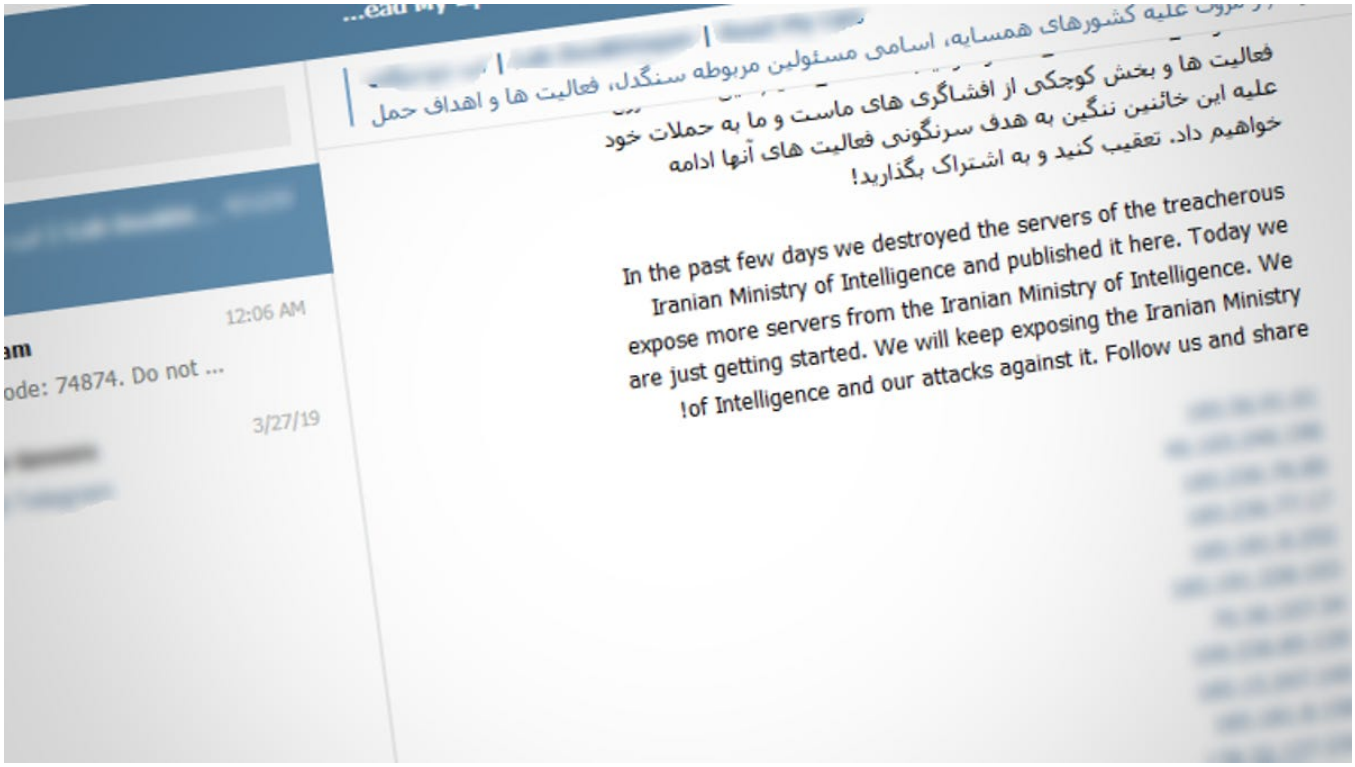
Source code of Iranian cyber-espionage tools leaked on Telegram

zdnet.com/article/source-code-of-iranian-cyber-espionage-tools-leaked-on-telegram/



Tech

Home Tech Security

APT34 hacking tools and victim data leaked on a secretive Telegram channel since last month.

Written by Catalin Cimpanu, Contributor April 17, 2019 at 4:24 p.m. PT

in

-
-
-
-

In an incident reminiscent of the Shadow Brokers leak that exposed the NSA's hacking tools, someone has now published similar hacking tools belonging to one of Iran's elite cyber-espionage units, known as APT34, Oilrig, or HelixKitten.

The hacking tools are nowhere near as sophisticated as the NSA tools leaked in 2017, but they are dangerous nevertheless.

Victim data also dumped online

The tools have been leaked since mid-March on a Telegram channel by an individual using the Lab Dookhtegan pseudonym.

Besides hacking tools, Dookhtegan also published what appears to be data from some of APT34's hacked victims, mostly comprising of username and password combos that appear to have been collected through phishing pages.

ZDNet was previously aware of some of these tools and victim data after this reporter received a tip in mid-March. In a Twitter DM, a Twitter user shared some of the same files that were discovered today on Telegram, and we believe that this Twitter user is the Telegram Lab Dookhtegan persona.


APT34 Twitter

Image: ZDNet

In our Twitter conversation, the leaker claimed to have worked on the group's DNSpionage campaign, but this should be taken with a grain of salt, as the leaker could very well be a member of a foreign intelligence agency trying to hide their real identity while giving more credence to the authenticity of Iran's hacking tools and operations.

Furthermore, ZDNet has also learned that the same Twitter persona had also contacted tens of other reporters and infosec researchers with the same message, in an attempt to promote the leak. Similarly, the same persona has also posted links to some of these hacking tools on public hacking-focused forums. On these forums, he claimed to be selling the hacked files, yet, he never mentioned anything about a price.

Authenticity confirmed

Several cyber-security experts have already confirmed the authenticity of these tools. Chronicle, Alphabet's cyber-security division, confirmed this to ZDNet earlier today.

In the Telegram channel discovered today, the hacker leaked the source code of six hacking tools, and the content from several active backend panels, where victim data had been collected.

Hacking tools:
- Glimpse (newer version of a PowerShell-based trojan that Palo Alto Networks names BondUpdater)
- PoisonFrog (older version of BondUpdater)
- HyperShell (web shell that Palo Alto Networks calls TwoFace)
- HighShell (another web shell)
- Fox Panel (phishing kit)
- Webmask (DNS tunneling, main tool behind DNSpionage)

Besides source code for the above tools, Dookhtegan also leaked on the Telegram channel data taken from victims that had been collected in some of APT34's backend command-and-control (C&C) servers.


APT34 victim data

Image: ZDNet

In total, according to Chronicle, Dookhtegan leaked data from 66 victims, mainly from countries in the Middle East, but also Africa, East Asia, and Europe.

Data was taken from both government agencies, but also from private companies. The two biggest companies named on the Telegram channel are Etihad Airways and Emirates National Oil. A list of the victims (but without company/government agency names) is available here.

Data leaked from each victim varied, ranging from usernames and password combos to internal network servers info and user IPs.

Additionally, Dookhtegan also leaked data about past APT34 operations, listing the IP addresses and domains where the group had hosted web shells in the past, and other operational data.


APT34 web shells

Image: ZDNet

Besides data on past operations, the leaker also doxxed Iranian Ministry of Intelligence officers, posting phone numbers, images, and names of officers involved with APT34 operations. For some officers, Dookhtegan created PDF files containing their names, roles, images, phone numbers, email addresses, and social media profiles.


APT34 doxx

Image: ZDNet

It was clear from the detailed doxing packages that the leaker had a bone to pick with the Iranian Ministry of Intelligence officers, to which he referred many times as "cruel," "ruthless," and "criminal."

"We have more secret information about the crimes of the Iranian Ministry of Intelligence and its managers and we are determined to continue to expose them," Dookhtegan said in a Telegram message posted last week.

The leaker also posted screenshots on the Telegram channel alluding to destroying the control panels of APT34 hacking tools and wiping servers clean.


APT34 destroyed server

Image: ZDNet


APT34 BIOS destroy

Image: ZDNet

The data leaked on this Telegram channel is now under analysis by several cyber-security firms, *ZDNet* was told. It has also made its way on other file sharing sites, such as GitHub.

"It's likely this group will alter their toolset in order to maintain operational status," Brandon Levene, Head of Applied Intelligence at Chronicle, told *ZDNet* today in an email "There may be some copycat activity derived from the leaked tools, but it is unlikely to see widespread use."

This is because the tools aren't sophisticated and aren't top-tier tools like the ones leaked in the Shadow Brokers' NSA leak. Nation-state or criminal groups who will reuse these tools will most likely do it as a smoke-screen or false flag, to mask their operations as APT34.

These were 2017's biggest hacks, leaks, and data breaches

More cybersecurity coverage:

Editorial standards

Show Comments