Apparently Linked Iran Spy Groups Target Middle East

By Eduard Kovacs

Published: 2015-12-08 · Archived: 2026-04-05 17:23:35 UTC

Two Iran-based threat groups that appear to be linked have been conducting cyber espionage campaigns aimed at entities in Iran and other Middle Eastern countries, Symantec reported on Monday.

The threat actors, dubbed by the security firm **Cadelle** and **Chafer**, have been using custom-made backdoors to target individuals and organizations, particularly airlines and telecoms companies, in Iran and Middle Eastern countries such as Afghanistan and Saudi Arabia. One targeted organization was located in the United States.

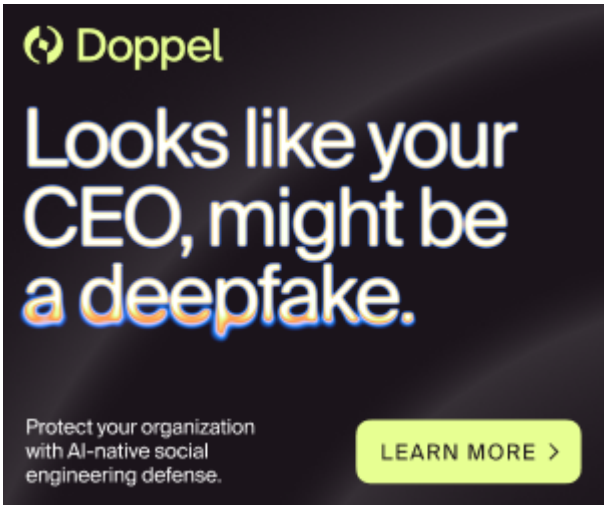
Based on the profiles of the victims, experts believe the attackers are focusing on tracking the movements and communications of certain Iranian individuals. It's not uncommon for Iranians to use anonymous proxy services to circumvent their government's Internet censorship mechanisms and keep their online activities private, and since these types of services have also been attacked, the targets appear to be of interest to an Iranian entity.

Symantec has been monitoring Cadelle and Chafer since July 2014, but command and control (C&C) server information suggests that the groups started their activities as early as 2011.

Cadelle uses a piece of malware identified by Symantec as **Backdoor.Cadelspy**, while Chafer relies on threats detected as **Backdoor.Remexi** and Backdoor.Remexi.B to steal information from infected devices.

Cadelspy, which is delivered via a dropper, is designed to harvest system information and clipboard data, log keystrokes, collect the titles of open windows, record audio, capture screenshots and photos via the webcam, and

steal documents printed by the user.



Remexi is an unsophisticated yet efficient backdoor Trojan that provides attackers a remote shell on the infected computer. Researchers say the threat has been used to collect usernames and passwords that help the attackers gain access to other machines on the victim's network.

Symantec believes each of the threat groups has between five and ten members. Both actors are mainly active on the same days and during the same time of day, which coincide with Iran's working week (Saturday through Thursday) and the country's timezone. An analysis of the Cadelspy backdoor revealed some strings that appear to represent dates written according to the Solar Hijri calendar, which is used in Iran and Afghanistan.

While they haven't seen any overlaps in the infrastructure used by Cadelle and Chafer, experts believe the groups could be directly linked or working separately for a single entity. This is based not only on similar working hours and targets, but also on the fact that infections with both Cadelspy and Remexi have been spotted on the same computers within a small timeframe. In one case, both threats were intermittently active on an organization's systems for a period of more than ten months.

The attackers picked up their activity this year. The highest number of Cadelspy infections were observed by Symantec in September, when nine organizations were hit by the malware. The number of Remexi infections peaked in June when the systems of eight organizations were compromised.

Cadelle and Chafer are not the only threat groups linked to Iran. Security firms have also analyzed the activities of an actor dubbed "Rocket Kitten," which has been targeting entities in the Middle East and Europe. A different threat group, best known for Operation Cleaver, has also been linked to Iran. In fact, Symantec has pointed out that Remexi attacks are reminiscent of Operation Cleaver and they could be a continuation of the campaign.
