# Microsoft: Iran Unit Behind Charlie Hebdo Hack-and-Leak Op

After the French satirical magazine Charlie Hebdo launched a cartoon contest to mock Iran's ruling cleric, a state-backed Iranian cyber unit struck back with a hack-and-leak campaign that was designed to provoke fear with the claimed pilfering of a big subscriber database, Microsoft security researchers say.

The FBI blames the same Iranian cyber operators, Emennet Pasargad, for an influence operation that sought to interfere in the 2020 U.S. presidential election, the tech giant said in a blog published Friday. Iran has in recent years stepped up false-flag cyber operations as a tool for discrediting foes.

Calling itself "**Holy Souls**" and posing as hacktivists, the group claimed in early January to have obtained personal information on 200,000 subscribers and Charlie Hebdo merchandise buyers, according to Microsoft's Digital Threat Analysis Center.

As proof of the data theft, "Holy Souls" released a 200-record sample with names, phone numbers and home and email addresses of Charlie Hebdo subscribers that "could put the magazine's subscribers at risk for online or physical targeting" by extremists. The group then advertised the supposed complete data cache on several dark web sites for $340,000.

Microsoft said it did not know whether anyone purchased the cache.

A representative for Charlie Hebdo said Friday that the newspaper would not comment on the Microsoft research. Iran's mission to the United Nations did not immediately respond to a request for comment Friday.

The Jan. 4 sample release coincided with the publication of Charlie Hebdo's cartoon contest issue. Entrants were asked to draw offensive caricatures of Iran's supreme leader, Ayatollah Ali Khamenei.

The French newspaper Le Monde verified multiple victims of the leak from the sample, Microsoft said. The Iranian cyber operators sought to boost news of the hack-and-leak operation — and fuel outrage at the cartoon edition — through fake French "sock-puppet" accounts on social media platforms that included Twitter, Microsoft said.

The operation coincided with verbal attacks by Tehran condemning Charlie Hebdo's "insult."

The provocatively irreverent magazine has a long history of publishing vulgar cartoons which critics consider deeply insulting to Muslims. Two French-born al-Qaida extremists attacked the newspaper's office in 2015, killing 12 cartoonists, and it Charlie Hebdo has been the target of other attacks over the years.

The magazine billed the Khamenei caricature contest as a show of support for nationwide antigovernment protests that have convulsed Iran since the mid-September death of Mahsa Amini, a 22-year-old woman detained by Iran's morality police for allegedly violating the country's strict Islamic dress code.

After the cartoon issue was published, Iran shut down a decades-old French research institute. Last week, it announced sanctions targeting more than 30 European individuals and entities, including three senior Charlie Hebdo staffers. The sanctions are largely symbolic as they bar travel to Iran and allow its authorities to block bank accounts and confiscate

property in Iran.

*Microsoft: Iran Unit Behind Charlie Hebdo Hack-and-Leak Op*