Microsoft Attributes Charlie Hebdo Attack to NEPTUNIUM | Security Insider

Archived: 2026-04-05 16:44:08 UTC

Microsoft Threat Intelligence

Today, Microsoft's Digital Threat Analysis Center (DTAC) is attributing a recent influence operation targeting the satirical French magazine Charlie Hebdo to an Iranian nation-state actor. Microsoft calls this actor NEPTUNIUM, which has also been identified by the U.S. Department of Justice as Emennet Pasargad.

In early January, a previously unheard-of online group calling itself "Holy Souls," which we can now identify as NEPTUNIUM, claimed that it had obtained the personal information of more than 200,000 Charlie Hebdo customers after "gain[ing] access to a database." As proof, Holy Souls released a sample of the data, which included a spreadsheet detailing the full names, telephone numbers, and home and email addresses of accounts that had subscribed to, or purchased merchandise from, the publication. This information, obtained by the Iranian actor, could put the magazine's subscribers at risk of online or physical targeting by extremist organizations.

We believe this attack is a response by the Iranian government to a cartoon contest conducted by Charlie Hebdo. One month before Holy Souls conducted its attack, the magazine announced it would be holding an international competition for cartoons "ridiculing" Iranian Supreme Leader Ali Khamenei. The issue featuring the winning cartoons was to be published in early January, timed to coincide with the eighth anniversary of an attack by two al-Qa'ida in the Arabian Peninsula (AQAP)-inspired assailants on the magazine's offices.

Holy Souls advertised the cache of data for sale for 20 BTC (equal to roughly $340,000 at the time). The release of the full cache of stolen data – assuming the hackers actually have the data they claim to possess – would essentially constitute the mass doxing of the readership of a publication that has already been subject to extremist threats (2020) and deadly terror attacks (2015). Lest the allegedly stolen customer data be dismissed as fabricated, French paper of record Le Monde was able to verify "with multiple victims of this leak" the veracity of the sample document published by Holy Souls.

After Holy Souls posted the sample data on YouTube and multiple hacker forums, the leak was amplified by a concerted operation across several social media platforms. This amplification effort made use of a particular set of influence tactics, techniques and procedures (TTPs) DTAC has witnessed before in Iranian hack-and-leak influence operations.

The attack coincided with criticism of the cartoons from the Iranian government. On January 4, Iranian Foreign Minister Hossein Amir-Abdollahian tweeted: "The insulting and discourteous action of the French publication […] against the religious and political-spiritual authority will not be […] left without a response." That same day, the Iranian Foreign Ministry summoned the French Ambassador to Iran over Charlie Hebdo's "insult." On January 5, Iran shuttered the French Institute for Research in Iran in what the Iranian Foreign Ministry described as a "first step," and said it would "seriously pursue the case and take the required measures."

Source: https://www.microsoft.com/en-us/security/business/security-insider/threat-briefs/iran-response-for-charlie-hebdo-attacks/