

The DOJ indicts Iranians for alleged Trump campaign 'hack-and-leak' scheme

The three hackers, all of whom have ties to Iran's Islamic Revolutionary Guard Corps, allegedly gained access to the accounts of campaign officials using social engineering and spear phishing, a tactic that attempts to trick victims into disclosing sensitive information. They then used the hijacked accounts to steal nonpublic campaign documents and emails, which they shared with the press.

As outlined in the indictment, the US linked the hackers to an Iranian internet service provider, Respina Networks, which allegedly allowed them "unrestricted" internet access outside of Iran. It also goes over how they used a commercial virtual private network (VPN) to create numerous phony domains like "tinyurl.ink" and "mailer-daemon.online," which they eventually used to mislead their victims.

The US is charging the three hackers with wire fraud, material support to a terrorist organization, and conspiracy to obtain information from protected computers. "These hack-and-leak efforts by Iran are a direct assault on the integrity of our democratic processes," Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division said in the press release. "Iranian government actors have long sought to use cyber-enabled means to harm U.S. interests."

<https://www.theverge.com/2024/9/27/24256133/doj-iranian-hackers-donald-trump-campaign>