TechXplore

Hacker claims breach of FBI's critical-infrastructure portal

December 15 2022, by Frank Bajak

An FBI seal is seen on a wall on Aug. 10, 2022, in Omaha, Neb. A hacker who reportedly posed as the CEO of a financial institution claims to have obtained access to the more than 80,000-member database of InfraGard, an FBI-run outreach program that shares sensitive information on national security and cybersecurity threats with public officials and private sector individuals who run U.S. critical infrastructure. Credit: AP Photo/Charlie Neibergall, File

A hacker who reportedly posed as the CEO of a financial institution claims to have obtained access to the more than 80,000-member database of InfraGard, an FBI-run outreach program that shares sensitive information on national security and cybersecurity threats with public officials and private sector actors who run U.S. critical infrastructure.

The hacker posted samples they said were from the database to an online forum popular with cybercriminals last weekend and said they were asking $50,000 for the entire database.

The hacker obtained access to InfraGard's online portal by posing as the CEO of a financial institution, they told independent cybersecurity journalist Brian Krebs, who broke the story. They called the vetting process surprisingly lax.

The FBI declined to comment. Krebs reported that the agency told him it was aware of a potential false account and was looking into the matter.

InfraGard's memberhip is a veritable critical infrastructure Who's Who. It includes business leaders, IT professionals, military, state and local law enforcement and government officials involved in overseeing the safety of everything from the electrical grid and transportation, to health care, pipelines, nuclear reactors, the defense industry, dams and water plants and financial services. Founded in 1996, it is the FBI's largest public-private partnership, with local alliances affiliated with all its field offices. It regularly shares threat advisories from the FBI and the Department of Homeland Security and serves as a behind-closed-doors social media site for select insiders.

The database has the names, affiliations and contact information for tens of thousands of InfraGard users. Krebs first reported its theft on Tuesday.

The hacker, going by the username USDoD on the BreachForums site, said on the site that records of only 47,000 of the forum's members'—slightly more than half—include unique emails. The hacker also posted that the data contained neither Social Security numbers nor dates of birth. Although fields existed in the database for that information, InfraGard's security-conscious users had left them blank.

However, the hacker told Krebs that they had been messaging InfraGard members, posing as the financial institution's CEO, to try to obtain more personal data that could be criminally weaponized.

The AP reached the hacker on the BreachForums site via private message. They would not say whether they had found a buyer for the stolen records or answer other questions. But they did say that Krebs' article "was 100% accurate."

The FBI did not offer an explanation for how the hacker was able to trick it into approving the InfraGard membership. Krebs reported that the hacker had included a contact email address that they controlled—as well as the CEO's real mobile phone number—when applying for InfraGard membership in November.

Krebs quoted the hacker as saying InfraGard approved the application in early December and that they were able to use the email to receive a one-time authentication code.

Once inside, the hacker said, the database information was easy to obtain with a simple software script.

Citation: Hacker claims breach of FBI's critical-infrastructure portal (2022, December 15)

retrieved 28 April 2024 from
https://techxplore.com/news/2022-12-hacker-breach-fbi-critical-infrastructure-portal.html