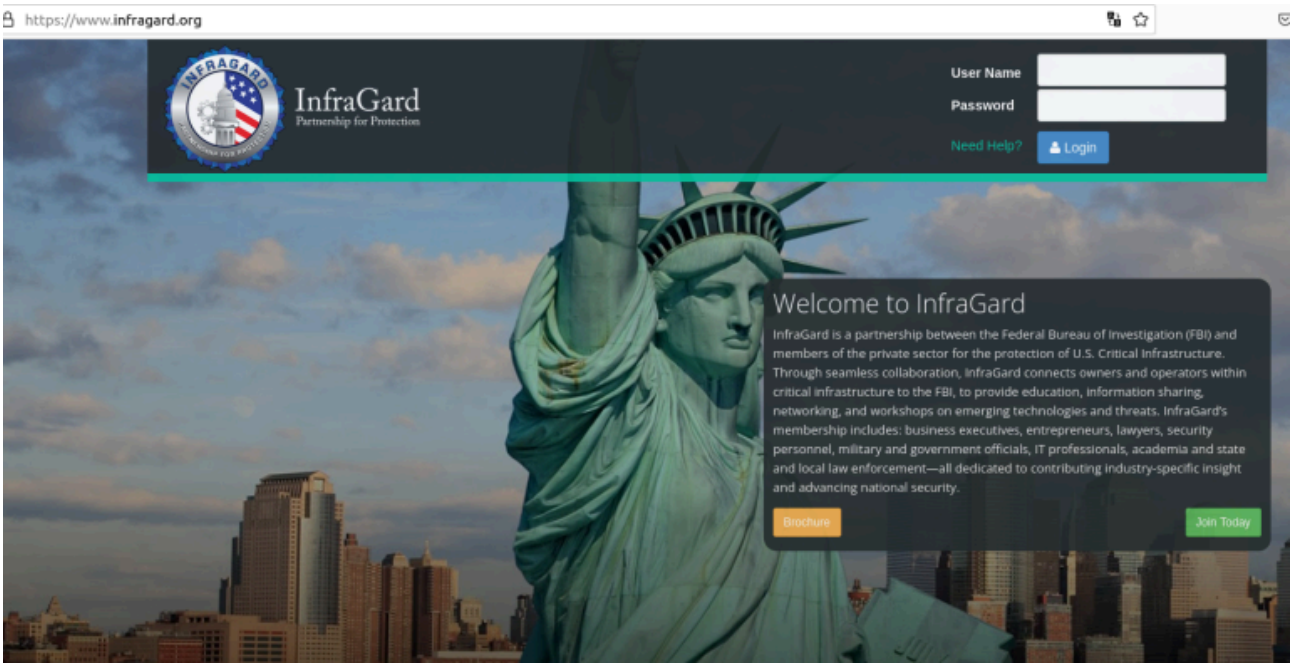
FBI's Vetted Info Sharing Network 'InfraGard' Hacked

Published: 2022-12-14 · Archived: 2026-04-05 16:25:03 UTC

InfraGard, a program run by the **U.S. Federal Bureau of Investigation** (FBI) to build cyber and physical threat information sharing partnerships with the private sector, this week saw its database of contact information on more than 80,000 members go up for sale on an English-language cybercrime forum. Meanwhile, the hackers responsible are communicating directly with members through the InfraGard portal online — using a new account under the assumed identity of a financial industry CEO that was vetted by the FBI itself.



On Dec. 10, 2022, the relatively new cybercrime forum **Breached** featured a bombshell new sales thread: The user database for InfraGard, including names and contact information for tens of thousands of InfraGard members.

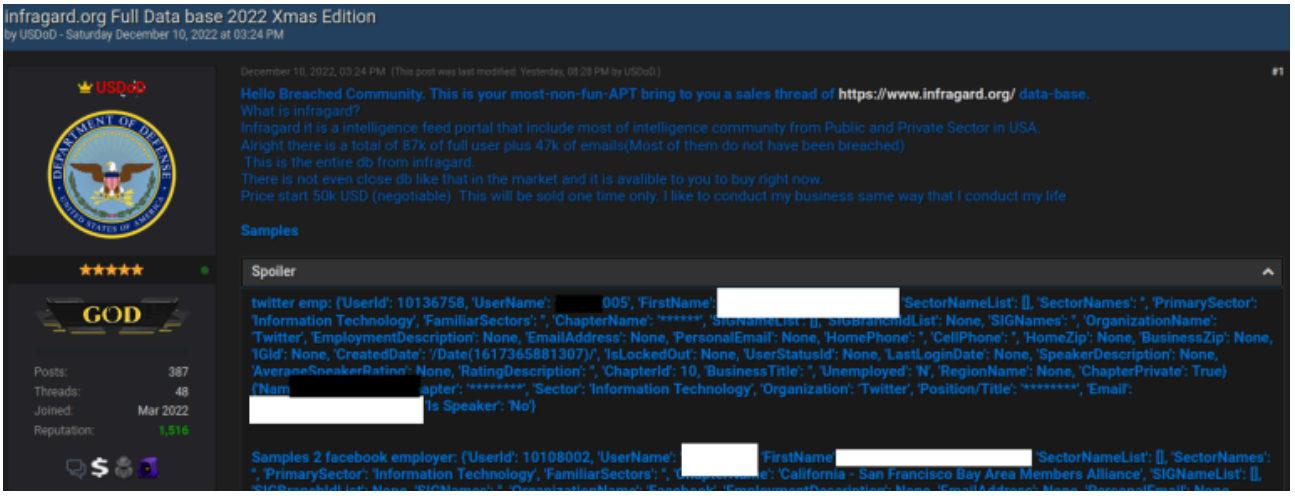
The FBI's InfraGard program is supposed to be a vetted Who's Who of key people in private sector roles involving both cyber and physical security at companies that manage most of the nation's critical infrastructures — including drinking water and power utilities, communications and financial services firms, transportation and manufacturing companies, healthcare providers, and nuclear energy firms.

"InfraGard connects critical infrastructure owners, operators, and stakeholders with the FBI to provide education, networking, and information-sharing on security threats and risks," the FBI's InfraGard fact sheet reads.

In response to information shared by KrebsOnSecurity, the FBI said it is aware of a potential false account associated with the InfraGard Portal and that it is actively looking into the matter.

"This is an ongoing situation, and we are not able to provide any additional information at this time," the FBI said in a written statement.

KrebsOnSecurity contacted the seller of the InfraGard database, a Breached forum member who uses the handle "**USDoD**" and whose avatar is the seal of the **U.S. Department of Defense**.



USDoD's InfraGard sales thread on Breached.

USDoD said they gained access to the FBI's InfraGard system by applying for a new account using the name, Social Security Number, date of birth and other personal details of a chief executive officer at a company that was highly likely to be granted InfraGard membership.

The CEO in question — currently the head of a major U.S. financial corporation that has a direct impact on the creditworthiness of most Americans — told KrebsOnSecurity they were never contacted by the FBI seeking to vet an InfraGard application.

USDoD told KrebsOnSecurity their phony application was submitted in November in the CEO's name, and that the application included a contact email address that they controlled — but also the CEO's real mobile phone number.

"When you register they said that to be approved can take at least three months," USDoD said. "I wasn't expected to be approve[d]."

But USDoD said that in early December, their email address in the name of the CEO received a reply saying the application had been approved (see redacted screenshot to the right). While the FBI's InfraGard system requires multi-factor authentication by default, users can choose between receiving a one-time code via SMS or email.

"If it was only the phone I will be in [a] bad situation," USDoD said. "Because I used the person['s] phone that I'm impersonating."

USDoD said the InfraGard user data was made easily available via an Application Programming Interface (API) that is built into several key components of the website that help InfraGard members connect and communicate with each other.

USDoD said after their InfraGard membership was approved, they asked a friend to code a script in Python to query that API and retrieve all available InfraGard user data.

“InfraGard is a social media intelligence hub for high profile persons,” USDoD said. “They even got [a] forum to discuss things.”

To prove they still had access to InfraGard as of publication time Tuesday evening, USDoD sent a direct note through InfraGard’s messaging system to an InfraGard member whose personal details were initially published as a teaser on the database sales thread.

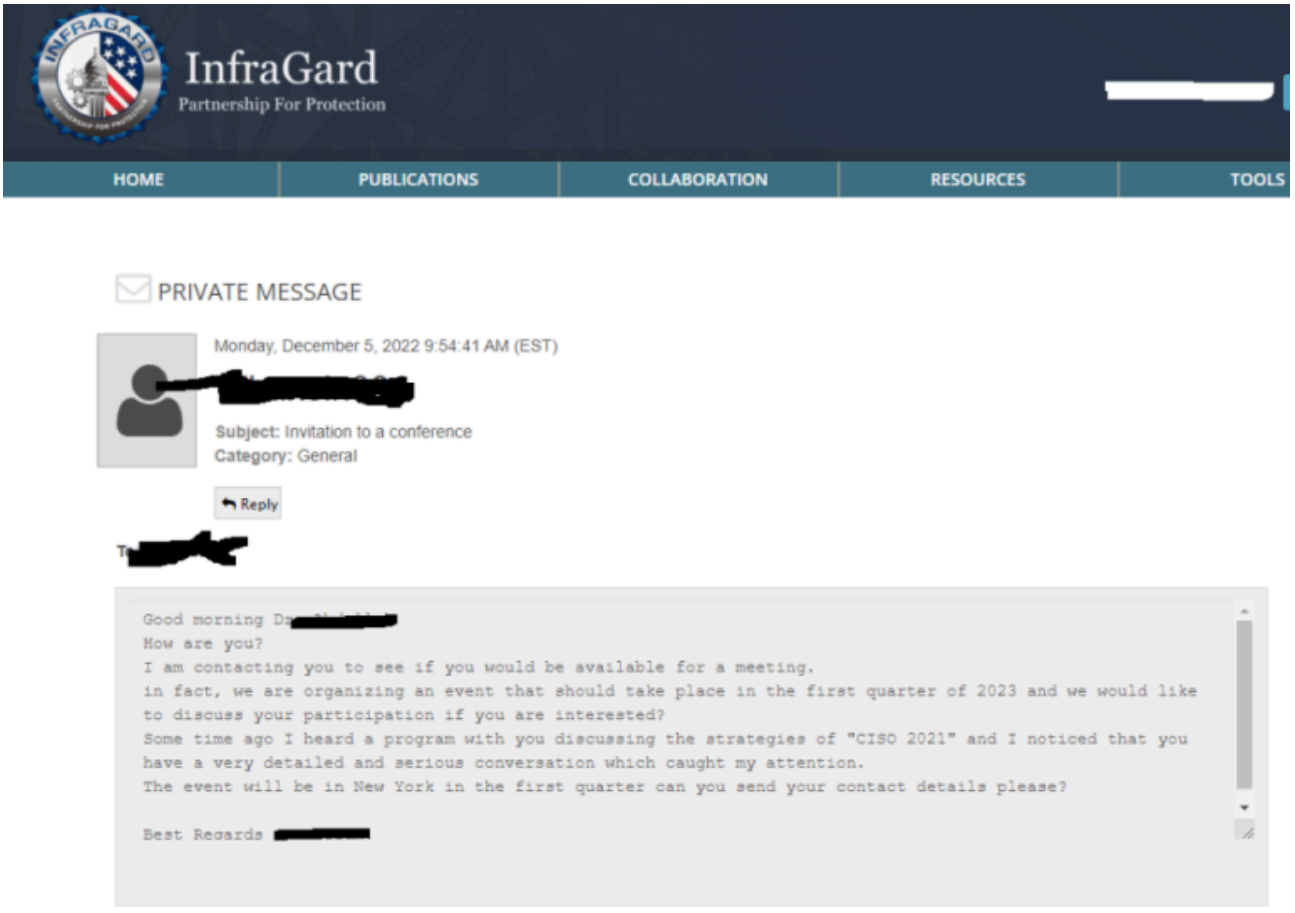
That InfraGard member, who is head of security at a major U.S. technology firm, confirmed receipt of USDoD’s message but asked to remain anonymous for this story.

USDoD acknowledged that their $50,000 asking price for the InfraGard database may be a tad high, given that it is a fairly basic list of people who are already very security-conscious. Also, only about half of the user accounts contain an email address, and most of the other database fields — like Social Security Number and Date of Birth — are completely empty.

“I don’t think someone will pay that price, but I have to [price it] a bit higher to [negotiate] the price that I want,” they explained.

While the data exposed by the infiltration at InfraGard may be minimal, the user data might not have been the true end game for the intruders.

USDoD said they were hoping the imposter account would last long enough for them to finish sending direct messages as the CEO to other executives using the InfraGuard messaging portal. USDoD shared the following redacted screenshot from what they claimed was one such message, although they provided no additional context about it.



A screenshot shared by USDoD showing a message thread in the FBI's InfraGard system.

USDoD said in their sales thread that the guarantor for the transaction would be **Pompompurin**, the administrator of the cybercrime forum Breached. By purchasing the database through the forum administrator's escrow service, would-be buyers can theoretically avoid getting ripped off and ensure the transaction will be consummated to the satisfaction of both parties before money exchanges hands.

Pompompurin has been a thorn in the side of the FBI for years. Their Breached forum is widely considered to be the second incarnation of **RaidForums**, a remarkably similar English-language cybercrime forum shuttered by the U.S. Department of Justice in April. Prior to its infiltration by the FBI, RaidForums sold access to more than 10 billion consumer records stolen in some of the world's largest data breaches.

In November 2021, KrebsOnSecurity detailed how Pompompurin abused a vulnerability in an FBI online portal designed to share information with state and local law enforcement authorities, and how that access was used to blast out thousands of hoax email messages — all sent from an FBI email and Internet address.

Update, 10:58 p.m. ET: Updated the story after hearing from the financial company CEO whose identity was used to fool the FBI into approving an InfraGard membership. That CEO said they were never contacted by the FBI.

Update, 11:15 p.m. ET: The FBI just confirmed that it is aware of a potential false account associated with the InfraGard portal. The story now includes their full statement.

This is a developing story. Updates will be noted here with timestamps.
