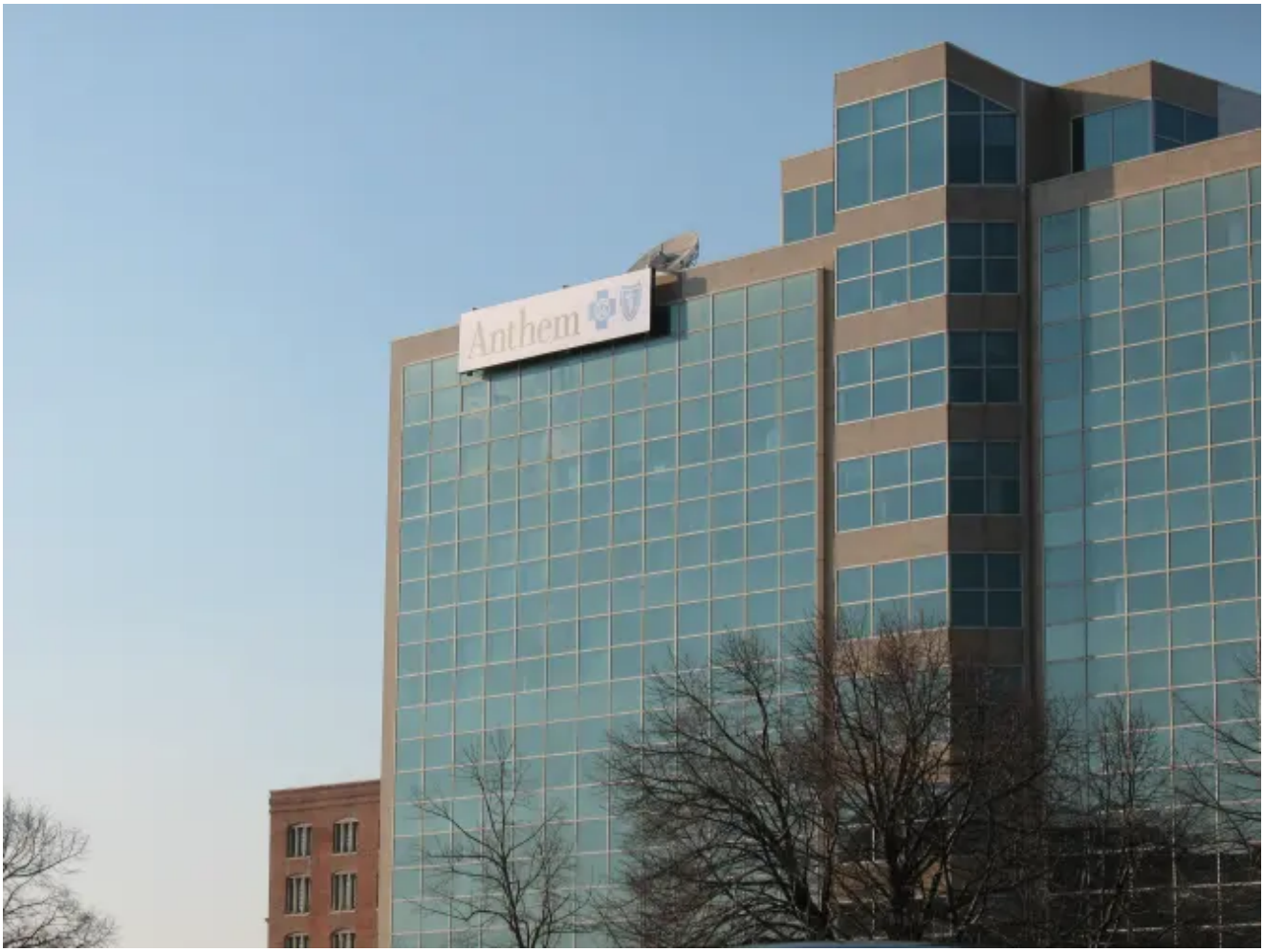
Related news

cyberscoop.com/anthem-breach-indictment-chinese-national/

May 9, 2019



government

Chinese national indicted for 2015 Anthem breach

(Matthew Hurst / Flickr)
Written by Sean Lyngaas
May 9, 2019 | CYBERSCOOP
A federal grand jury has indicted a Chinese national for being part of an “extremely sophisticated hacking group” that breached U.S. businesses, including the seminal 2015 hack of health insurer Anthem that exposed personal information on nearly 79 million people.

The indictment unsealed Thursday alleges that 32-year-old Fujie Wang breached Anthem and three other unnamed U.S. businesses, scoping out personally identifiable information (PII) and confidential business data.

Another person identified only as John Doe was also indicted.

The two defendants were charged with conspiracy to commit fraud and “related activity in relation to computers and identity theft,” along with conspiracy to commit wire fraud and “two substantive counts of intentional damage to a protected computer,” the Department of Justice announced.

The Anthem breach compromised sensitive personal data, including Social Security numbers, and prompted a record $16 million settlement with the U.S. government over potential Health Insurance Portability and Accountability Act (HIPAA) violations.

The indictment, unsealed in a federal court in Indianapolis — where Anthem is headquartered — outlines how the defendants allegedly infiltrated their targets. They went after employees of the victim organizations with spearphishing emails, which were used to install backdoor tools for remote access to networks, according to the indictment. After locating the information they wanted to steal, Wang and Doe allegedly extracted the data by bundling it in encrypted archiving files and then routing the data through multiple computers back to China.

In the case of Anthem, Wang and Doe bided their time in devising their attack, according to prosecutors, surveying the health insurer’s enterprise data center, which housed the PII, throughout October and November 2014.

Matt Gorham, assistant director of the FBI’s Cyber Division, credited the communication between victim organizations and the bureau in tracking down the alleged culprits.

“Because the victim companies promptly notified the FBI of malicious cyber activity, we were able to successfully investigate and identify the perpetrators of this large-scale, highly sophisticated scheme,” Gorham said in a statement.

An Anthem spokesperson could not immediately be reached for comment.