THE UNITED STATES DEPARTMENT of JUSTICE
STICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Thursday, May 9, 2019

Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People

A federal grand jury returned an indictment unsealed today in Indianapolis, Indiana, charging a Chinese national as part of an extremely sophisticated hacking group operating in China and targeting large businesses in the United States, including a computer intrusion and data breach of Indianapolis-based health insurer Anthem Inc. (Anthem).

Assistant Attorney General Brian A. Benczkowski of the Justice Department's Criminal Division, U.S. Attorney Josh Minkler for the Southern District of Indiana, Assistant Director Matt Gorham of the FBI's Cyber Division and Special Agent in Charge Grant Mendenhall of the FBI's Indianapolis Field office made the announcement.

The four-count indictment alleges that Fujie Wang (王 福 杰 in Chinese Hanzi), 32, and other members of the hacking group, including another individual charged as John Doe, conducted a campaign of intrusions into U.S.-based computer systems. The indictment alleges that the defendants gained entry to the computer systems of Anthem and three other U.S. businesses, identified in the indictment as Victim Business 1, Victim Business 2 and Victim Business 3. As part of this international computer hacking scheme, the indictment alleges that beginning in February 2014, the defendants used sophisticated techniques to hack into the computer networks of the victim businesses without authorization, according to the indictment. They then installed malware and tools on the compromised computer systems to further compromise the computer networks of the victim businesses, after which they identified data of interest on the compromised computers, including personally identifiable information (PII) and confidential business information, the indictment alleges.

"The allegations in the indictment unsealed today outline the activities of a brazen China-based computer hacking group that committed one of the worst data breaches in history," said Assistant Attorney General Benczkowski. "These defendants allegedly attacked U.S. businesses operating in four distinct industry sectors, and violated the privacy of over 78 million people by stealing their PII. The Department of Justice and our law enforcement partners are committed to protecting PII, and will aggressively prosecute perpetrators of hacking schemes like this, wherever they occur."

"The cyber attack of Anthem not only caused harm to Anthem, but also impacted tens of millions of Americans," said U.S. Attorney Minkler. "This wanton violation of privacy will not stand, and we are committed to bringing those responsible to justice. I would also like to thank Anthem for its timely and substantial cooperation with our investigation."

"This case is significant not only because it showcases the FBI's cyber investigative capabilities, but also because it highlights the importance of FBI and private industry relationships," said Assistant Director Matt Gorham. "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. The FBI is committed to investigating cyber-attacks that compromise American industry and the American people. As we did in this case, we will work side by side with victim companies to ensure justice is served."

"Anthem's cooperation and openness in working with the FBI on the investigation of this sophisticated cyber-attack was imperative in allowing for the identification of these individuals. This also speaks to the strong partnerships the FBI has with the private sector, as well as the tenacity and global reach of the Bureau," said Special Agent in Charge Grant Mendenhall. "It should also be noted that the speed with which Anthem initially notified the FBI of the intrusion on their networks was also a key factor in being able to determine who was responsible for the breach and should serve as an example to other organizations that might find themselves in a similar situation."

The indictment further alleges that the defendants then collected files and other information from the compromised computers and then stole this data. As part of the computer intrusion and data breach of Anthem, the defendants identified and ultimately stole data concerning approximately 78.8 million persons from Anthem's computer network, including names, health identification numbers, dates of birth, Social Security numbers, addresses, telephone numbers, email addresses, employment information and income data, according to the indictment.

Wang and Doe are charged with one count of conspiracy to commit fraud and related activity in relation to computers and identity theft, one count of conspiracy to commit wire fraud, and two substantive counts of intentional damage to a protected computer.

According to the indictment, the defendants used extremely sophisticated techniques to hack into the computer networks of the victim businesses. These techniques included the sending of specially-tailored "spearfishing" emails with embedded hyperlinks to employees of the victim businesses. After a user accessed the hyperlink, a file was downloaded which, when executed, deployed malware that would compromise the user's computer system by, in pertinent part, installing a tool known as a backdoor that would provide remote access to that computer system through a server controlled by the defendants.

The defendants sometimes patiently waited months before taking further action, eventually engaging in reconnaissance by searching the network for data of interest, according to the indictment. This data included PII and confidential business information. The indictment alleges that the defendants accessed the computer network of Anthem without authorization for the purpose of conducting reconnaissance on Anthem's enterprise data warehouse, a system that stores a large amount of PII, on multiple occasions in October and November 2014.

The indictment further alleges that once the data of interest had been identified and located, the defendants then collected the relevant files and other information from the compromised computers using software tools. The defendants then allegedly stole the data of interest by placing it into encrypted archive files and then sending it through multiple computers to destinations in China. The indictment alleges that on multiple occasions in January 2015, the defendants accessed the computer network of Anthem, accessed Anthem's enterprise data warehouse, and transferred encrypted archive files containing PII from Anthem's enterprise data warehouse from the United States to China.

Finally, the defendants allegedly then deleted the encrypted archive files from the computer networks of the victim businesses, in an attempt to avoid detection. In late January 2015, the defendants deleted certain archive files containing PII that they had previously transferred from Anthem's enterprise data warehouse.

Defendant Wang is specifically alleged to have controlled two domain names connected to the criminal activity. According to the indictment, one of these domain names was associated with a backdoor used in the intrusion victimizing Victim Business 1, and the other was associated by Wang with a server used to create an email account used to conduct spearfishing attacks against employees of Victim Business 3.

This case was investigated by the FBI's Indianapolis Field Office. Senior Counsel William A. Hall, Jr. of the Criminal Division's Computer Crime and Intellectual Property Section and Assistant U.S. Attorney and Deputy Chief of the General Crimes Unit Steven D. DeBrota of the Southern District of Indiana are prosecuting the case. Significant assistance was provided by the Justice Department's National Security Division and the Criminal Division's Office of International Affairs.

Charges contained in an indictment are merely allegations, and the defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

Attachment(s):

Download Anthem Indictment
Download Fujie-Wang Wanted Poster

Topic(s):
Cyber Crime

Component(s):
Criminal Division
Federal Bureau of Investigation (FBI)
USAO - Indiana, Southern

Press Release Number:
19-502

Updated May 9, 2019