US says Chinese military stole masses of Americans' data

10 February 2020, by Eric Tucker and Michael Balsamo

Attorney General William Barr speaks during a news conference, Monday, Feb. 10, 2020, at the Justice Department in Washington, as Principal Associate Deputy Attorney General Seth Ducharm looks on. Four members of the Chinese military have been charged with breaking into the networks of the Equifax credit reporting agency and stealing the personal information of tens of millions of Americans, the Justice Department said Monday, blaming Beijing for one of the largest hacks in history. (AP Photo/Jacquelyn Martin)

Four members of the Chinese military have been charged with breaking into the computer networks of the Equifax credit reporting agency and stealing the personal information of tens of millions of Americans, the Justice Department said Monday, blaming Beijing for one of the largest hacks in history to target consumer data.

The hackers in the 2017 breach stole the personal information of roughly 145 million Americans, collecting names, addresses, Social Security and driver's license numbers and other data stored in the company's databases. The intrusion damaged the company's reputation and underscored China's increasingly aggressive and sophisticated intelligence-gathering methods.

"The scale of the theft was staggering," Attorney General William Barr said Monday in announcing the indictment. "This theft not only caused significant financial damage to Equifax, but invaded the privacy of many millions of Americans, and imposed substantial costs and burdens on them as they have had to take measures to protect against identity theft."

The case is the latest U.S. accusation against Chinese hackers suspected of breaching networks of American corporations, including steel manufacturers, a hotel chain and a health insurer. It comes as the Trump administration has warned against what it sees as the growing political and economic influence of China, and efforts by Beijing to collect data for financial and intelligence purposes and to steal research and innovation.

The indictment arrives at a delicate time in relations between Washington and Beijing. Even as President Donald Trump points to a preliminary trade pact with China as evidence of his ability to work with the Communist government, other members of his administration have been warning against cybersecurity and surveillance risks posed by China, especially as the tech giant Huawei seeks to become part of new, high-speed 5G wireless networks across the globe.

This July 21, 2012, file photo shows signage at the corporate headquarters of Equifax Inc. in Atlanta. The deadline to seek cash payments and claim free services as part of Equifax's $700 million settlement over a massive data breach is Wednesday, Jan. 22, 2020. (AP Photo/Mike Stewart, File)

Attorney General William Barr, right, next to FBI Deputy Director David Bowdich, speaks during a news conference, Monday, Feb. 10, 2020, at the Justice Department in Washington. Four members of the Chinese military have been charged with breaking into the networks of the Equifax credit reporting agency and stealing the personal information of tens of millions of Americans, the Justice Department said Monday, blaming Beijing for one of the largest hacks in history. (AP Photo/Jacquelyn Martin)

Experts and U.S. officials say the Equifax theft is consistent with the Chinese government's interest in accumulating as much information about Americans as possible.

The data can be used by China to target U.S. government officials and ordinary citizens, including possible spies, and to find weaknesses and vulnerabilities that can be exploited—such as for purposes of blackmail. The FBI has not seen that happen yet in this case, said Deputy Director David Bowdich, though he said it "doesn't mean it will or will not happen in the future."

"We have to be able to recognize that as a counterintelligence issue, not a cyber issue," Bill Evanina, the U.S. government's top counterintelligence official, said of the Equifax case.

The four accused hackers are suspected members of the People's Liberation Army, an arm of the Chinese military that was blamed in 2014 for a series of intrusions into American corporations.

Prosecutors say they exploited a software vulnerability to gain access to Equifax's computers, obtaining log-in credentials that they used to navigate databases and review records. They also took steps to cover their tracks, the indictment says, wiping log files on a daily basis and routing traffic through about three dozen servers in nearly 20 countries.

Besides stealing personal information, the hackers also made off with some of the company's sensitive trade secrets, including database designs, law enforcement officials said.

Equifax, headquartered in Atlanta, maintains a massive repository of consumer information that it sells to businesses looking to verify identities or assess creditworthiness. All told, the indictment says, the company holds information on hundreds of millions of people in America and abroad.

None of the accused hackers is in U.S. custody. But officials nonetheless hope criminal charges can be a deterrent to foreign hackers and a warning to other countries that American law enforcement has the capability to pinpoint individual culprits. Even so, while China and the U.S. committed in 2015 to halt acts of cyber espionage against each other, the Equifax intrusion and others like it make clear that Beijing has continued its operations.

A spokesperson for the Chinese Embassy in

Washington did not return an email seeking comment Monday.

The case resembles a 2014 indictment that accused five members of the PLA of hacking into American corporations to steal trade secrets. U.S. authorities also suspect China in the 2015 breach of the federal Office of Personnel Management and of intrusions into the Marriott hotel chain and health insurer Anthem.

Attorney General William Barr speaks during a news conference, Monday, Feb. 10, 2020, at the Justice Department in Washington. Four members of the Chinese military have been charged with breaking into the networks of the Equifax credit reporting agency and stealing the personal information of tens of millions of Americans, the Justice Department said Monday, blaming Beijing for one of the largest hacks in history. (AP Photo/Jacquelyn Martin)

Such hacks "seem to deliberately cast a wide net" so that Chinese intelligence analysts can get deep insight into the lives of Americans, said Ben Buchanan, a Georgetown University scholar and author of the upcoming book "The Hacker and the State."

"This could be especially useful for counterintelligence purposes, like tracking American spies posted to Beijing," Buchanan said.

Barr, who at an event last week warned of Beijing's aspirations of economic dominance, said Monday the U.S. has long "witnessed China's voracious appetite for the personal data of Americans."

"This kind of attack on American industry is of a piece with other Chinese illegal acquisitions of sensitive personal data," Barr said.

The criminal charges, which include conspiracy to commit computer fraud and conspiracy to commit economic espionage, were filed in federal court in Atlanta.

Attorney General William Barr, left, arrives to speak, next to Assistant Attorney General John Demers and U.S. Attorney for the Northern District of Georgia Byung "BJay" Pak, right, during a news conference, Monday, Feb. 10, 2020, at the Justice Department in Washington. Four members of the Chinese military have been charged with breaking into the networks of the Equifax credit reporting agency and stealing the personal information of tens of millions of Americans, the Justice Department said Monday, blaming Beijing for one of the largest hacks in history. (AP Photo/Jacquelyn Martin)

Equifax last year reached a $700 million settlement over the data breach, with the bulk of the funds intended for consumers affected by it.

Equifax officials told the Government Accountability Office the company made many mistakes, including having an outdated list of computer systems administrators. The company didn't notice the intruders targeting its databases for more than six weeks. Hackers exploited a known security

vulnerability that Equifax hadn't fixed.

While company stock has recovered, Equifax's reputation has not fully. The company was dragged in front of Congress no less than four times to explain what happened.

The company is about to start paying out claims on its $700 million settlement, of which more claimants have opted in to getting a cash settlement than accept credit counseling. So many claims have been made for the cash that the lawyers suing Equifax and the Federal Trade Commission have warned claimants that the chance of getting the full cash value of the settlement was unlikely.