



BUSINESS DAY

Chinese Businessman Is Charged in Plot to Steal U.S. Military Data

By **MATT APUZZO** JULY 11, 2014

WASHINGTON — A Chinese businessman in Canada hacked into Boeing's computers and stole information about United States military aircraft and weapons, the Justice Department said on Friday, describing a corporate espionage case that is unusual for the huge amount of data involved.

The businessman, Su Bin, spent years taking data from Boeing, the Federal Bureau of Investigation said in court documents, and working with two unidentified contacts in China sought to sell the information to companies there.

There is no indication that the Chinese government orchestrated the attacks, or that anyone breached classified systems or stole classified information. But the assault on one of the nation's most sophisticated military contractors is a reminder that even seemingly safe computer systems are vulnerable.

In March, Chinese hackers broke into computers that stored the personal information of all United States government employees. In May, the Justice Department accused five Chinese officials with hacking into Westinghouse Electric, United States Steel and other companies.

Mr. Bin owned a Chinese aviation company called Lode Tech that had offices in Canada, where Mr. Bin lived. He was arrested there on June 28, the F.B.I. said, and is expected in court there later this month for a bail

hearing.

The Justice Department is seeking his extradition to the United States. He is charged with unauthorized computer access.

“We remain deeply concerned about cyber-enabled theft of sensitive information and we have repeatedly made it clear that the United States will continue using all the tools our government possesses to strengthen cybersecurity and confront cybercrime,” Marc Raimondi, a Justice Department spokesman, said.

Court documents do not say how the hackers breached Boeing’s computers. But Noel A. Neeman, the F.B.I. agent who wrote the document, describes a general strategy that will be familiar to anyone whose email or social media accounts have been compromised: Hackers send an email with a link to a malicious piece of code. Clicking on that link gives hackers access to computer systems.

While court documents quote from emails describing elaborate hacking schemes and successful efforts to obtain aircraft schematics, Mr. Neeman writes that those accounts “could have been exaggerated.” The hackers’ description of Boeing’s computer network is not accurate and the confidential design information they claim to have seized was stored across multiple servers, including two on Air Force bases, Mr. Neeman writes.

A Boeing spokeswoman said the company was cooperating with the investigation.

Boeing was first breached in January 2010, and according to emails obtained by the F.B.I., more than 65 gigabytes of data was stolen over the next two years. The primary focus was Boeing’s C-17 military cargo plane. The documents also indicate that the three men stole a comparatively small amount of information related to Lockheed Martin’s F-22 and F-35 jets. It is not clear from the documents how that breach occurred.

Boeing will cease production of the C-17 next year after two decades building the planes.

The Chinese government is developing its own cargo plane, which is similar in some respects to the C-17.

The court documents describe efforts to sell the seized information in China, including to state-owned companies, but it does not say whether the hackers succeeded. No defense lawyer is named in the court documents, which were filed in Los Angeles.

Computer breaches are a major source of friction between the United States and China. The United States says it hacks computers only to gain national security information, while China uses it to gain an economic advantage.

But evidence revealed by Edward J. Snowden, the former National Security Agency contractor, shows the N.S.A. went deep into the computer systems of Huawei, a major maker of computer network equipment, and ran many programs to intercept the conversations of Chinese leaders and the military.

A version of this article appears in print on July 12, 2014, on page B1 of the New York edition with the headline: Chinese Businessman Is Charged in Plot to Steal U.S. Military Data.