Chinese national admits hacking US defense firms

March 23 2016

A Chinese national pleaded guilty Wednesday to charges stemming from the hacking of trade secrets from US defense contractors, including plans for transport and fighter jets, officials said.

Su Bin, 50, had been charged in a 2014 indictment with hacking into the computer networks of Boeing and other contractors, as part of a scheme to steal plans for the F-22 and F-35 fighter jets and C-17 transport aircraft.

In a plea agreement filed in a California federal court, Su admitted to conspiring with two unnamed persons in China from October 2008 to March 2014 to gain unauthorized access to the computer networks of defense firms to obtain "sensitive military information and to export that information illegally from the United States to China," the Justice Department said in a statement.

Court documents did not indicate to whom Su was sending the plans, but the case highlighted growing concerns in the United States about Chinese hacking of American trade secrets, a topic which has been addressed by President Barack Obama and his Chinese counterpart Xi Jinping.

"Su Bin admitted to playing an important role in a conspiracy, originating in China, to illegally access sensitive military data, including data relating to military aircraft that are indispensable in keeping our military personnel safe," Assistant Attorney General John Carlin said.

"This plea sends a strong message that stealing from the United States and our companies has a significant cost; we can and will find these criminals and bring them to justice."

Arrested in Canada

Su was initially arrested in Canada in July 2014 on a warrant based on a US request. He waived extradition and was sent to the United States in February 2016.

Su Bin, also known as Stephen Su and Stephen Subin, was a China-based businessman in the aviation and aerospace fields.

According to prosecutors, Su would e-mail the co-conspirators pictures and other documents, with guidance regarding what persons, companies and technologies to target for hacking.

After the data was stolen, Su translated the information from English into Chinese.

Su and his co-conspirators each wrote, revised and emailed reports about the information and technology they had acquired "to the final beneficiaries of their hacking activities," the Justice Department said.

Sentencing was set for July 13. Su faces a maximum penalty of five years in prison and a fine of $250,000 or twice the gross gain from the offense.

Last September, Obama and Xi addressed the issue of cybertheft at their Washington meeting, and both leaders agreed it was unacceptable.

Obama said after the talks that "we've agreed that neither the US or the Chinese government will conduct or knowingly support cyber-enabled

theft of intellectual property."

Xi said "China strongly opposes and combats the theft of commercial secrets and other kinds of hacking attacks."

Analysts have been cautious, warning that it remained to be seen if Beijing would live up to its agreement to crack down on hacking.

One report by a cybersecurity firm said hackers linked to the Chinese government kept up efforts to break into US computer networks shortly after the cybersecurity agreement.