FBI: Chinese national supplied rare, malicious malware

August 25 2017, by Michael Balsamo

A Chinese national has been charged in California with distributing a type of computer malware that has been linked to attacks on U.S. businesses and to the theft of personnel records of millions of U.S. government employees, authorities said.

Defendant Yu Pingan, 36, knew the rare malware known as "Sakula" would be used to hack U.S. companies, the FBI said in court documents obtained Friday.

The malware has also been linked to hacks at the U.S. Office of Personnel Management in 2014 and 2015, when hackers accessed massive amounts of information from security clearance forms of federal workers and contractors.

The court filing against Yu does not specifically mention those hacks. U.S. officials have said the Chinese government is responsible for those breaches.

Asked about the arrest of Yu, Hua Chunying, a Chinese foreign ministry spokeswoman in Beijing, said at a regular briefing that she was unaware of the situation.

But, she added, "China has a clear and consistent position in fighting against all kinds of cybercrimes. Also, we will proactively protect the legitimate rights and interest of overseas Chinese nationals."

Yu worked with unidentified co-conspirators in China to "acquire and use malicious software tools, some of which were rare variants previously unidentified by the FBI and information security community,'" the criminal complaint said.

Yu, a native of Shanghai, was arrested Monday night at Los Angeles International Airport and is due back in court next month. His attorney, Michael Berg, did not immediately respond to a request for comment.

The software was used to target companies based in Massachusetts, Arizona, San Diego and Los Angeles from 2012 to 2014, federal officials said.

An FBI agent wrote in an affidavit that "the novelty and rarity of this malware is evidence that only a small group of hackers knew of it and that they were working together."