FU QIANG

Racketeering Conspiracy; Conspiracy; Identity Theft; Aggravated Identity Theft; Access Device Fraud; Obtaining Information by Unauthorized Access to Protected Computers; Intentionally Causing Damage to Protected Computers; Threatening to Damage a Protected Computer; Money Laundering

DESCRIPTION

Alias: StandNY	
Date(s) of Birth Used: March 11, 1982	**Place of Birth:** China
Hair: Black	**Eyes:** Brown
Sex: Male	**Race:** Asian
Nationality: Chinese	**Languages:** Chinese

REMARKS

FU Qiang has ties to Chengdu, China.

CAUTION

FU Qiang is part of a Chinese hacking group known as APT 41 and BARIUM. On August 11, 2020, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals FU Qiang, JIANG Lizhi, and QIAN Chuan on multiple charges including Racketeering Conspiracy; Conspiracy; Identity Theft; Aggravated Identity Theft; Access Device Fraud; Obtaining Information by Unauthorized Access to Protected Computers; Intentionally Causing Damage to Protected Computers; Threatening to Damage a Protected Computer; and Money Laundering. These charges stem from their alleged unauthorized computer intrusions while employed by Chengdu 404 Network Technology Company. The defendants allegedly conducted supply chain attacks to gain unauthorized access to networks throughout the world, targeting hundreds of companies representing a broad array of industries to include: social media, telecommunications, government, defense, education, and manufacturing. These victims included companies in Australia, Brazil, Germany, India, Japan and Sweden. The defendants allegedly targeted telecommunications providers in the United States, Australia, China (Tibet), Chile, India, Indonesia, Malaysia, Pakistan, Singapore, South Korea, Taiwan, and Thailand. The defendants allegedly deployed ransomware attacks and demanded payments from victims.

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Washington D.C.