Iranian Hackers

https://www.cnn.com/2021/11/11/politics/fbi-iran-hacking-warning/index.html

Hackers in Iran have been searching cybercriminal websites for sensitive information stolen from American and foreign businesses. They've also been looking for information about how to break into these businesses. This information could help them plan future hacks.The FBI warns that criminals may use ransomware as a tool to extort money from businesses. The bureau also suggests that companies should consider what data may have been stolen and whether it might be used to harm their networks.Bleeping computer reported the FBI warning. CNN has requested comment on the warning. The FBI does not identify hackers by name. Iran is suspected of being behind this attack. Cybercriminals associated with the Iranian government may be involved.Cyber attacks are becoming more sophisticated. Some people think that Iran is behind these cyberattacks. These hackers pose as ransomware operators while disrupting businesses. They use malware to steal data and money.Iran was responsible for hacking into the email accounts of Republican senators before the 2016 presidential election to send fake news messages about Hillary Clinton.

1) Hackers stole personal information of more than 3,000 Americans

2) Hackers stole trade secrets and other sensitive business information

3) Hackers also used social media to impersonate employees of US companies

4) Hackers were able to access company servers remotely

5) Hackers stole files containing personal information about victims

6) Hackers stole files with sensitive business information. The defendants used fake names and email accounts to trick victims into clicking on malicious links. Then they stole the victims' private information.The three men were arrested in Iran.

They face charges in the US.-" Esphargham and Bayati are accused of conspiring to hack into computer systems at the U.S. Department of Defense, NASA, and the National Oceanic and Atmospheric Administration.

- Esphargham is also accused of intentionally damaging computers belonging to the United States government.

- Bayati is accused of hacking into an online database used by the U.S. Army Corps of Engineers.The maximum penalty for each count is five years in prison, three years of supervised release, a $250,000 fine, and a $100 special assessment.