FEDERAL BUREAU OF INVESTIGATION

CASE EXAMPLE: CYBER THREATS

CHINESE CYBER HACKERS' TARGETING OF U.S. AEROSPACE AND MILITARY INTELLECTUAL PROPERTY

Over a six-year period, Su Bin, a Chinese citizen living in Canada, conspired with two people in China to gain unauthorized access to protected computer networks in the United States. Together they targeted information about the United States' fighter jets and military cargo aircraft program, and they sought to illegally export that information to China.

TWO PEOPLE IN CHINA HACKED INTO PROTECTED COMPUTER NETWORKS IN THE UNITED STATES AND STOLE INFORMATION ABOUT U.S. FIGHTER JETS AND MILITARY CARGO AIRCRAFT TO ILLEGALLY EXPORT THAT INFORMATION TO CHINA

As part of their conspiracy, Su would email the others guidance about which individuals, technologies, and corporations—including a world-renowned U.S. aerospace company—to target during their computer intrusions. One of Su's co-conspirators would gain access to information residing on U.S. companies' computers, using techniques to avoid detection, and then email Su the directory file listings and folders displaying the accessible data. Su would direct his co-conspirator to steal particular files and folders—specifically targeting flight test data, outlines of aircrafts' pipeline and electrical wiring systems, and detailed drawing measurements of their wings, fuselage, and other parts.

Su would translate the stolen data from English into Chinese, and he and his co-conspirators wrote reports detailing the information and technology they had acquired, including its value to the stolen data's final beneficiaries. Su's plea agreement made clear the information he and his co-conspirators intentionally stole included data listed on the International Traffic in Arms Regulations' U.S. Munitions List, which cannot be exported without a license. He admitted he hoped to sell the data he and his co-conspirators illegally acquired for a profit.

CONTACT US:

For more information, contact your local field office at
https://www.fbi.gov/contact-us/field-offices

CYBER THREATS: VULNERABILITIES, INDICATORS, AND MITIGATION

VULNERABILITIES

Some circumstances that may render organizations more vulnerable to cyber intrusions include:

- Involvement in classified information, financial information, manufacturing, and advanced technology
- Lonely employees trying to prove self-worth through malicious activity
- Angry or disgruntled employees seeking revenge
- Outdated firewall protections and software

INDICATORS

A cyber intrusion threat typically demonstrates one or more of the following indicators:

- A disgruntled hacker wanting to retaliate against the government and/or company
- Acquisition of sensitive information without a need to know
- Continuous rerouting of websites, indicating social engineering malware
- Social media requests from unknown individuals
- Rewritten computer code from an unauthorized source
- A request for sensitive information unrelated to the requestor's job or company
- Concealed hyperlinks on a website or in a document that cause an employee to unknowingly expose the company network to the theft of sensitive data

MITIGATION

There are steps organizations may take to identify and deter potential cyber intrusions. The FBI offers these for information, but each company must assess applicability in terms of its own policies, processes, and legal guidelines.

- Educate and regularly train employees on security policies and protocols.
- Update software, firewalls, and anti-virus programs.
- Install Intrusion Detection Systems (IDSs).
- Establish Virtual Private Networks (VPNs) for added protection.
- Ensure proprietary information online is carefully protected.
- Employ appropriate screening processes to hire new employees.
- Provide nonthreatening, convenient methods for employees to report suspicious behavior, and encourage such reporting.
- Routinely monitor computer networks for suspicious activities.
- Ensure physical security personnel and information technology security personnel have the tools they need to share information.
- Encourage responsible use of social media sites and ensure online profiles have proper security protections in place.