FEDERAL BUREAU OF INVESTIGATION

CHINA CYBER THREAT: CHINESE MILITARY HACKERS TARGET U.S. BUSINESSES

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

Five Chinese military officers were indicted for economic espionage and other offenses directed at six U.S. companies in the nuclear power, metals, and solar industries. The officers were members of the Chinese People's Liberation Army Unit 61398 and were in charge of spotting, assessing, and attacking U.S. industries targeted by the Chinese government.

A U.S. SOLAR COMPANY WAS COMPLETELY DRIVEN OUT OF THE CHINESE MARKET AS A DIRECT RESULT OF THIS LOSS

Unit 61398 had been assigned to create a secret database to hold U.S. corporate intelligence on the iron and steel industries. During trade discussions with a U.S. steel company, the Chinese officers sent spearphishing* emails containing malware to employees in the U.S. steel company's litigations department, resulting in the theft of hostnames, descriptions of their computers, and identified vulnerabilities in the U.S. company's servers.

The Chinese military officers, using hacker names such as UglyGorilla and KandyGoo, targeted a U.S. nuclear power plant construction company during its negotiations with a large Chinese state-owned enterprise. The cyber hackers stole roughly 700,000 pages of emails, including trade secret designs for components of the nuclear power plants. Additional losses included cost, pricing, and strategy information, giving the Chinese company an unfair advantage in the negotiations.

The U.S. Department of Commerce determined Chinese solar product manufacturers used financial information stolen by Unit 61398 from a U.S. solar company to undercut U.S.-produced solar products. The compromised information included cash flow, manufacturing metrics, production line information, costs, and attorney-client conversations. The U.S. solar company was completely driven out of the Chinese market as a direct result of this loss.

CONTACT US:

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

** Spear phishing is an email-spoofing attack that targets a specific organization or individual, seeking unauthorized access to sensitive information. Spear-phishing attempts are not typically initiated by random hackers but are more likely to be conducted by perpetrators out for financial gain, trade secrets, or military information.*

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
- Acquitision 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
- Requests for sensitive information outside the requestor's purview
- 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 program.
- Install Intrusion Detection Systems (IDSs).
- Establish Virtual Private Networks (VPNs) for added protection.
- Ensure propriety information on company networks or transmitted via the internet 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.