Foreign Collection Methods: Indicators and Countermeasures

IDENTIFY

- Requests for Information
- Academic Solicitation
- Suspicious Network Activity
- Targeting at Trade Shows
- Solicitation and Marketing /Seeking Employment
- Foreign Visits
- Elicitation

REPORT

- Reporting of Foreign Collection Attempts is key to protecting your organization's information. Adversaries can target classified and unclassified materials, including sensitive and proprietary data, controlled unclassified information, and more.

The United States faces an expanding array of foreign intelligence threats. The U.S. government and its public and private sector partners are at increased risk for targeting by adversaries and no organization is immune from these efforts to obtain both classified and unclassified information. Pursuant to Section 811 of the Intelligence Authorization Act, Executive Branch Departments and Agencies must ensure that the Federal Bureau of Investigation (FBI) is advised immediately of any information, regardless of its origin, which indicates that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power. Private sector partners can make reports directly to their local FBI field office and should reach out should they encounter any suspicious activities or suspicious foreign contacts.

The most common foreign collection methods, used in over 80% of targeting cases, are:

- Requests for Information
- Academic Solicitation
- Suspicious Network Activity
- Targeting at conferences, conventions, and trade shows
- Solicitation and Marketing /Seeking Employment
- Foreign Visits
- Elicitation and Recruitment

If you suspect you may have been a target of any of the methods included here, or have been targeted by any other method, report it immediately.

For more Counterintelligence Awareness Resources click here.

"There is one evil that I dread, and that is, their spies."
- General George Washington, 1777

REQUESTS FOR INFORMATION

Technique

This method uses an information request that was not sought or encouraged. Requests may originate from known or unknown sources including:

- Foreign companies
- Individuals
- Foreign government officials
- Organizations

Indicators

There are several possible indicators of unsolicited and direct requests, including, but not limited to, those listed below. The requestor:

- Sends a request using a foreign address
- Has never met recipient
- Identifies self as a student or consultant
- Identifies employer as a foreign government
- States that work is being done for a foreign government or program
- Asks about a technology related to a defense program, project, or contract
- Asks questions about defense-related programs using acronyms specific to the program
- Insinuates the third party he/she works for is "classified" or otherwise sensitive
- Admits he/she could not get the information elsewhere because it was classified or controlled
- Advises the recipient to disregard the request if it causes a security problem, or the request is for information the recipient cannot provide due to security classification, export controls, etc.
- Advises the recipient not to worry about security concerns
- Assures the recipient that export licenses are not required or not a problem
- Fails to identify the end user

Countermeasures

The following countermeasures can protect against unsolicited and direct requests:

- View unsolicited and direct requests with suspicion, especially those received via the internet
- Respond only to people who are known after verifying their identity and address and ensuring proper authorization for release of information.
- If the requester cannot be verified or the request is suspicious:

    ⇒ Do not respond in any way
    ⇒ Report the incident to security personnel

If you suspect you may have been a target of this method, report it.

SOLICITATION AND MARKETING/SEEKING EMPLOYMENT

The solicitation and seeking employment collection method may take many forms including, but not limited to, joint ventures or research partnerships, offering of services, or internship programs for foreign students.

"The arrests of 10 Russian spies last year provided a chilling reminder that espionage on U.S. soil did not disappear when the Cold War ended."

FBI Counter-intelligence Division, 10/31/2011

Technique

- Places foreign personnel in close proximity to cleared personnel
- Provides opportunity to build relationships that may be exploited
- Places adversary inside facility to collect information on desired technology

Indicators

- Foreign visitors mail or fax documents written in a foreign language to a foreign embassy or foreign country
- Foreign visitors request:
  - ⇒ Access to the LAN
  - ⇒ Unrestricted facility access
  - ⇒ Company personnel information

Countermeasures

The following countermeasures may guard against this collection method:

- Review all documents being faxed or mailed; use a translator, when necessary
- Provide foreign representatives with stand-alone computers
- Share the minimum amount of information appropriate to the scope of the joint venture/research
- Educate employees extensively
  - ⇒ Project scope
  - ⇒ Handling and reporting elicitation
- Sustainment training
- Refuse to accept unnecessary foreign representatives into the facility
- Develop a Technology Control Plan (TCP)

If you suspect you may have been a target of this method, report it.

Russian spy Christopher Metsos (right), swaps information in a "brush pass" with an official from the Russian Mission in New York in 2004.
-FBI Vault, FOIA Release

SUSPICIOUS NETWORK ACTIVITY

Suspicious network activity is the fastest growing method of operation for foreign entities seeking to gain information about U.S. interests. It may also be referred to as *cyber terror*, *cyber threats*, *cyber warfare*, etc.

Technique

An adversary may target anyone or any system at any facility, using a number of methods:

- Input of falsified, corrupted data
- Malware, malicious code, viruses
- Hacking
- Chat rooms-elicitation
- Email solicitation (phishing)

"Dillinger or Bonnie and Clyde could not do a thousand robberies in all 50 states in the same day from their pajamas from Belarus. That's the challenge we face today."

- James B. Comey, Director, FBI

Indicators

The following is a list of suspicious indicators related to suspicious internet activity and cyber threats:

- Unauthorized system access attempts
- Unauthorized system access to or disclosure of information
- Any acts that interrupt or result in a denial of service
- Unauthorized data storage or transmission
- Unauthorized hardware and software modifications
- Emails received from unknown senders with foreign addresses

Countermeasures

The following countermeasures can be taken to guard against this collection method:

- Develop and implement a Technology Control Plan (TCP)
- Conduct frequent computer audits:
  - ⇒ Ideally: Daily
  - ⇒ At minimum: Weekly
- Do not rely on firewalls to protect against all attacks
- Report intrusion attempts
- Direct personnel to avoid responding to or clicking on links from unknown sources and to report such items
- Disconnect computer system temporarily in the event of a severe attack

If you suspect you may have been a target of this method, report it.

ACADEMIC SOLICITATION

Technique

This method uses students, professors, scientists or researchers as collectors improperly attempting to obtain sensitive or classified information.

Requests may originate from known or unknown sources including:

- Foreign Universities or Academic Centers
- Individuals overseas or placed in the U.S.
- Quasi-governmental Organizations such as research centers and institutes

Indicators

There are several possible indicators of academic solicitation, including, but not limited to, those listed below:

- Foreign students accepted to a U.S. university or at postgraduate research programs are recruited by their home country to collect information, and may be offered state-sponsored scholarships as an incentive for their collection efforts.
- U.S. researchers receive requests to provide dual-use components under the guise of academic research.
- U.S. researchers receive unsolicited emails from peers in their academic field soliciting assistance on fundamental and developing research.
- U.S. professors or researchers are invited to attend or submit a paper for an international conference.
- Overqualified candidates seeking to work in cleared laboratories as interns.
- Candidates seeking to work in cleared laboratories whose work is incompatible with the requesting individual's field of research.
- Intelligence entities will send subject matter experts (SMEs) requests to review research papers, in hopes the SME will correct any mistakes.

Countermeasures

The following countermeasures can protect against academic solicitation:

- View unsolicited academic solicitations with suspicion, especially those received via the internet.
- Respond only to people who are known after verifying their identity and address.
- Ensure any response to known or unknown requestors includes only information authorized for release.
- If the requester cannot be verified or the request is suspicious:
  - ⇒ Do not respond in any way
  - ⇒ Report the incident to security personnel

If you suspect you may have been a target of this method, report it.

"Chinese Professors Among Six Defendants Charged with Economic Espionage and Theft of Trade Secrets for Benefit of People's Republic of China."

- U.S. Department of Justice May 29, 2015

FOREIGN VISIT

Technique

Suspicious contact during a foreign visit can occur at any time and may come from:

- One-time visitors
- Long-term visitors
  - ⇒ Exchange employees
  - ⇒ Official government representatives
  - ⇒ Students
- Frequent visitors
  - ⇒ Sales representatives
  - ⇒ Business associates

Indicators

Suspicious or inappropriate conduct during foreign visits can include:

- Requests for information outside the scope of what was approved for discussion
- Hidden agendas associated with the stated purpose of the visit
- Visitors/students requesting information, and then growing irate upon denial
- Individuals bringing cameras and/or video equipment into areas where no photographs are allowed
- Wandering visitors using distractions to slip away
- New visitors added to group at last minute or switching of prescreened visitors

Countermeasures

The following countermeasures can protect against unauthorized access by foreign visitors:

- Prior to visit, brief hosts and escorts on approved procedures
- Walk visitor route and identify vulnerabilities
- Prior to the visit, notify all employees about the visit, restrictions on the visitors, and the nature of the threat
- Debrief personnel in contact with visitors
- Ensure visitors do not bring recording devices, including cell phones, into the facility

If you suspect you may have been a target of this method, report it.

"Via visits... that are either pre-arranged by foreign contingents or unannounced, these are attempts to gain access to and collect protected information…"

- Defense Security Service, Targeting U.S. Technologies

TARGETING AT CONFERENCES, CONVENTIONS, AND TRADE SHOWS

This method directly links targeted programs and technologies with knowledgeable personnel.

Technique:

Technical experts may receive invitations to share their knowledge
Experts may be asked about restricted, proprietary, and classified information

Indicators

The following are suspicious indicators related to seminars, conventions, and trade shows.

Prior to event:

- Personnel receive an all-expenses-paid invitation to lecture in a foreign nation
- Entities want a summary of the requested presentation or brief 6 – 12 months prior to the lecture date
- Host unsuccessfully attempted to visit facilities in the past
- Travel to event may pose targeting opportunities

During event:

- Telephone monitoring and hotel room intrusions
- Conversations involving classified, sensitive, or export-controlled technologies
- Excessive or suspicious photography and filming of technology and products
- Casual conversations during and after the event hinting at future contacts or relations
- Foreign attendees' business cards do not match stated affiliations
- Attendees wear false name tags
- Individuals returning to same booth multiple times
- Detailed and probing questions about specific technology

"You can be targeted at any conference, convention, or trade show, foreign or domestic."

- Defense Security Service

Countermeasures

The following countermeasures can be to guard against this collection method:

- Consider what information is being exposed, where, when, and to whom
- Provide employees with detailed travel briefings concerning:
  - ⇒ The threat
  - ⇒ Precautions to take
  - ⇒ How to react to elicitation
- Take mock-up displays instead of real equipment
- Request a threat assessment from the program office
- Restrict information provided to only what is necessary for travel and hotel accommodations
- Carefully consider whether equipment or software can be adequately protected
- Debrief attendees after the event to identify potential suspicious activity

If you suspect you may have been a target of this method, report it.

ELICITATION AND RECRUITMENT

Wen Chyu Liu
Found Guilty
January 2012,
Trade Secret Theft

Intelligence officers spot and assess individuals for potential recruitment. Adversaries are not necessarily looking for someone with a high level of access; sometimes the potential for future access or the ability of the recruit to lead to other high value targets is enough to generate adversary interest.

Technique:

Once a potential recruit has been identified, adversaries begin to cultivate a relationship with that individual. In the "Development Phase," meetings with the recruit become more private and less likely to be observable or reportable. By the time the "recruitment and handling phase" is initiated, the individual is likely emotionally tied to the adversary.

Indicators

Spotting and Assessing can take place anywhere, but is always approached in a non-threatening and natural manner designed to elicit information. Elicitation is the strategic use of conversation to subtly extract information about you, your work, and your colleagues. Foreign intelligence entities elicit information using both direct and indirect questioning. They may create a cover story to explain the line of questioning in their attempts to make the discussion less suspicious.

Liu recruited at least four current and former coworkers, paid current and former coworkers for material and information, and bribed a coworker with $50,000 in cash to provide information.

Trade shows, business contacts, social events, or online venues such as chat rooms and social media, are used for this process. During the Spot and Assessment phase, the FIE will often explore potential exploitable weaknesses which may be used as a lever against the recruit. These could include: Drugs or Alcohol, Gambling, Adultery, Financial Problems, or other weaknesses.

The actual recruitment may involve appeals to ideological leanings, financial gain, blackmail or coercion, or any other of a number of motivators unique to that recruit. Some of these may manifest as observable and reportable behaviors.

Countermeasures

Any contact which suggests the employee concerned may be the target of an attempted exploitation by the intelligence services of another country must be reported. Do not share anything the elicitor or recruiter is not authorized to know, including personal information about yourself, your family, or your co-workers. If you believe someone is attempting to elicit information from you, you can:

- Change the topic
- Refer them to public websites
- Deflect the question
- Provide a vague answer
- Feign ignorance and ask the elicitor to explain what they know