Insider Threats and Cyber Threats

SPECIAL AGENT MICHAEL S. MORGAN
FEDERAL BUREAU OF INVESTIGATION
HOUSTON FIELD OFFICE

Insider Threat

A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.

PERSONAL FACTORS

- Greed or Financial Need
- Anger/Revenge
- Problems at work
- Ideology/Identification
- Divided Loyalty
- Adventure/Thrill
- Vulnerability to blackmail
- Ego/Self-image
- Vulnerability to flattery or the promise of a better job
- Ingratiation
- Compulsive and destructive behavior
- Family problems

Organizational Factors

- Availability and ease of access to IP
- Information is not properly labeled
- The ease that someone may exit the facility or network system.
- Employees are not trained on how to properly protect proprietary information.
- Work from home policies
- Perception that security is lax
- Time pressure

Behavioral Indicators

- Without need or authorization, takes proprietary or other material home via documents, thumb drives, computer disks, or e-mail.
- Inappropriately seeks or obtains proprietary or classified information on subjects not related to their work duties.
- Interest in matters outside the scope of their duties, particularly those of interest to foreign entities or business competitors.
- Unnecessarily copies material, especially if it is proprietary or classified.

Behavioral Indicators

- Remotely accesses the computer network while on vacation, sick leave, or at other odd times.

- Disregards company computer policies on installing personal software or hardware, accessing restricted websites, conducting unauthorized searches, or downloading confidential information.

- Works odd hours without authorization; notable enthusiasm for overtime work, weekend work, or unusual schedules when clandestine activities could be more easily conducted.

Behavioral Indicators

- Unreported foreign contacts (particularly with foreign government officials or intelligence officials) or unreported overseas travel.
- Short trips to foreign countries for unexplained or strange reasons.
- Unexplained affluence; buys things that they cannot afford on their household income.
- Engages in suspicious personal contacts, such as with competitors, business partners or other unauthorized individuals.

Behavioral Indicators

- Overwhelmed by life crises or career disappointments.
- Unusual interest in the personal lives of coworkers; asks inappropriate questions regarding finances or relationships.
- Concern that they are being investigated; leaves traps to detect searches of their work area or home; searches for listening devices or cameras.

Recent Cyber Incidents

Overview

- Cyber Threat Actors
- Malware & Cyber Attacks
- Prevention & Preparation

Cyber Threat Actors

- Criminal
  - transnational
  - opportunistic
  - money
- State Sponsored
  - well resourced
  - focused
  - information & access

Malware

- Malicious software
  - keylogger
  - copy sensitive data
  - webcam / microphone spy
  - web injects
  - destroy data
  - destroy equipment

Zero Day Vulnerability

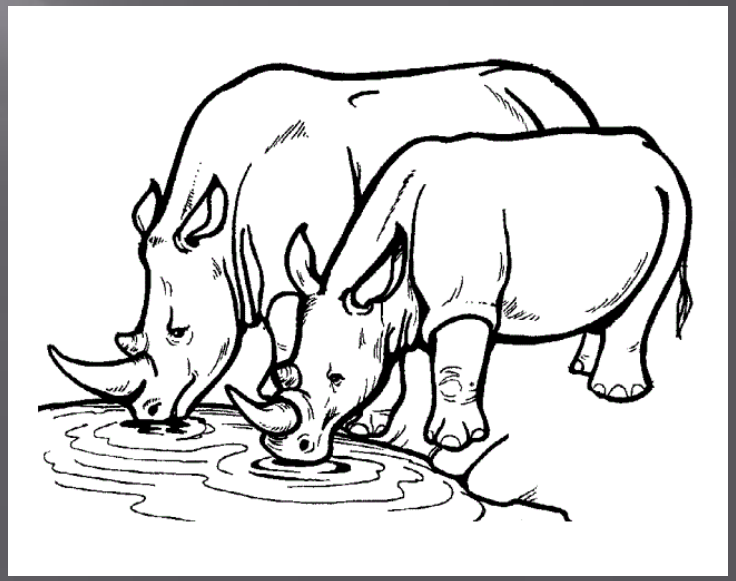
- All software has flaws
- Flaw unknown to vendor
  - "zero" days to repair
- Sold on criminal forums

Spear Phishing

- *Advanced* phishing scam
  - targets a particular person
  - sophisticated adversary
  - used to get the "big fish"
  - attachments & links

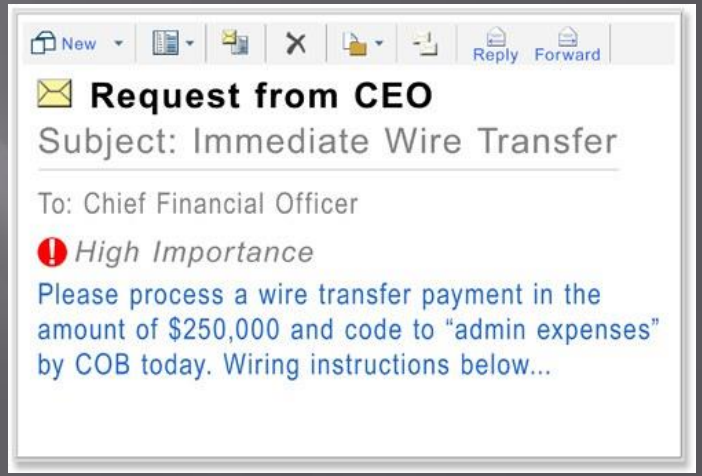
Watering Hole Attack

- Distribute malware
  - attackers compromise website
  - user loads website
  - actors select from compromised end users



Business Email Compromise

- Hijack accounting dept.
  - malware
  - social engineering
- Actors email personnel
  - email from "trusted source"
  - *wire $$ ASAP*
  - includes fake docs



Ransomware

- Take data hostage
  - enabled by phishing
  - encrypts all data
  - demands ransom
  - backups are best defense

Ransomware

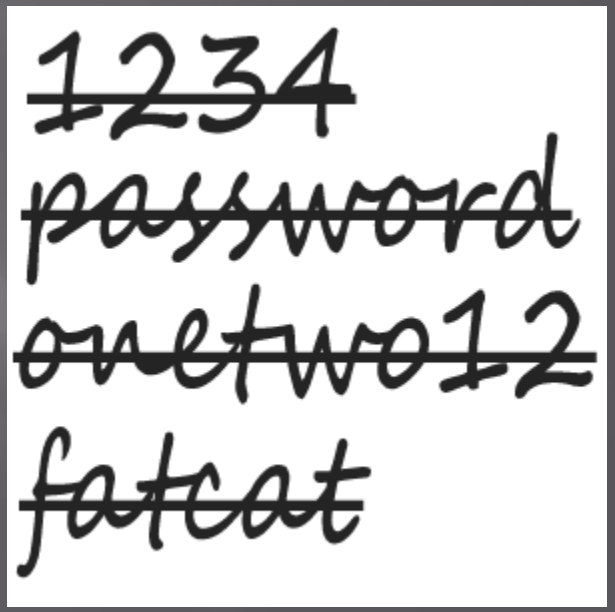

YOUR COMPUTER HAS BEEN LOCKED!
This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.
To unlock the computer you are obliged to pay a fine of $200.
You have 72 hours to pay the fine, otherwise you will be arrested.
You must pay the fine through
To pay the fine, you should enter the digits resulting code, which is located on the back of your in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY
BRAVERY
INTEGRITY
OK

Attack Mitigation

- Monitor network traffic
  - establish "normal" baseline
- Trust but Verify
- Layered security
- Incident handling process

Passwords / Authentication

- Password reuse
- Password reset questions
- Password managers
- Two factor authentication
- Biometrics



Trust Relationships

- Vendors & contractors
- Links between networks
  - limit connections
  - monitor access
- Incident handling process
- Cyber insurance

Make a Difference

- Educate and regularly train employees on security or other protocols.
- Use appropriate screening processes to select new employees.
- Provide non-threatening, convenient ways for employees to report suspicions.
- Routinely monitor computer networks for suspicious activity.
- Ensure security personnel have the tools they need.

IC3 & InfraGard

- Internet Crime Complaint Center – www.ic3.gov
  - collects reports of fraud
  - assesses trends
  - refers cases to FBI

- InfraGard – www.infragard.org
  - FBI / private sector partnership
  - critical infrastructure protection
  - Education
  - FLASH & PIN

Contact Information

MICHAEL S. MORGAN

Special Agent

Houston FBI

(713) 936-7734

MSMorgan@fbi.gov