John Chesson
Special Agent
InfraGard Coordinator

FBI San Francisco Division
Counter Intelligence Computer Intrusion

COMPUTER INTRUSION INVESTIGATIONS

Investigative Challenges

- Victim preparedness and response capabilities
- Volatility of uncollected digital evidence
- Speed of legal process for compelled disclosures
- Volume of digital evidence analysis
- Reliable attribution capabilities

Control System Access

Record ingress and egress to physically secure control system areas such as:

- Motor control centers
- Rack rooms
- Server rooms
- Telecommunications rooms
- Control system rooms.

Use physical controls such as:

- Sign in logs
- Photo ID badges
- Key cards and/or number pads
- A close-circuit television system.

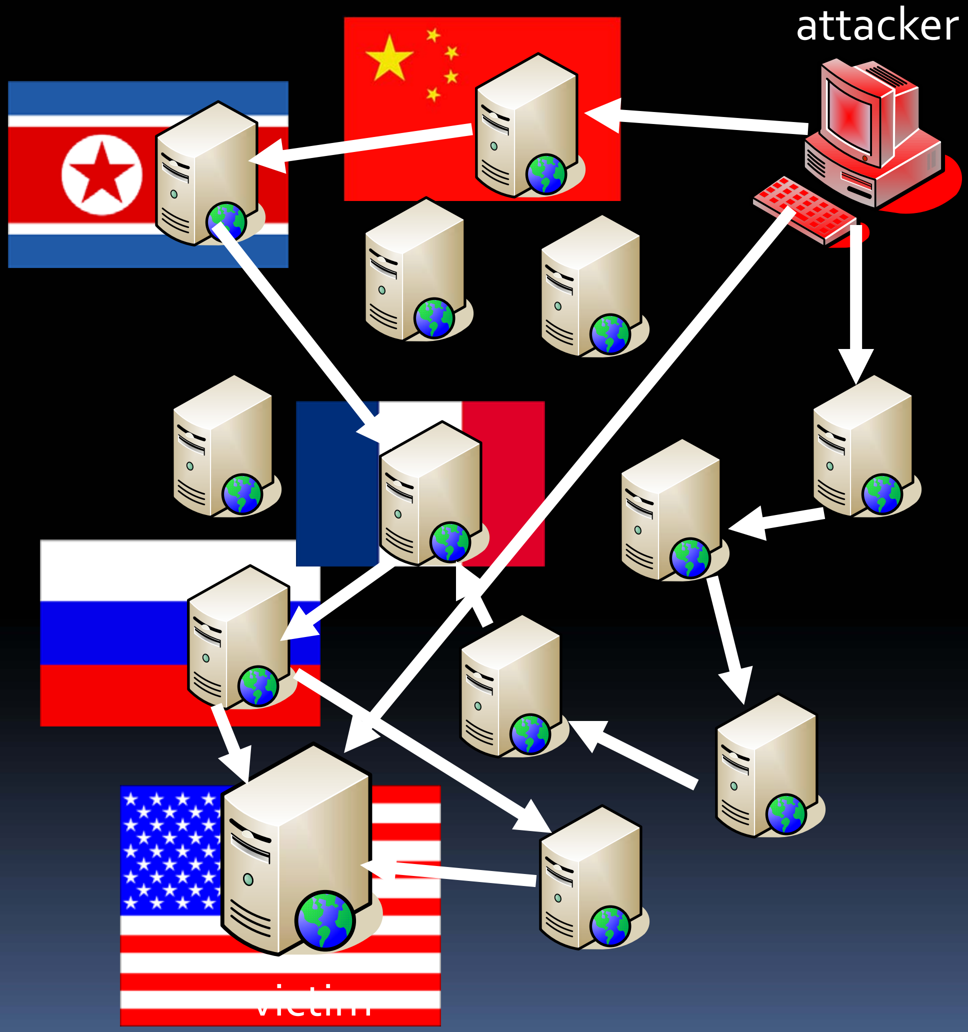
Use cyber security measures such as:

- Firewalls with effective configurations
- Virus protection with current updates
- DMZs to isolate business networks from operations
- Intrusion detection systems
- Encryption modules

Follow the principles of "least access," "need to know," and "separation of functions," and closely control the process of granting user authorizations, rather than allowing access by rank or precedent. Allow only authorized personnel to have physical access to central computer rooms and supervise any visitors.

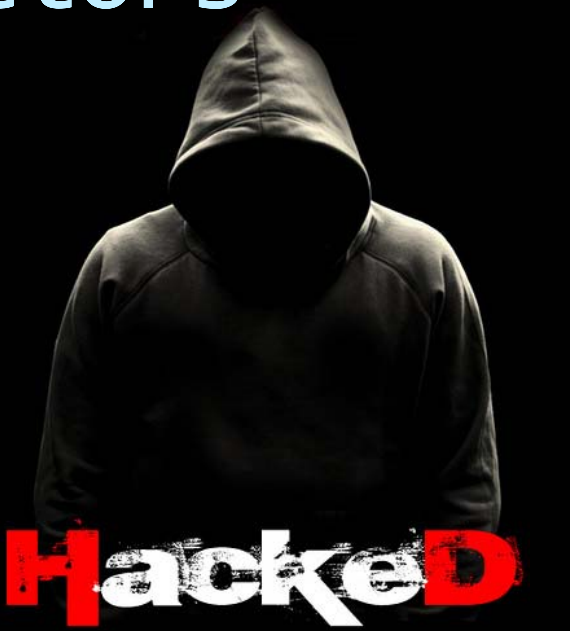
Attribution Challenges

- Web Proxy Services
- Onion Routers
- Botnets
- Compromised hosts computers
- Foreign ISPs
- Encryption



Cyber Threat Actors

- Script kiddies
- Hacktivist Groups
- Organized Crime
- Advanced Persistent Threat (APT)

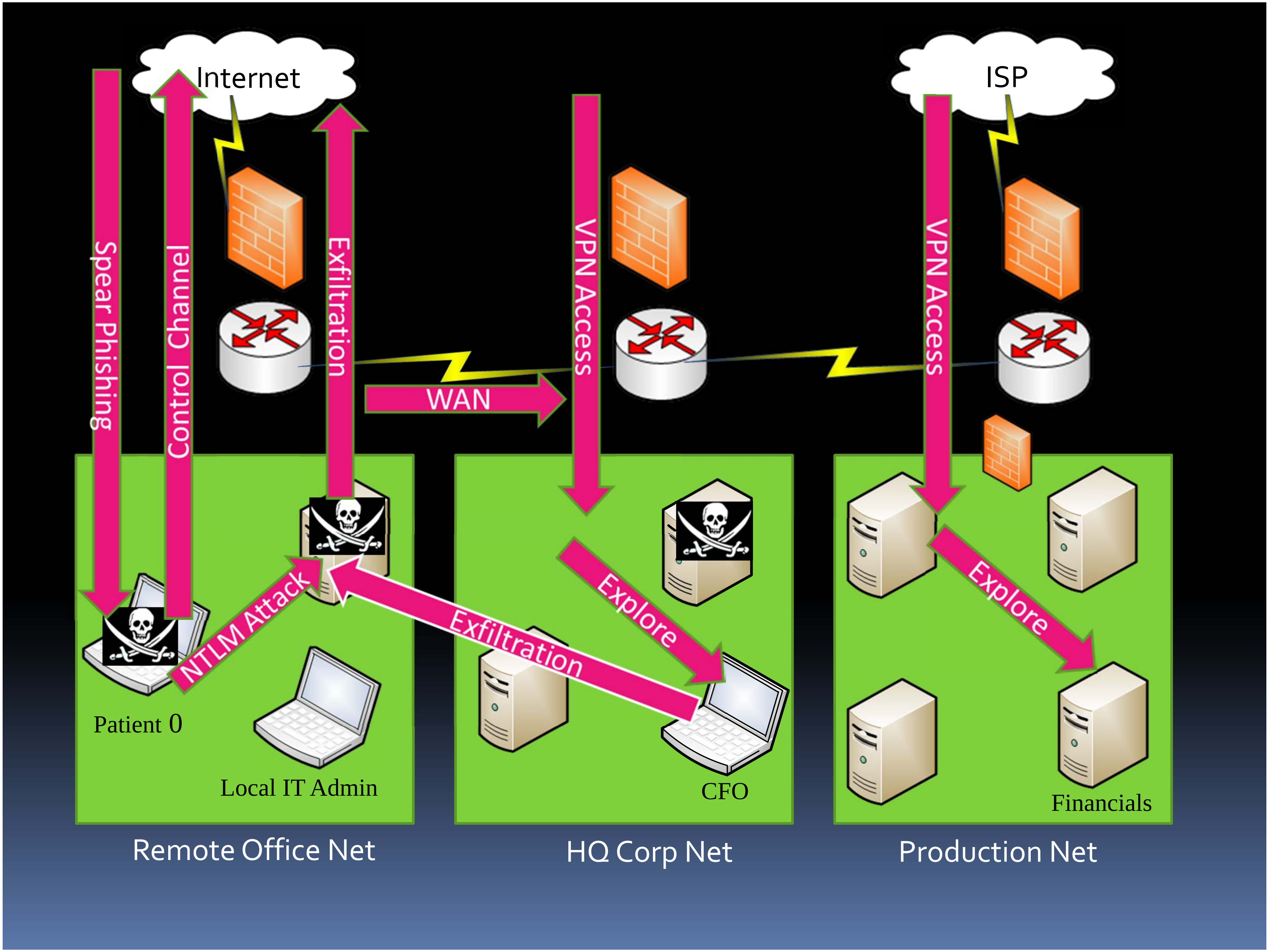


Advanced Persistent Threats

- State sponsored actors targeting
  - Businesses with global market advantage
  - US Gov't classified projects
- Suspected State goals
  - Gain competitive edge for global business
  - Steal research and intellectual property
  - Use your trusted relationships to propagate compromises in and outside your company

APT Methodology

- Social Engineering
- Exploit
- Establish Control
- Escalate Privilege
- Maintain Access
- Explore for Sensitive Data
- Exfiltrate the Goods


Internet
ISP
Spear Phishing
Control Channel
Exfiltration
WAN
VPN Access
VPN Access
NTLM Attack
Exfiltration
Explore
Explore
Patient 0
Local IT Admin
CFO
Financials
Remote Office Net
HQ Corp Net
Production Net

DON’T BE PATIENT 0:

Tips to reduce your vulnerability

- Personal computer use habits:
  - Don’t use Administrative User Account for
    - Internet surfing or checking emails
  - Disable scripts when using a web browser
    - i.e. Firefox Noscripts plugin
  - Always virus scan email attachments
- Social Media site habits:
  - Frequently review privacy settings
- International Travel habits:
  - Don’t take your phone or laptop

Cyber Attack Vectors

- Perimeter Vulnerability Exploitation
  - Firewall/IDS by-pass attacks
  - DMZ server attacks
- Perimeter By-pass
  - Wireless AP
  - VPN
- User mobile device exploit
  - Smart phone
  - Laptop
  - Writeable media Trojans

Intrusion Preparation

- Out of band communications
  - No VOIP & No Email
- Warning Banners – “Allows LE Monitoring”
- Management support
- Trained team members
  - Documentation and Evidence collection
- Liaison contact with local FBI
  - InfraGard

Warning Banner Sample

This system is restricted solely to COMPANY NAME authorized users for legitimate purposes only. The actual or attempted access, use, or modification of this system is strictly prohibited by COMPANY NAME. Unauthorized users are subject to company disciplinary proceedings and/or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws. The use of this system may be monitored, searched, and recorded for administrative and security reasons. Anyone accessing this system consents to such monitoring and search, and disclosure to law enforcement officials. All users must comply with COMPANY NAME corporate instructions regarding the protection of COMPANY NAME and customer assets.

How to notify the FBI

- APT suspected intrusions
  - DIBs reporting and local FBI
  - DSS reporting and local FBI
  - Local FBI notification
    - Call main number and ask for Computer Intrusion Squad…if not immediately available:
      - Provide duty agent basic information and request immediate call back from Cyber Squad.
- Non-intrusion can be reported to www.ic3.gov

Situational Awareness

- Join InfraGard: www.infragard.net
  - members only: https://infragard.org/
- National Terrorism Advisory System: www.dhs.gov/alerts
- MS-ISAC: www.msisac.org/index.cfm
- IT-ISAC: https://www.it-isac.org
- ES-ISAC: www.esisac.com/
- FS-ISAC: www.fsisac.com/
- US CERT: www.us-cert.gov/nav/t01/

Questions?

John B. Chesson

Special Agent

Federal Bureau of Investigation

San Francisco Division, San Jose Resident Agency

Counter Intelligence Computer Intrusion Squad (CY-4)

(408) 558-1065

john.chesson@ic.fbi.gov

FBI InfraGard Coordinator

San Francisco Bay InfraGard Chapter

www.sfbay-infragard.org