John B Chesson
Special Agent FBI

FBI San Francisco Division
Counter Intelligence Computer Intrusion

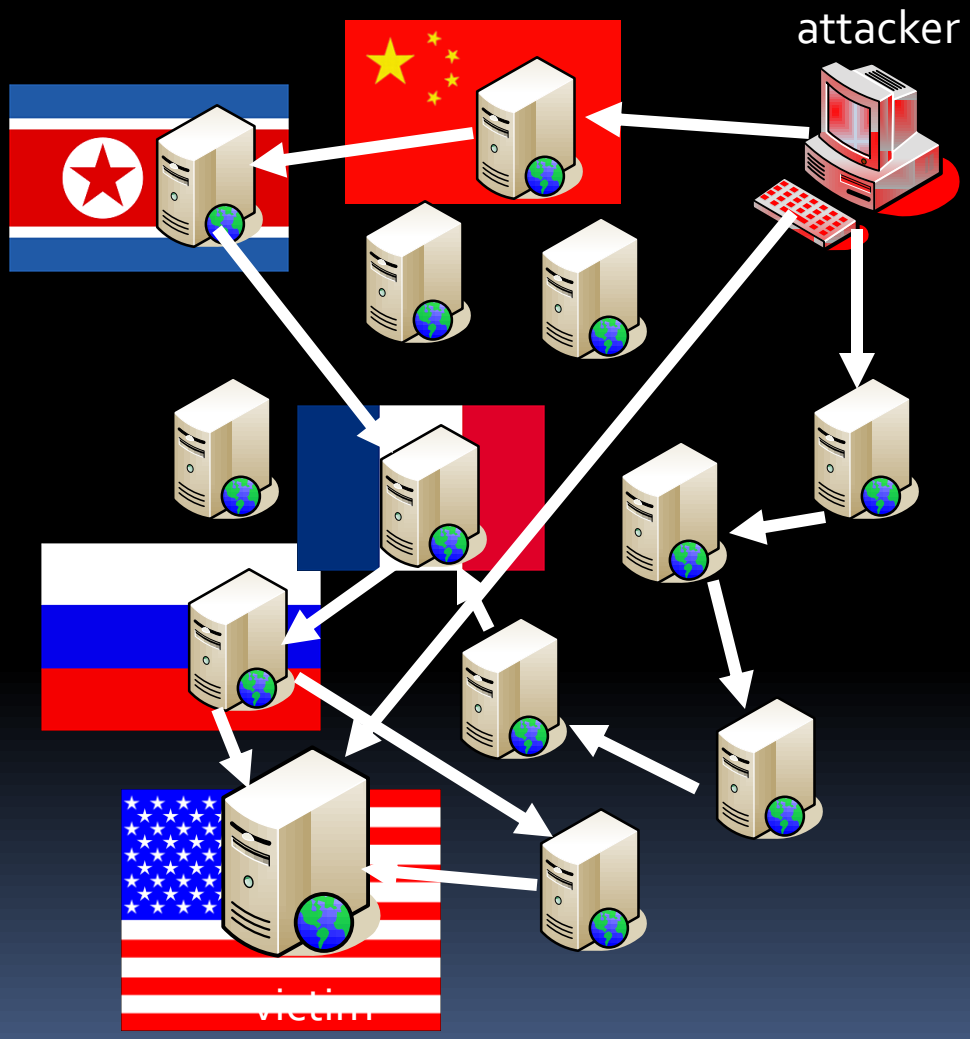
COMPUTER INTRUSION INVESTIGATIONS

Investigative Challenges

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

Attribution Challenges

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

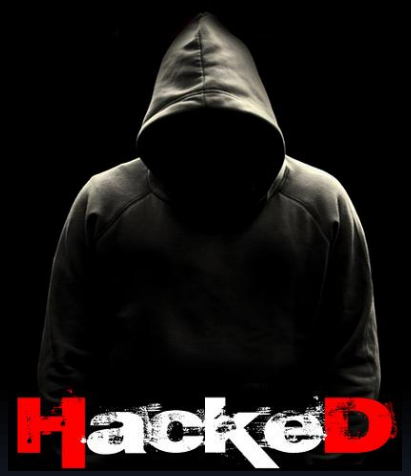


Cyber Attack Vectors

- Perimeter Vulnerability Exploitation
  - Firewall/IDS by-pass attacks
  - DMZ server attacks
- Perimeter By-pass
  - Email or Web Surfing
  - Wireless AP
  - VPN – stolen credentials
- User mobile device exploit
  - Smart phones
  - Laptops
  - Readable media Trojans (i.e. CD, DVD, Thumb Drive)

Cyber Threat Actors

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



Advanced Persistent Threats (APT)

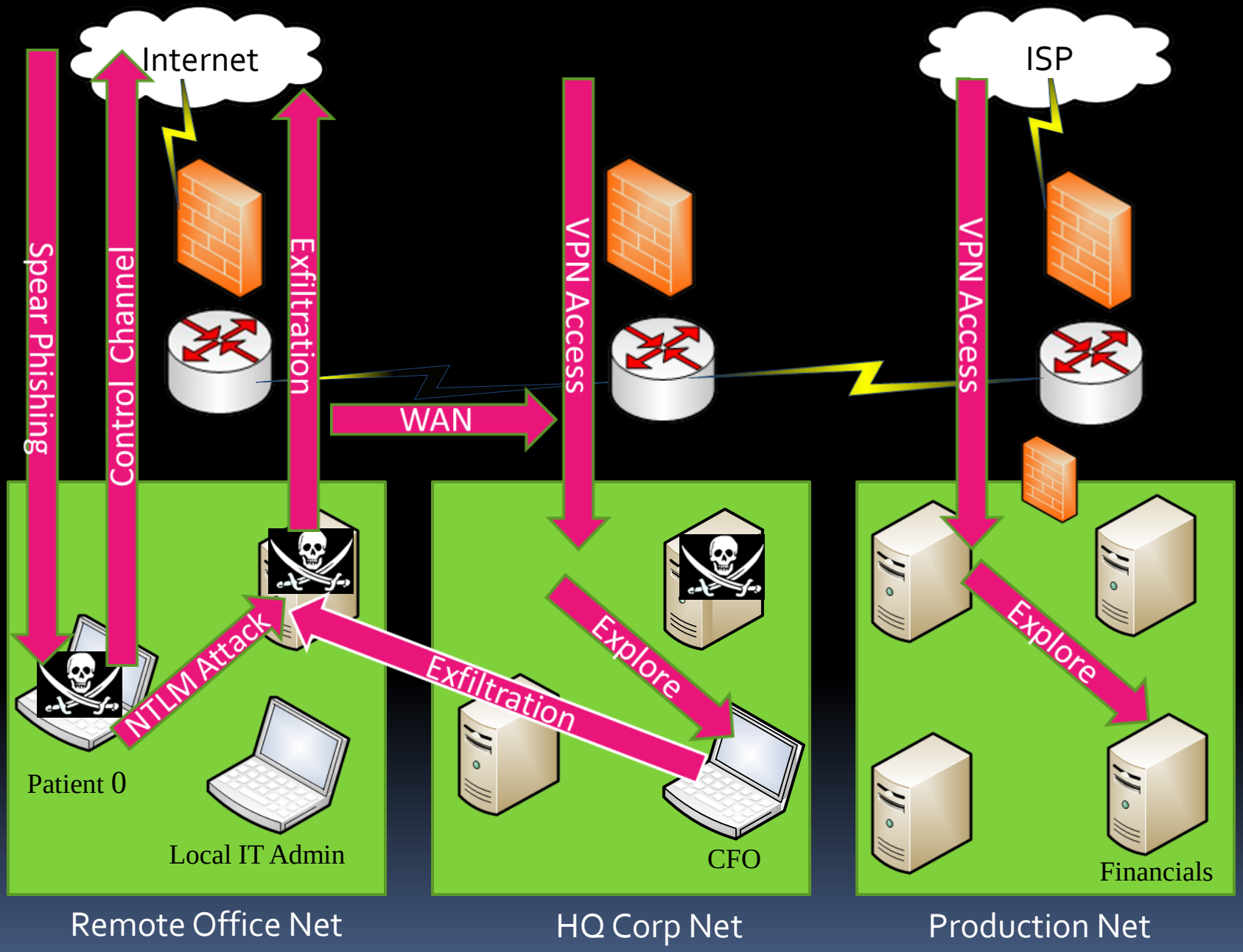
- State sponsored actors targeting
  - Businesses with global market advantage
  - US Gov't classified projects
- Suspected State goals
  - Gain competitive edge for global business
  - Steal research and intellectual property
  - Use your trusted relationships to propagate compromises in and outside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

APT indicators

- What is normal for your environment?
  - Beaconing out to Dynamic DNS domains
  - Data exfiltration spikes during odd times
  - Commonly open ports with uncommon protocols (like FTP on port 80)
- User login geo-location & temporal conflicts
  - Is a user logged in from two locations?
- Reconnaissance activities from systems inside your domain
  - Is someone “casing the joint?”

APT Methodology

- Reconnaissance – open source info on target
  - Social Engineering - email
- Exploit System - malware
  - Establish Control - beacon
  - Escalate Privilege – dump the hash
- Maintain Access – back doors
  - Explore for Sensitive Data – use network shares
- Exfiltrate the Goods

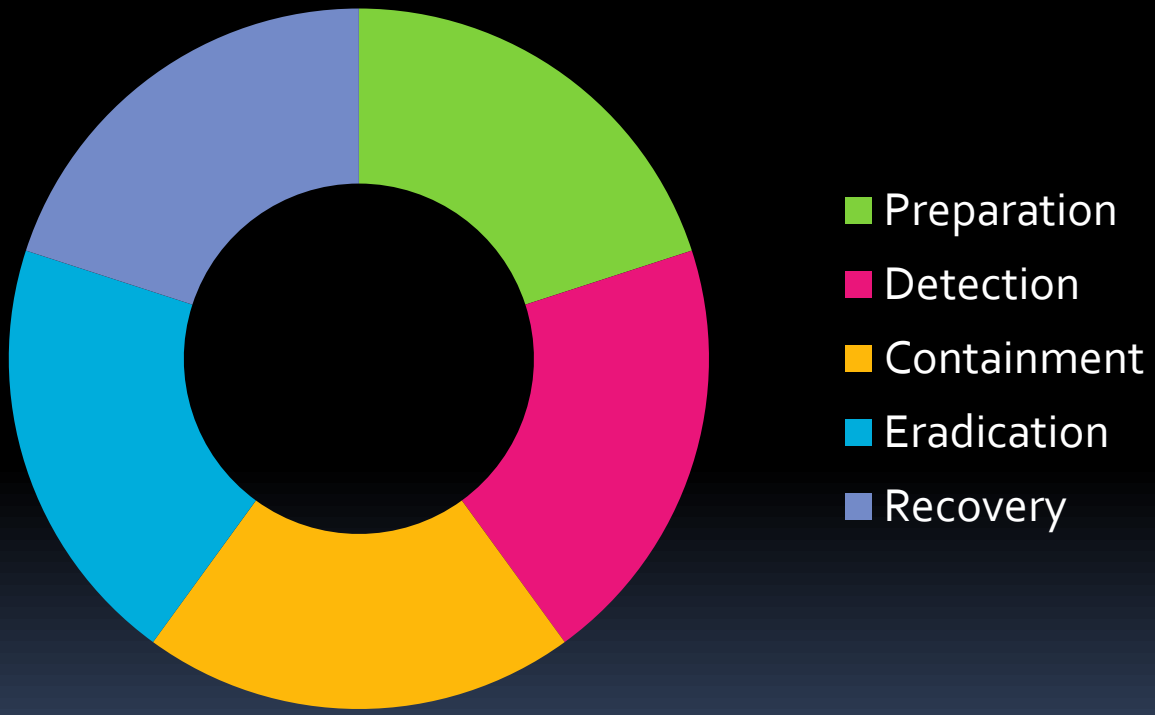

Internet
ISP
Spear Phishing
Control Channel
Exfiltration
VPN Access
VPN Access
WAN
NTLM Attack
Exfiltration
Explore
Explore
Patient 0
Local IT Admin
CFO
Financials
Remote Office Net
HQ Corp Net
Production Net

DON'T BE PATIENT 0:
Tips to reduce your vulnerability

- Personal computer use habits:
  - Don't use Administrative User Account
    - When Internet surfing or checking emails
  - Disable scripts when using a web browser
  - Always virus scan email attachments
  - Don't update software away from home
- Social Media site habits:
  - Be selective with what you share
  - Frequently review privacy settings
- International Travel habits:
  - Don't take your phone or laptop

“Good” Victims have:

Incident Response Plan



Key Preparation Points

- Out of band communications plan
  - 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

- Suspected Computer intrusions
  - Local FBI notification (SF FBI 415-553-7400)
    - 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/to1/

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

San Francisco Bay InfraGard Chapter

www.sfbay-infragard.org