THE "NEW NORMAL" IN CYBER CRIME

U. S. Attorney Office
Northern District of Texas
March 2013

What Is Cybercrime?

- Hacking
- DDOS attacks
- Domain name hijacking
- Malware
- Other computer related offenses, i.e. computer and internet used to facilitate criminal conduct

Federal Cybercrime Prosecutors

Computer Hacker – Intellectual Property – Crimes Unit = CHIPS

Created in 2001 in 10 cities including Dallas

CHIP prosecutors to focus on computer crime cases, assist in law enforcement training and industry outreach

CHIP Prosecutors involved in National Security Cyber Specialist program

What type is your company?

There are two types of companies,

“those who have been compromised and those that soon will be.”

Robert S. Muller III
Director
Federal Bureau of Investigation

What is the Cyber “New Normal”

Real World Cyber Threats
"The New Normal"

- Persistent intrusions by nation states
- Persistent intrusions by hacktivists
- Violations of privacy – both corporate and individual
- Theft of confidential business information
- Degradation and denial of service to legitimate businesses by DDOS attacks

Example: DDOS Attacks In The “New Normal”

- DDOS = Distributed Denial of Service
- More powerful, sophisticated and persistent
  - 100 gigabyte/sec
  - Designed to overwhelm with active requests
  - Still limited in impact

What's the government's role in the "New Normal?"

- A significant amount of malicious online activity of all types comes from overseas, (e.g. China, Eastern Europe, Middle East)
- It's the gov. responsibility to defend the U.S. from foreign attacks
- Gov. now focused on helping you help yourself by prevention.
- Cyber Exec. Order in Feb. 2013

Cybersecurity Executive Order

- Executive order, Improving Critical Infrastructure Cybersecurity, Feb. 12, 2013
- http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure;cybersecurity
- Directs gov. agencies to share info about cyber threats with the targets of those threats and directs NIST to establish standards to improve cybersecurity

Gov. Role In Preventing Cyber Threats—Info Sharing

- Cyber threats are a national security priority
- Gov. shares actionable info with private sector, i.e. hundreds of thousands of cyber signature and indicators shared with private sector and other nations in 2012
- Executive Order requires redoubling of the gov. effort

Gov. Role In Preventing Cyber Threats--Info Sharing, Cont'd

- Expands Enhanced Cyber security Services for critical infrastructure beyond U.S. defense industrial base
- Provides intrusion signatures to firms or their ISPs to help counter known malicious cyber activity.

Gov. Role in Prevention of Cyber Threats, Cyber Security Stds.

- Nat. Instit. Of Stds. And Tech. (NIST) to develop "Cybersecurity Framework" to reduce risks to critical infrastructure
- Develop standards, methodologies, procedures, best practices and process to address cyber risks
- Identify areas for improvement
- Technology neutral guidance
- Voluntary Critical Infrastructure Cyber security Program

National Security Cyber Specialists (NSCS)

- NSCS Network = Federal Prosecutors
- Work to develop relationships with private sector and other entities that have been or could become targets of national security cyber threats, e.g. cleared defense contractors, law firms, technical security companies, critical infrastructure companies.

NSCS Network Cont'd

- Respond to calls about cyber incidents
- Detect, deter and disrupt cyber threats by prosecution
- Emphasize that information received in an investigation will be treated with discretion afforded to sensitive national security info
- Discuss with targets ways to improve gov. response and cybersecurity efforts

What Is Your Role?

- Prepare for the worst—hope for the best. Treat any intrusion as a national security matter
- Senior management needs to understand the risk and business impact of various cyber events
- Participate in an information sharing organization (Ex: InfraGard)
- Use modern network defense best practices and technologies

What Is Your Role?, Cont'd

- Test your cyber security incident response plans – have contingencies in place with service providers should those plans fail
- Have robust cyber security policies and training programs
- Continuously monitor networks under the assumption that they have been breached

What Is Your Role, Cont'd

- Develop strong community-based response capabilities, such as the cyber equivalents of mutual assistance agreements.
- Prepare your Cyber Attack Packing List
- Follow the Cyber Attack Mitigation Tips

FBI Cyber Attack Packing List:

- Point of Contact for Legal, Technical and Project Management
- Legal Banner/Computer Use Agreement
- Employee Handbook/Corporate Policies
- Network Topography Maps
- Internal and External IP address and Host lists

Cyber Attack Packing List Cont'd:

- List of Network Devices (switches, routers, other devices)
- Incident Logs (Security, Host, IDS, Web, Database, Network)
- Archived Network Traffic
- Forensic Images of Compromised Hosts (live memory captures)
- Physical Access logs (video cameras, key cards, TFA devices)
- (Packing List Developed by FBI New York Cyber Branch)

Cyber Attack Mitigation Tips:

- Know your legal agreements with users and partner companies
- Make sure your IT Staff and managing Partners are talking regularly
- Segment your networks (Finance vs. HR/Payroll vs. Case Work)
- Segment your authentication – Two Factor Authentication

Cyber Attack Mitigation Tips, Cont'd:

- Application Security
- Security vs. Productivity
- Remember: Any network link is a potential intrusion vector
- Have at least 2 to 3 IT staff members trained in cyber incident response
- Contact the FBI as soon as an intrusion is identified.
- (Tips Developed by FBI New York Cyber Branch)

Two Types of Companies

- There are two types of companies: those who have been hacked and those who will be.
- So when---not if---your company is the victim of a cyber intrusion, please contact your local FBI office 972-559-5000 and ask to speak with an agent on the Cyber Task Force.

Federal Agency Contacts

- FBI at 972-559-5000 to report a cyber intrusion. Ask for Cyber Task Force agent.
- To mitigate the effects of a cyber intrusion contact CERT (U.S. Computer Emergency Readiness Team) https://forms.us-cert.gov/report/ or 888-282-0870.

Federal Agency Contacts Cont'd

- Contact NSCS Representative AUSA Linda Groves or AUSA Candina Heath at 214-659-8600 to report a cyber intrusion, or NSCS (National Security Cyber Specialists) NSCS_Watch@usdoj.gov.

And Now, A Word About INFRAGARD

FBI Special Agent Mark I. Ducatel

Membership Info at www.ntinfragard.org

INFRAGARD

- FBI Squads of trained agents in sixteen cities including Dallas. FBI Cyber squad investigates only computer crimes.
- InfraGard Program developed by FBI in 1998 to protect critical U.S. infrastructure, e.g. utilities, communications, transportation and government services. 150 private sector members in Dallas.
- FBI Special Agent Mark Ducatel

For More Information

- Linda Groves, Deputy Criminal Chief, Economic Crimes Section, 214.659.8600, Linda.Groves@usdoj.gov
- Candina Heath Assistant U. S. Attorney, Economic Crimes Section, 214.659.8600, Candina.Heath@usdoj.gov