FBI and Cyber Security for ICS/SCADA Systems

Federal Bureau of Investigation
SSA G. Thomas Winterhalter, Jr.
Cyber Division
Overview

- FBI Mission
- Cyber Threats
- FBI Response
- What is the FBI seeing?
Mission

1. Protect the United States from Terrorist Attack.
2. Protect the United States against foreign intelligence operations and espionage.
3. Protect the United States against cyber based attacks and high technology crimes.

Proactive vs. Reactive
Mission: Coordinate, supervise and facilitate the FBI's investigation of those federal violations in which the Internet, computer systems, or networks are exploited as ... targets of terrorist organizations, foreign government sponsored intelligence operations, or criminal activity;
Mission

- Identify and neutralize the most significant individuals or groups conducting computer intrusions, the dissemination of malicious code, and/or other computer supported operations.

- The FBI is the only U.S. agency charged with the authority to investigate both criminal and national security computer intrusions.
Cyber Threats - Three View Points

"All the regulated industries--the electric utilities, the gas pipelines and oil refineries, the water and transportation systems--are still vulnerable to cyber attack."

- Richard Clarke

"The idea that hackers are going to bring the nation to its knees is too far-fetched a scenario to be taken seriously."

- James Lewis

“The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards.”

- Gene Spafford
The Risk Equation

Risk = Threat x Vulnerability x Consequence

• Threat: Any person, circumstance or event with the potential to cause loss or damage.

• Vulnerability: Any weakness that can be exploited by an adversary or through accident.

• Consequence: The amount of loss or damage that can be expected from a successful attack.

- Mark Fabro, INL
Criminal Cyber Threats

- Exploitation of Resources (Botnets)
- ACH Fraud
- Extortion
- Insider Threats
Cyber Terrorism

- No full-scale cyber attacks.
  - DDOS
  - Defacements

- Growing presence of terrorist organizations on the internet.
  - Internet being used not to just recruit or radicalize, but to incite.

- Growing use of social networking sites to collaborate and promote violence.
Counterintelligence and Economic Espionage

- Espionage used to be spy vs. spy.
  - Today our adversaries can sit on the other side of the globe and have access to an entire network at their fingertips.

- Who are they?
  - Nation-State Actors
  - Mercenaries for Hire
  - Rogue Hackers
  - Transnational Criminal Syndicates
Counterintelligence and Economic Espionage

- What are they after?
  - Technology
  - Intelligence
  - Intellectual Property
  - Military Weapons
  - Military Strategy

- They have everything to gain; we have a great deal to lose.
Counterintelligence and Economic Espionage

- Who is doing it? Which nation-state poses the greatest danger of a cyber attack?
  - To an extent ... this is an irrelevant question.
  - Information is being lost at an enormous rate.
  - Whether it is political, ideological, or financial, the information may be bought and sold by anyone, anywhere in the world, whether friend or foe.
Level One
Ankle biter or Script Kiddies
The careless Beginner
Obvious publicly available tools.

Level Two
Black Hat Criminal Hacker
Sophisticated and crafted tools with some “Zero Day.”
The careful expert
QUIET

Level Three
State Actor, Insider with Valid Credentials, Higher sophistication.
Working at multiple network layers
Zero-Day, supply chain, and worse…
SILENT
General Methodology

- **Initial Effort**
  - Reconnaissance
    - Profiling Targets
    - Scanning and Mapping
  - Exploitation
    - Intrusion of Hosts
    - Establishing Foothold
  - Exfiltration
    - Aggregation of Materials
    - Removal of content to Remote network
  - Persistence
    - Backdoors, Obtain valid credentials
  - Denial & Deception
    - Modification of logs, cleanup of staging files
Detection

Operational Sophistication

Technical Sophistication

Scanning → Intrusion → IDS → Firewall → Valid Credentials → Insider Support → Persistence → Statistical Signal Analysis
Attack Sophistication vs. Intruder Technical Knowledge

- Tracking and Tracing Cyber-Attacks: Howard F. Lipson
Primary Intrusion Vectors

“The exploitation of Trust”

- The trusted inbound e-mail.
- The publicly available trusted web site of appropriate business interest.
- The download of trusted code from a trusted and authorized vendor.
- The trusted outward facing server.
- The necessary trust of the internal network.
- The connections with trusted business partners.
Trusted E-mail

- Email contains attachment or link which recipient is likely to open.
- Crafted to appear to come from a trusted source
- Attachments tailored to recipients likely interest
- Broad address and personnel information are available open source.
Trusted Web Site

- Intrusion into web site with an identifiable user base.
- Modification of lead web page
- Redirection to poorly administered web site for code download.
- Deployment of tool through browser begins beaconing activity.
Trusted Applications

- Intrusion into software vendor or other trusted site
- Modification of code which is otherwise trusted and authorized
- Tool deploys when authorized software package is installed
- Again, tool supports beaconing activity.
Trusted Server

- Intrusion through a Web Server to a backend server like a database (SQL Injection).
- Server is trusted, and often improperly located within internal network.
- Excess trust granted because server is internal.
Trusted Relationships

- Intrusion through a trusted business partner
- Friendly party is intruded - access is likely to appear to have valid credentials
- Daisy-chain of trusts - Problem exacerbated by promiscuity of business networks
Significant Consequences

- Obfuscated Exfiltration of Data
- Subsequent exploitation of internal networks
- Reconnaissance
- Persistence
- Subtle
Key Elements of Association

- Similarity or identity of exploit, access and command and control tools
- Tactics, Techniques and Procedures
- Totality of Circumstances
- Attack vectors
- Target Analysis
- IP address range
- Routing
Exfiltration

- Once access is gained, intruders begin reviewing network
- Broad collection effort begins with aggregation of file lists and escalates to volumes of proprietary data
- Use of permitted protocols for removing volumes of data from the victim network
Persistence
What we DON’T see...

- Network presence can and does exceed security methods
- Advanced zero-day code, and the use of valid credentials may be impossible to detect with data forensics alone
- Persistent presence
- Exploitation as opposed to just exfiltration
Reporting

- Many significant intrusions are NOT viewed as criminal matters which might expose a victim to publicity.

- Because of the nature of some of these threats, if you see it, you are almost certainly not alone.

- We need information to aid in mitigation and defense of others - Like a ship taking on water, this problem spreads...
Damage Assessment

- Don’t stop at the identification of the intrusion vector
- Immediate clean-up may remove the intrusion but leave the persistent presence
- You may miss the shift from a lower noise level intrusion to a higher order exfiltration effort.
- If possible, determine the depth of the intrusion before wiping machines.
FBI Response

What the FBI can do

- **Investigate**
  - National and global
  - Combine technical skills and investigative experiences
  - Long-term commitment of resources

- **Forensics (RCFL)**

- **Patterns and Links**

- **Bring national security concerns to intelligence community**
FBI Response

- 56 Field Offices with Cyber Squads.
- 60 FBI Legal Attaché Offices around the world.
- Cyber Trained Agents embedded with foreign police forces.
National Cyber Investigative Joint Task Force

Cyber Action Team

Groups that are focusing on key threats and trends.

- These groups consist of agents, officers, and analysts from different agencies.
- ICS/SCADA TFC – FBI, DHS, and OGA partnering together.
- Establishing cooperative working relationships with regulatory groups and agencies.
  - InfraGard
What is InfraGard?

- InfraGard is a partnership between the FBI and the public and private industry.
- Includes business executives, entrepreneurs, military and government officials, computer professionals, academia, state and local law enforcement and concerned citizens.
- It encourages sharing information between the government and the private sector for the purpose of protecting the national critical infrastructure.
InfraGard and the FBI

Two way information flow

With the goal of protecting our Critical Infrastructures
InfraGard’s Mission & Goals

- Information sharing to reduce threats and vulnerabilities to critical infrastructures

- Develop and support a partnership with InfraGard members and the FBI to support all FBI investigative programs
FBI Program vs Private Sector

- Provide vetting for membership
- Provide Secure Infrastructure
- Provide Law Enforcement Sensitive (LES) Intel Products
- Conduit for Investigations

MOU

Information Flow

- Self govern
- Identify Subject Matter Experts (SMEs)
- Provide non-government Intelligence
- Liaise with other Government Agencies
- Marketing/Fundraising
- Education
How is Information Shared?

- InfraGard uses a secure web site to communicate with members

- Website Contains:
  - Department of Homeland Security (DHS) threat alerts, warnings, and vulnerabilities
  - Intelligence Bulletins
  - FBI Agents assigned to each Chapter, bring meaningful news and information
FBI’s Structure of InfraGard

- Supervised by the Public/Private Alliance Unit (PPAU), Strategic Outreach & Initiatives Section, Cyber Division
- Nationally, there are over 33,000 members comprising 86 InfraGard Chapters
- Each field office has a Special Agent InfraGard Coordinator who is a point of contact for the IMA and who recruits and vets new members
- Special Interest Groups
Why Should I Share Information with InfraGard?

- InfraGard provides an avenue to share information with a vetted membership that wants to help the FBI and get feedback.
- Some of the members are experts in their field.
- Members may see similar activity and report it to their local field office.
How to Apply for InfraGard

- Visit the public website, www.infragard.net
- Click on “Become A Member”
  - Meet membership requirements.
- Fill out the application in a writeable pdf format and mail it to your local FBI Field Office or bring it to your Chapter Coordinator
FBI Response

What the FBI cannot do

“We cannot investigate if we are not aware of the problem”

- FBI Director Robert S. Mueller, III

And...

The FBI must work within the framework of the law.

....which can take time.
FBI Response

What the FBI won’t do

- Take over your systems.
- Repair your systems.
- Share proprietary information with competitors.
- Provide investigation-related information to the media or shareholders.

- In essence … we will not further victimize the victim.
What is the FBI seeing?

- Davis Besse Nuclear Power Plant
- Maroochy
- California Offshore Oil Rig
- Carrell Clinic HVAC
- Los Angeles Traffic Lights
- Company network diagrams viewable to the public on their website.
What is the FBI seeing?

- Theft of Service
  - Company reported that smart meters being modified to steal service. Estimated yearly losses are approximately $400 Million.
  - We are working with the company, the ES-ISAC, and NERC to ensure that the appropriate information is disseminated up and down the chain.
  - We are working with the company to identify what the modifications may have exposed the network to.
What is the FBI seeing?

- Report provided from ES-ISAC and DOE:
  - Single unauthorized packet was dropped and logged as reaching the external interface of a firewall protecting NERC CIP critical cyber assets at a utility company.
  - Port 0 and source address of a foreign country that is often viewed as a threat.
  - Approximately two weeks later similar packet discovered with a different source address from a country that is viewed as benign.

Company has applied rules to firewall and is not seeing the packets anymore.
What is the FBI seeing?

- Agents in the field are approaching companies across all facets based on information and intelligence to report possible breaches.
- In circumstances where key critical infrastructure companies are affected we are working cooperatively with DHS to ensure both a “law enforcement perspective” and “protection perspective” are represented.
FBI Director Mueller at RSA:

“No one country, company, or agency can stop cyber crime. A “bar the windows and bolt the doors” mentality will not ensure our collective safety. Fortresses will not hold forever; walls will one day fall down. We must start at the source; we must find those responsible.

“The only way to do that is by standing together. Together we can find better ways to safeguard our systems and stop those who would do us harm. For ultimately, we face the same threat. We both serve the American people. And we must continue to do everything we can, together, to minimize these attacks.”