National Electric Sector
Cybersecurity Organization

Cybersecurity Landscape for the Utility Industry and Considerations for State Regulators

Chairman's Forum on Cybersecurity
and Critical Infrastructure

Kentucky Public Service Commission, Hearing Room One
January 25 2012 Frankfort, KY

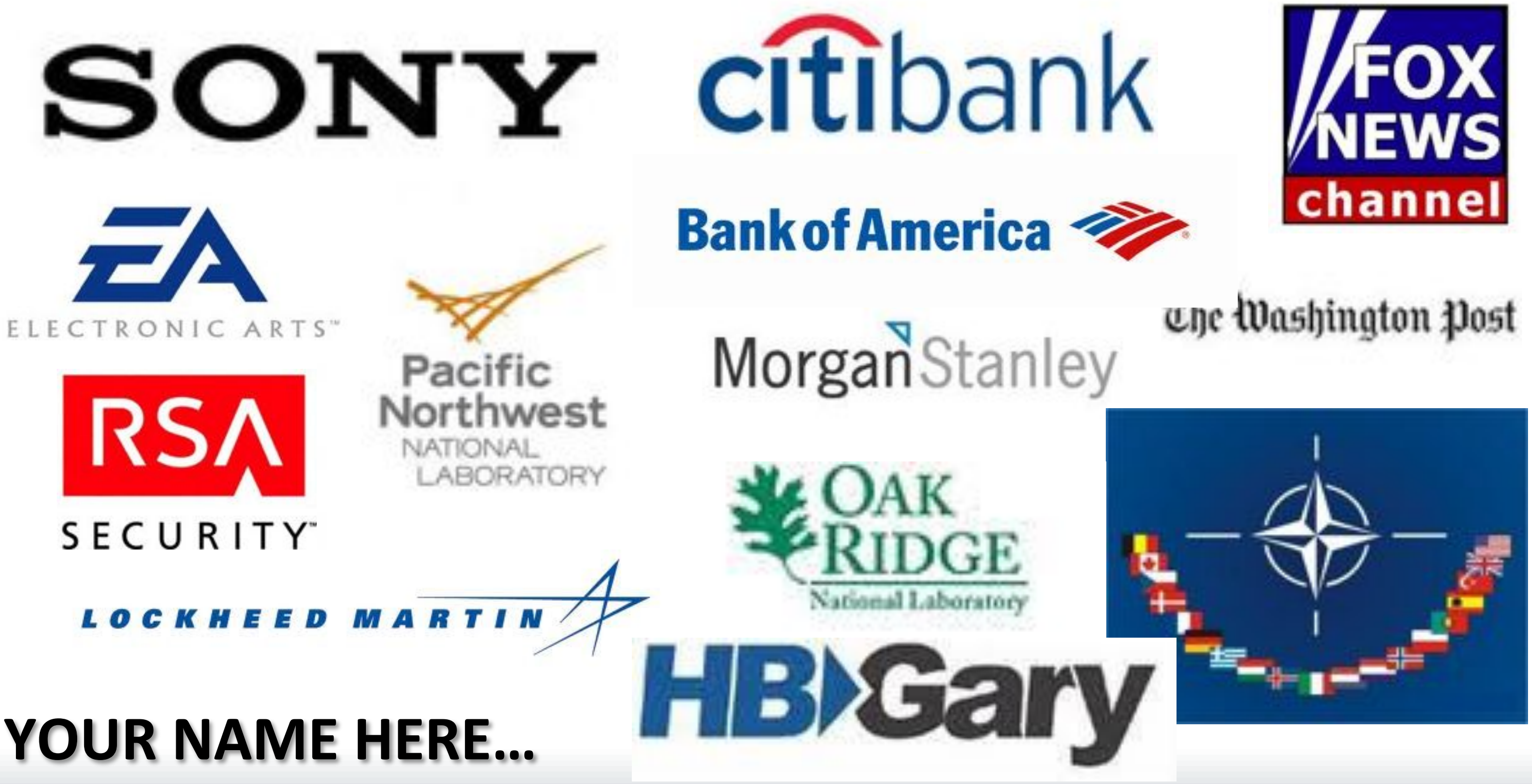
SPECTRUM OF CYBER THREATS TO OUR BULK POWER AND DISTRIBUTION SYSTEMS

Advantage: Adversaries

Motivated, adaptive adversaries exist, and they don't follow the rules or regulatory checklists

The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

Advantage: Adversaries



YOUR NAME HERE…

Technology Landscape

- Emergent intelligence
- A new digital world order
- Widespread connectivity
- Hyper-embeddedness
- Lingering legacy

The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

Regulatory Landscape

- Smart Grid interoperability
- Compliance vs. Security
- Data breach disclosure
- Vendor, utility responsibility
- Intelligent islanding

The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

Cybersecurity Landscape

- Research, espionage, organized crime, warfare
- Nation state quality defense is the new norm
- Isolation is extremely difficult
- Bolt-ons are complex
- Cyber-kinetic impacts

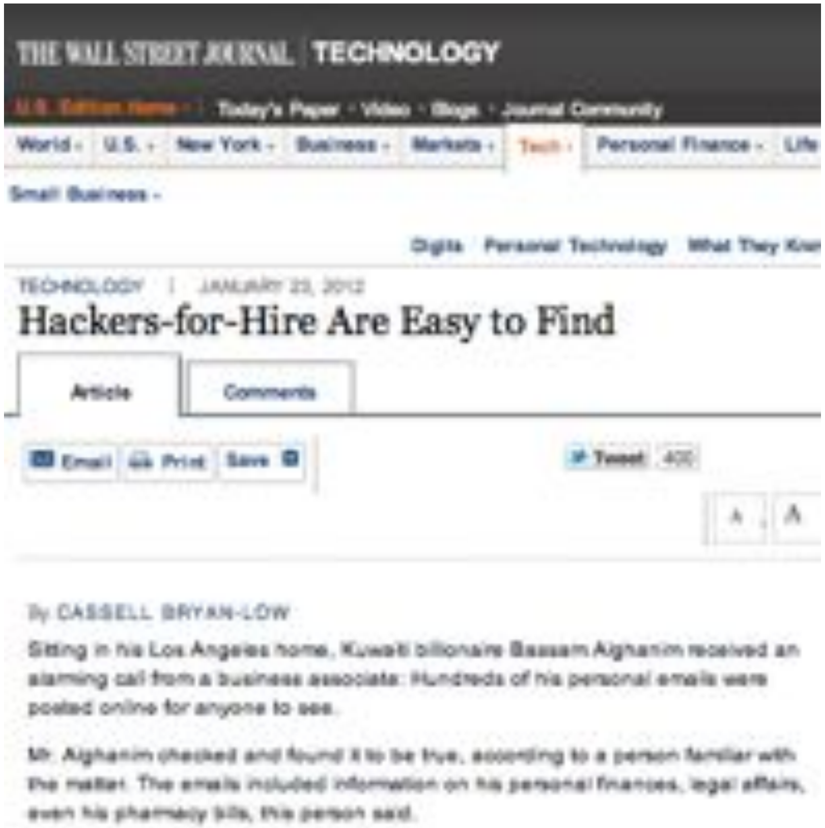
The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

Cybersecurity Landscape

- Aurora
  - – Demonstration of cyber-kinetic attack on generator
- Stuxnet
  - – “Most sophisticated malware…”
  - – “Game changer…”
- Duqu
  - – Industrial equipment target

The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

Cybersecurity Landscape


THE WALL STREET JOURNAL | TECHNOLOGY
U.S. Edition Home | Today's Paper · Video · Blogs · Journal Community
World · U.S. · New York · Business · Markets · Tech · Personal Finance · Life
Small Business
Digits | Personal Technology | What They Know
Article
Comments
Email
Print
Save
Tweet
400
A
A

TECHNOLOGY | JANUARY 23, 2012

Hackers-for-Hire Are Easy to Find

By CASSELL BRYAN-LOW

Sitting in his Los Angeles home, Kuwaiti billionaire Bassam Alghanim received an alarming call from a business associate: Hundreds of his personal emails were posted online for anyone to see.

Mr. Alghanim checked and found it to be true, according to a person familiar with the matter. The emails included information on his personal finances, legal affairs, even his pharmacy bills, this person said.

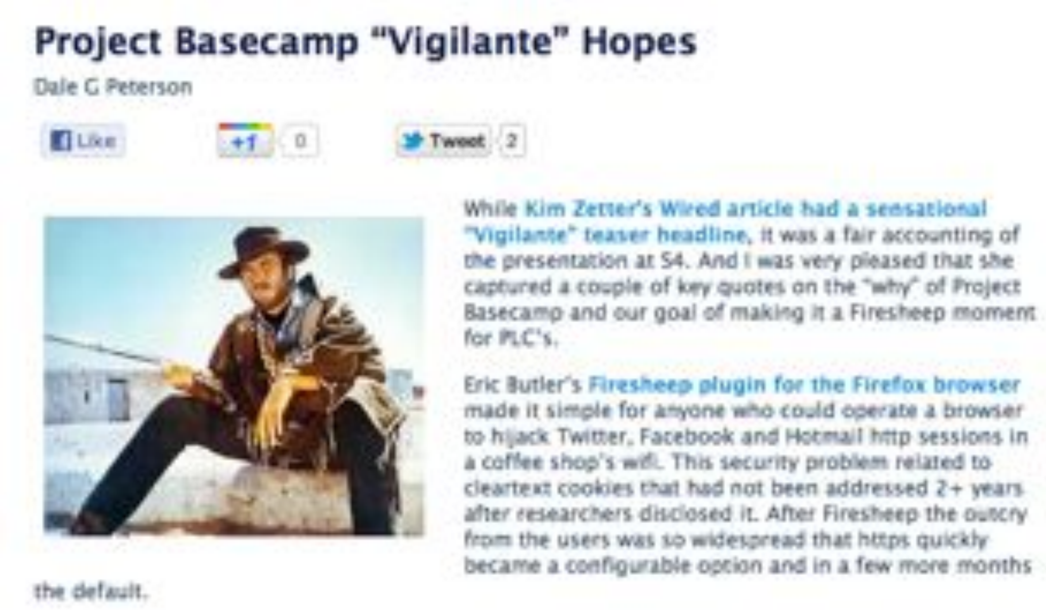
"Mr. Alghanim's lawyers allege in court filings that his brother hired investigators to illegally access his email with the help of Chinese hackers. ***Cost to hire the hackers: about $400.****"*

One such site, hiretohack.net, advertises online services including being able to "crack" passwords for major email services in ***less than 48 hours. It says it charges a minimum of $150***

http://online.wsj.com/article/SB10001424052970203471004577145140543496380.html

The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

Vulnerability Disclosure

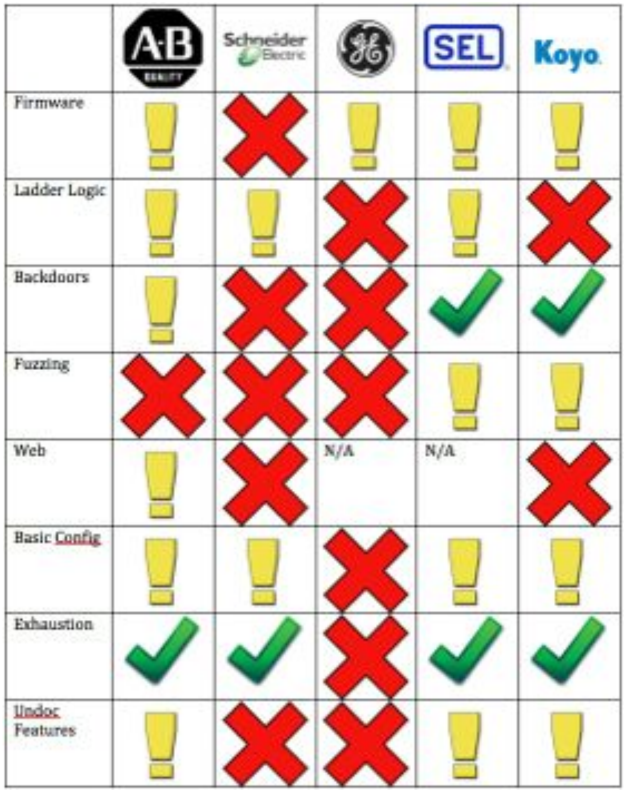


Project Basecamp "Vigilante" Hopes

Dale G Peterson

While Kim Zetter's Wired article had a sensational "Vigilante" teaser headline, it was a fair accounting of the presentation at S4. And I was very pleased that she captured a couple of key quotes on the "why" of Project Basecamp and our goal of making it a Firesheep moment for PLC's.

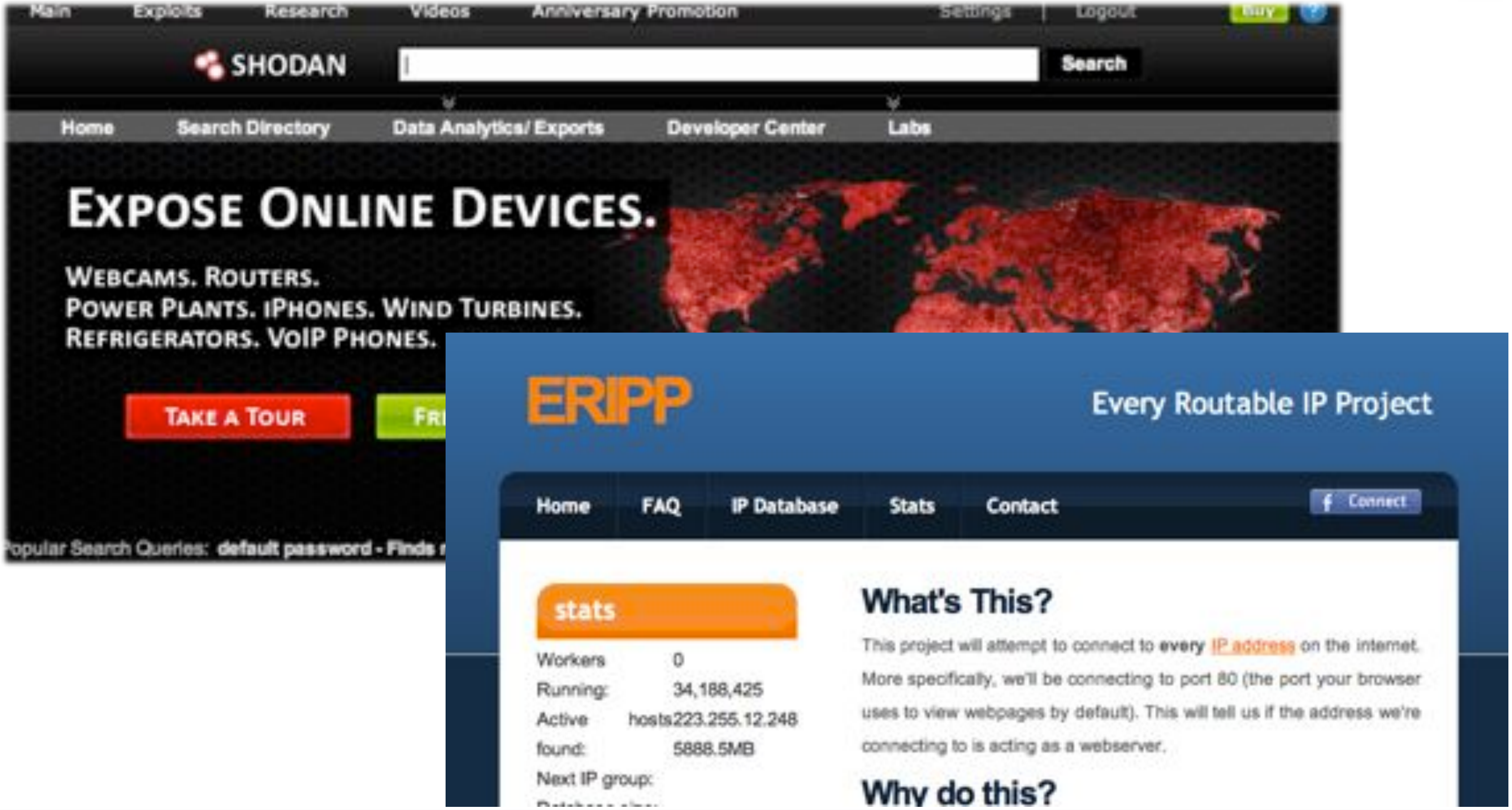
Eric Butler's Firesheep plugin for the Firefox browser made it simple for anyone who could operate a browser to hijack Twitter, Facebook and Hotmail http sessions in a coffee shop's wifi. This security problem related to cleartext cookies that had not been addressed 2+ years after researchers disclosed it. After Firesheep the outcry from the users was so widespread that https quickly became a configurable option and in a few more months the default.



	AB	Schneider Electric	GE	SEL	Koyo
Firmware	!	✗	!	!	!
Ladder Logic	!	!	✗	!	✗
Backdoors	!	✗	✗	✓	✓
Fuzzing	✗	✗	✗	!	!
Web	!	✗	N/A	N/A	✗
Basic Config	!	!	✗	!	!
Exhaustion	✓	✓	✗	✓	✓
Undoc Features	!	✗	✗	!	!

Source: www.digitalbond.com

Anonymous Reconnaissance



Expose Online Devices.

Webcams. Routers.
Power Plants. iPhones. Wind Turbines.
Refrigerators. VoIP Phones.

opular Search Queries: **default password - Finds r**

Every Routable IP Project

stats

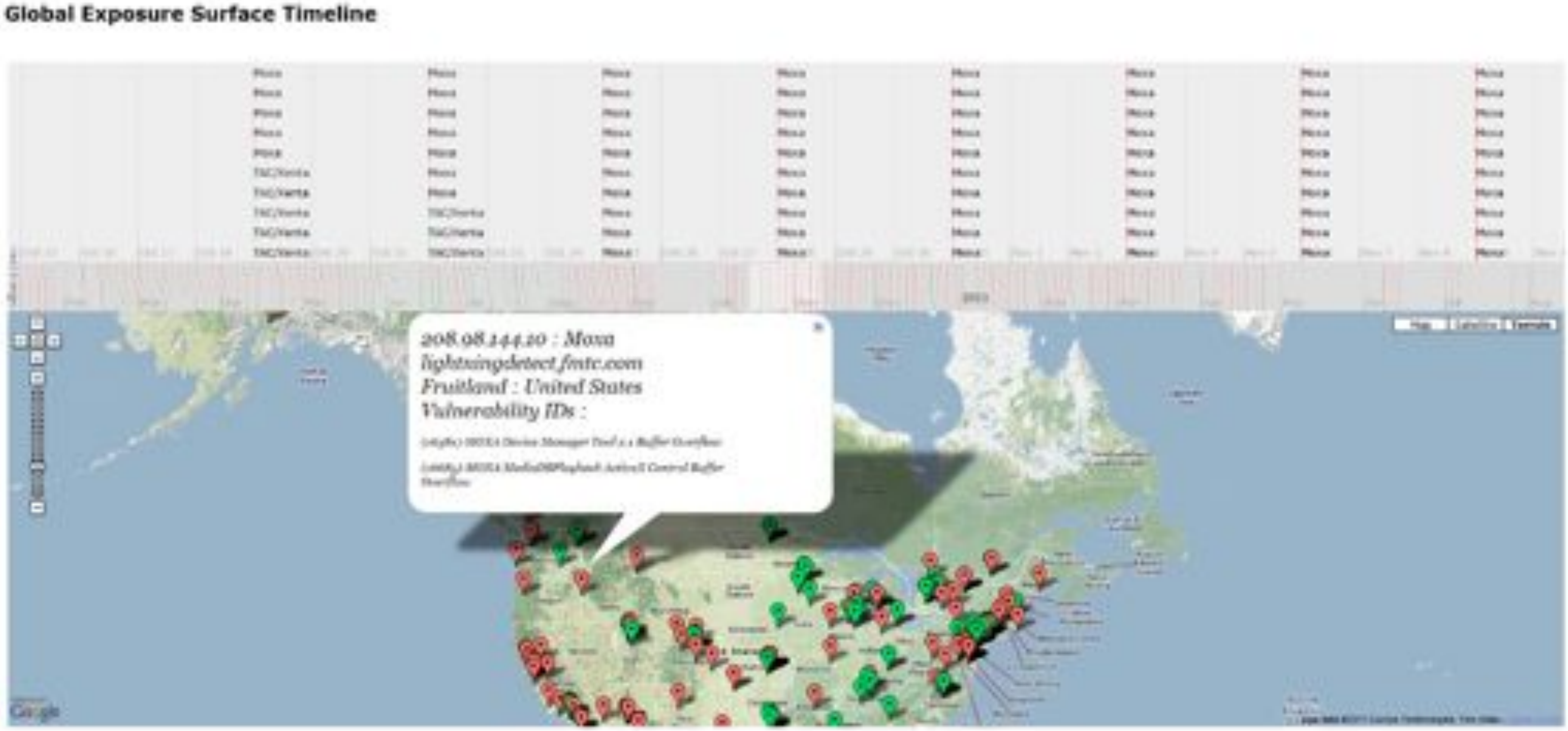
Workers 0
Running: 34,188,425
Active hosts 223.255.12.248
found: 5888.5MB
Next IP group:

What's This?

This project will attempt to connect to **every** IP address on the internet. More specifically, we'll be connecting to port 80 (the port your browser uses to view webpages by default). This will tell us if the address we're connecting to is acting as a webserver.

Why do this?

10,000 Reasons to Worry



Global Exposure Surface Timeline

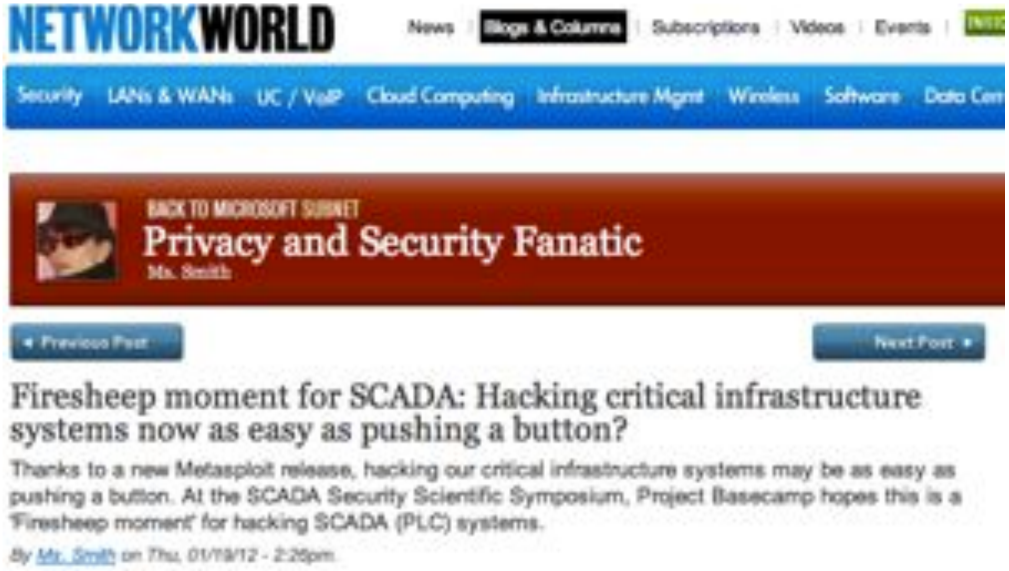
208.08.144.20 : Moxa
lightningdetect.fmtc.com
Fruitland : United States
Vulnerability IDs :

([illegible]) MOXA Device Manager Tool 2.1 Buffer Overflow

([illegible]) MOXA MediaDBPlayback ActiveX Control Buffer Overflow

Source: www.wired.com/threatlevel/2012/01/10000-control-systems-online

Push of a Button



Firesheep moment for SCADA: Hacking critical infrastructure systems now as easy as pushing a button?

Thanks to a new Metasploit release, hacking our critical infrastructure systems may be as easy as pushing a button. At the SCADA Security Scientific Symposium, Project Basecamp hopes this is a 'Firesheep moment' for hacking SCADA (PLC) systems.

By Ms. Smith on Thu, 01/19/12 - 2:26pm

Source: Network World (http://goo.gl/K5xZ7)

*"In some scarier than your average security news, thanks to several Program Logic Controllers (PLC) exploits that were added to Metasploit today, "**hacking SCADA systems can be push of a button easy,**" tweeted HD Moore, CSO of Rapid7 and Chief Architect of Metasploit."*

The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

Is There a Solution?

- Equipped, empowered and engaged people
- Protection, detection, response
- Defense in depth
- Drills, exercises
- Options, spares

The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

CONSIDERATIONS FOR STATE REGULATORS

The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec
with funding assistance from the U.S. Department of Energy.

Nothing New Under The Sun

- Mature security practices; highly refined
  - Defense in Depth
  - Principle of Least Privilege
  - Segregation of Duties
  - Need to Know
  - Availability, Integrity and Confidentiality
- No Silver Bullet, 100%, Total Security
- Strong protection has never been easy, inexpensive or quick to implement (pick two)

Art vs. Science

"…security is an art – and you cannot legislate art."

Bill Bryan, Deputy Assistant Secretary of Infrastructure Security & Energy Restoration, US DOE

What Can State Regulators Do?

- Get and stay **educated**
- Strategic **communication**, in all directions
- Work **collaboratively** with utilities
- Support measures to get **actuarial data**
- Support secure **procurement** measures
- Support appropriate **staffing** levels
- Support security **training/education**

The National Electric Sector Cybersecurity Organization (NESCO) is operated by EnergySec with funding assistance from the U.S. Department of Energy.

What Can State Regulators Do?

- Ask questions…
  - Who is ultimately responsible for cybersecurity in your organization?
  - How many dedicated security staff do you have?
  - What security training/education/awareness are you providing to all staff and how often?
  - Are you participating in local, state, regional, national security/disaster or energy assurance exercises?
  - Are you using the DHS/MS-ISAC Procurement Language or IEC 62443?

What Can State Regulators Do?

- More questions…
  - Where do you get your situational awareness data?
  - What cybersecurity technologies do you use (general platforms, not specific technologies)?
  - How frequently do you performed an exhaustive inventory of all control systems and associated communication links?
  - Can the ICS networks be intelligently islanded from corporate networks and the Internet?

Protect Your Own

- State Commission systems may be targets
  - Sutton's rule: "because that's where the money is"
  - What type of information are you asking for?
  - How much of it do you keep?
  - How much should be public vs. classified/non-public?
- How are you protecting your systems and data?
- Do you go through security reviews?
- What if you made the front page?

Good Communication

- Ratepayers want a secure grid, until they see the costs (both capital and operational)
- “Common Practice” vs. “Best Practice”
- Early and regular, fact-based communication can minimize negative public reaction
- Remind ratepayers that smart, informed decisions are being made
- Stay well-informed, **things change fast**

Questions…

Patrick C Miller
President & CEO, EnergySec
Principal Investigator, National Electric Sector Cybersecurity Organization
patrick.miller@energysec.org
503.446.1212 (desk)
@patrickcmiller (twitter)
www.energysec.org