New York State Energy Planning Board

Cyber Security
and the
Energy Infrastructure

New York State
Division of Homeland Security and
Emergency Services
Office of Cyber Security

Office of Cyber Security Overview

- Established as the Office of Cyber Security and Critical Infrastructure Coordination in September 2002

- Responsible for leading the State's efforts regarding cyber security readiness and critical infrastructure coordination

- Operates on the principles of collaboration and cooperation

WHAT IS HAPPENING IN 2012?

- Cyber incidents reported by the owners and operators of critical infrastructure were up over 200% from FY 2010.
  - DHS Control Systems Security Program, Year in Review, October, 2011

- “Cyber search engine Shodan exposes industrial control systems to new risks”
  - Washington Post, June 3, 2012

WHAT IS HAPPENING IN 2012?

- Andrew James Miller was arrested for trying to sell access to two National Energy Research Scientific Computing Center supercomputers for $50,000.

  - U.S. Department of Justice, June 14, 2012

- "[B]oards and senior management still are not exercising appropriate governance over the privacy and security of their digital assets."

  - Carnegie Mellon University CyLab 2012 Report

Threats and Attacks Have Moved from the Theoretical and Alleged to the Actual

2003 NORTHEAST BLACK OUT

U.S.-Canada Power System Outage Task Force

"…provided sufficient certainty to exclude the probability that a malicious cyber event directly caused or significantly contributed to the power outage events."

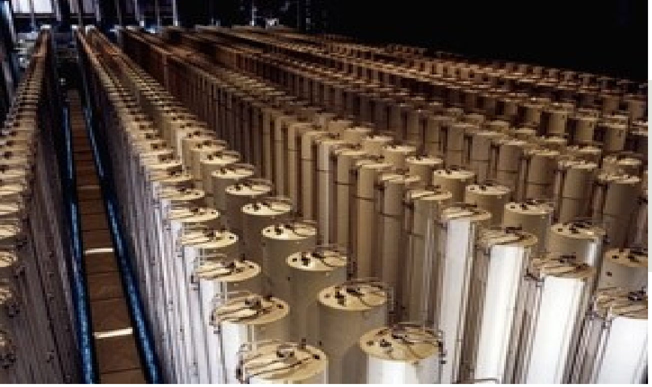
- But –
  - Indications of procedural and technical IT management vulnerabilities were observed in some facilities.
  - A failure in a software program not linked to malicious activity may have significantly contributed to the power outage.

BRAZILIAN BLACK OUTS

Allegations that black outs in 2005, 2007, and 2009 were the result of cyber intrusions.

Notwithstanding speculation by security “experts” and reporting on 60 Minutes, there was no evidence that the disruptions of service were caused by hackers.

AURORA PROJECT



STUXNET

- Stuxnet is a Windows-specific computer worm first discovered in June 2010.
- It is the first discovered worm that spies on and reprograms industrial systems.
- It was specifically written to attack systems used to control and monitor industrial processes used in power plants, oil and gas refineries, factories and so on.
- The worm can be used for both espionage and sabotage.

“Comedy of Errors Led to False ‘Water-Pump Hack’ Report”

Curran-Gardner Public Water District - Springfield, Illinois

- **Widely reported that a malicious cyber intrusion from an IP address located in Russia caused a SCADA system to power on and off, resulting in a water pump burnout.**

- **A detailed analysis by ICS-CERT and the FBI found no evidence of a cyber intrusion into the SCADA system.**

© Copyright Larry Senalik 2011

- **ICS-CERT deployed a fly-away team to the facility to interview personnel, perform physical inspections, and collect logs and artifacts for analysis.**

Intrusion in a Local Government – Unintended Compromise?

- FBI investigation in 2006 disclosed a compromised computer within a local government, apparently to covertly use the computer as a distribution system for e-mails or pirated software.
- The hacker operating on the Internet tapped into an employee’s laptop and then used an employee’s remote access as the point of entry and installed a virus and spyware on the network.
- Administrative network also supports water treatment operations.
- Potential that hackers could have changed critical systems, chemical levels, and operating parameters.

Critical Infrastructure
Growing Awareness, but Uncertain Response

"In the Dark: Crucial Industries Confront Cyberattacks"

- McAfee/Center for Strategic and International Studies

Survey of 200 executives of critical electricity infrastructure:

- Eighty-five percent had experienced network infiltrations.
- Twenty-five percent reported daily or weekly denial-of-service attacks.
- Nearly two-thirds reported they frequently (at least monthly) found malware designed for sabotage on their systems.

Critical Infrastructure
Growing Awareness, but Uncertain Response

"The State of IT Security: A Study of Utilities and Energy Companies" - Q1 Labs/Ponemon Institute

- 291 IT and IT security practitioners in utilities and energy companies participated:
  - Seventy-one percent responded that the management team in their organizations does not understand or appreciate the value of IT security.
  - Forty-one percent indicate that their security operations are not proactive in managing risks associated with SCADA networks and critical infrastructure.

Targeting Critical Infrastructure

“On a daily basis, the U.S. is being targeted.”

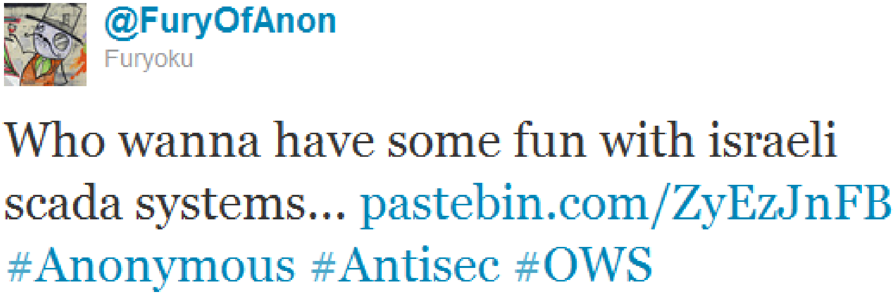
Sanaz Browarny

Chief, Intelligence and Analysis
Control Systems Security Program
U.S. Department of Homeland Security (April 2012)

Results of 2011 ICS-CERT “fly-away“ network and forensics investigations:

- **7 of 17** “fly-away trips” originated as spear-phishing attacks via e-mail against utility personnel.
- **11 of the 17** incidents were very “sophisticated,” signaling a well-organized “threat actor.”
- **12 of 17** cases the **most basic type of network security for corporate and industrial control systems would likely have detected or fended off the attack.**

Targeted by “Hacktivists”



@FuryOfAnon
Furyoku

Who wanna have some fun with israeli scada systems... pastebin.com/ZyEzJnFB #Anonymous #Antisec #OWS

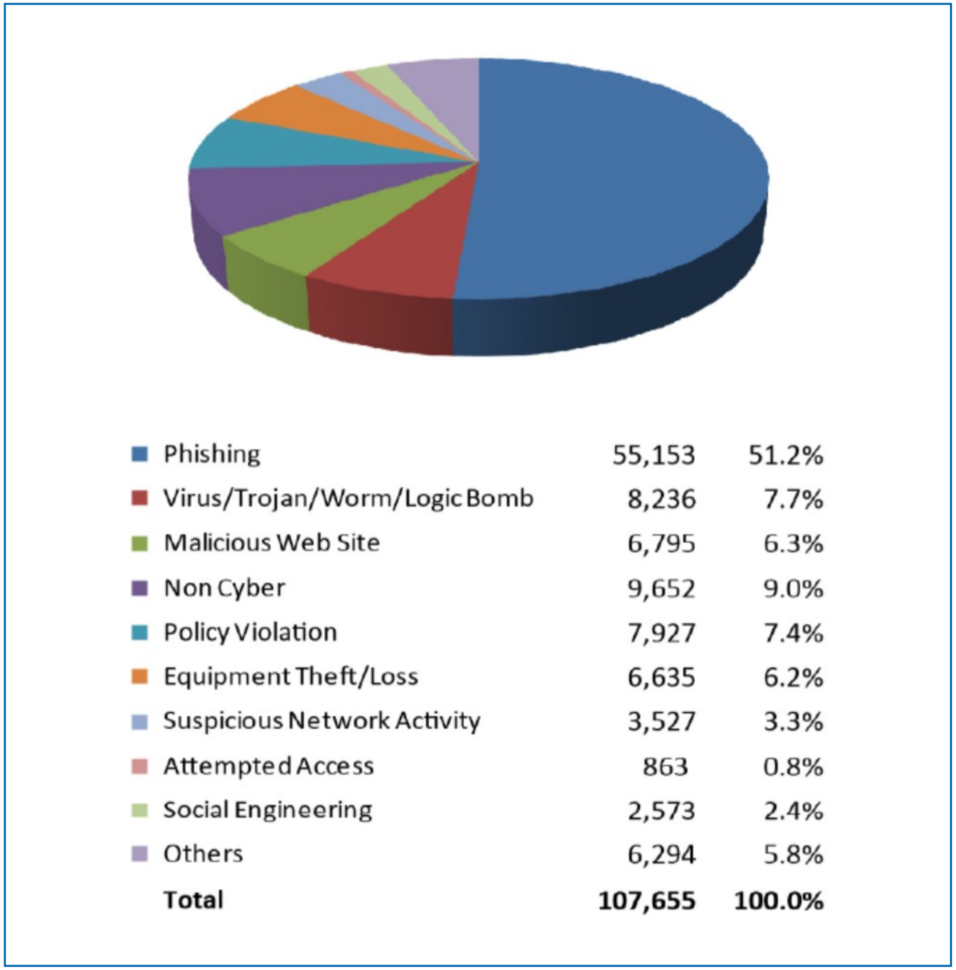
Targeted by Terrorists

Al-Qaeda Video Identifies "Internet Piracy," Attacks On Cyber Infrastructure As Important Parts Of Jihad

Spear Phishing

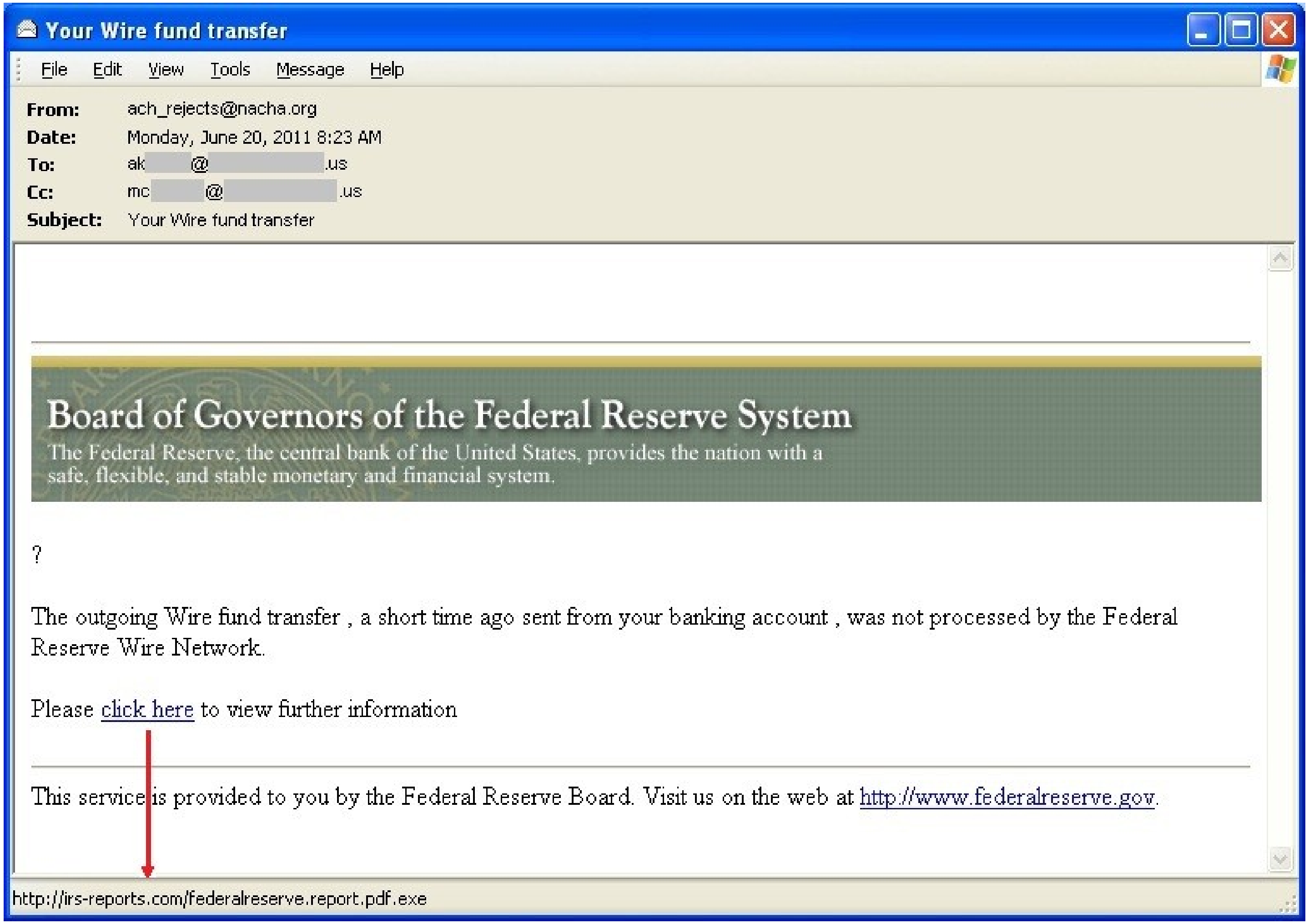
Targeted E-Mails as a Common Attack Vector

US-CERT Statistics for 2011



■	Phishing	55,153	51.2%
■	Virus/Trojan/Worm/Logic Bomb	8,236	7.7%
■	Malicious Web Site	6,795	6.3%
■	Non Cyber	9,652	9.0%
■	Policy Violation	7,927	7.4%
■	Equipment Theft/Loss	6,635	6.2%
■	Suspicious Network Activity	3,527	3.3%
■	Attempted Access	863	0.8%
■	Social Engineering	2,573	2.4%
■	Others	6,294	5.8%
	Total	**107,655**	**100.0%**

Traditional Phishing



From: ach_rejects@nacha.org
Date: Monday, June 20, 2011 8:23 AM
To: ak[redacted]@[redacted].us
Cc: mc[redacted]@[redacted].us
Subject: Your Wire fund transfer

Board of Governors of the Federal Reserve System

The Federal Reserve, the central bank of the United States, provides the nation with a safe, flexible, and stable monetary and financial system.

?

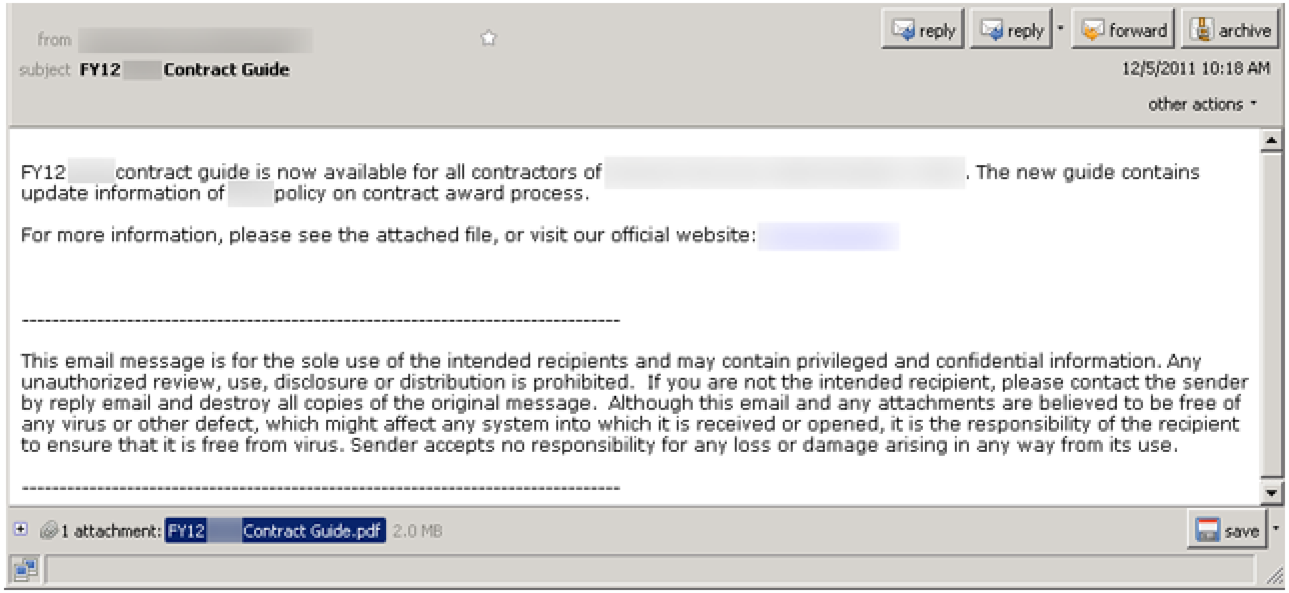
The outgoing Wire fund transfer , a short time ago sent from your banking account , was not processed by the Federal Reserve Wire Network.

Please click here to view further information

This service is provided to you by the Federal Reserve Board. Visit us on the web at http://www.federalreserve.gov.

http://irs-reports.com/federalreserve.report.pdf.exe

Spear Phishing -- Focus on Government Facilities and Contractors



from [redacted]

subject FY12 [redacted] Contract Guide

12/5/2011 10:18 AM

FY12 [redacted] contract guide is now available for all contractors of [redacted]. The new guide contains update information of [redacted] policy on contract award process.

For more information, please see the attached file, or visit our official website: [redacted]

This email message is for the sole use of the intended recipients and may contain privileged and confidential information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message. Although this email and any attachments are believed to be free of any virus or other defect, which might affect any system into which it is received or opened, it is the responsibility of the recipient to ensure that it is free from virus. Sender accepts no responsibility for any loss or damage arising in any way from its use.

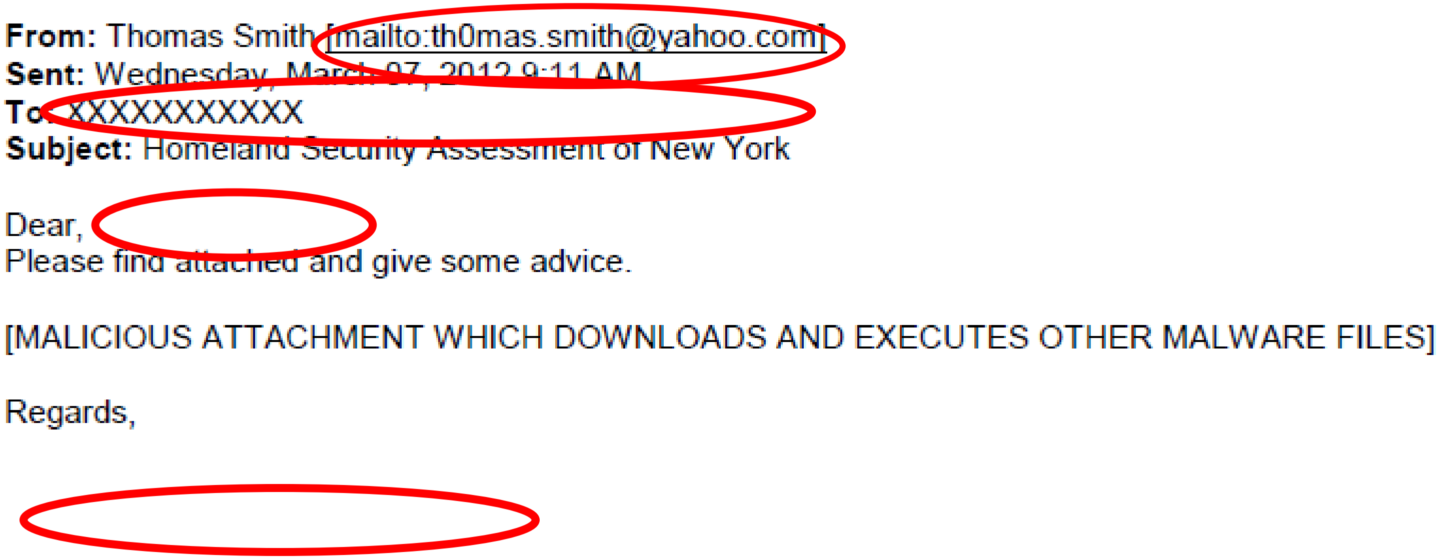
----

1 attachment: FY12 [redacted] Contract Guide.pdf 2.0 MB

In attacks that became public on December 7, attackers created sophisticated, custom attacks on defense contractors and other organizations, with special e-mails and attachments targeting specific individuals within those organizations.

These attacks used a vulnerabilities known as "zero days," which are vulnerabilities that were previously unknown to the developer of the software.

Spear Phishing -- Focus on Government Facilities and Contractors



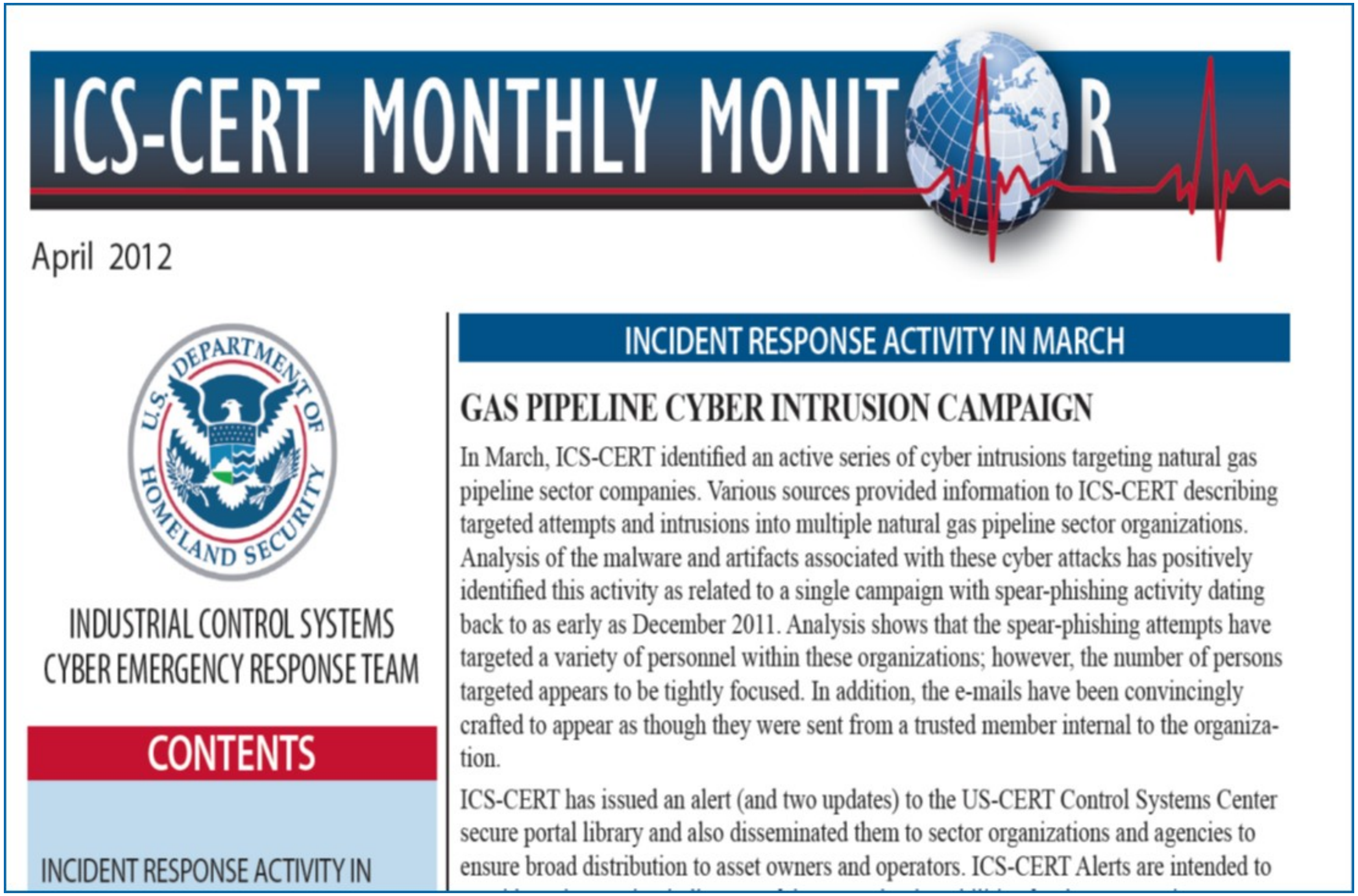
From: Thomas Smith [mailto:th0mas.smith@yahoo.com]
Sent: Wednesday, March 07, 2012 9:11 AM
To: XXXXXXXXXXX
Subject: Homeland Security Assessment of New York

Dear,
Please find attached and give some advice.

[MALICIOUS ATTACHMENT WHICH DOWNLOADS AND EXECUTES OTHER MALWARE FILES]

Regards,

Spear Phishing -- Focus on Industrial Control Systems



ICS-CERT MONTHLY MONITOR

April 2012

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

CONTENTS

INCIDENT RESPONSE ACTIVITY IN

INCIDENT RESPONSE ACTIVITY IN MARCH

GAS PIPELINE CYBER INTRUSION CAMPAIGN

In March, ICS-CERT identified an active series of cyber intrusions targeting natural gas pipeline sector companies. Various sources provided information to ICS-CERT describing targeted attempts and intrusions into multiple natural gas pipeline sector organizations. Analysis of the malware and artifacts associated with these cyber attacks has positively identified this activity as related to a single campaign with spear-phishing activity dating back to as early as December 2011. Analysis shows that the spear-phishing attempts have targeted a variety of personnel within these organizations; however, the number of persons targeted appears to be tightly focused. In addition, the e-mails have been convincingly crafted to appear as though they were sent from a trusted member internal to the organization.

ICS-CERT has issued an alert (and two updates) to the US-CERT Control Systems Center secure portal library and also disseminated them to sector organizations and agencies to ensure broad distribution to asset owners and operators. ICS-CERT Alerts are intended to

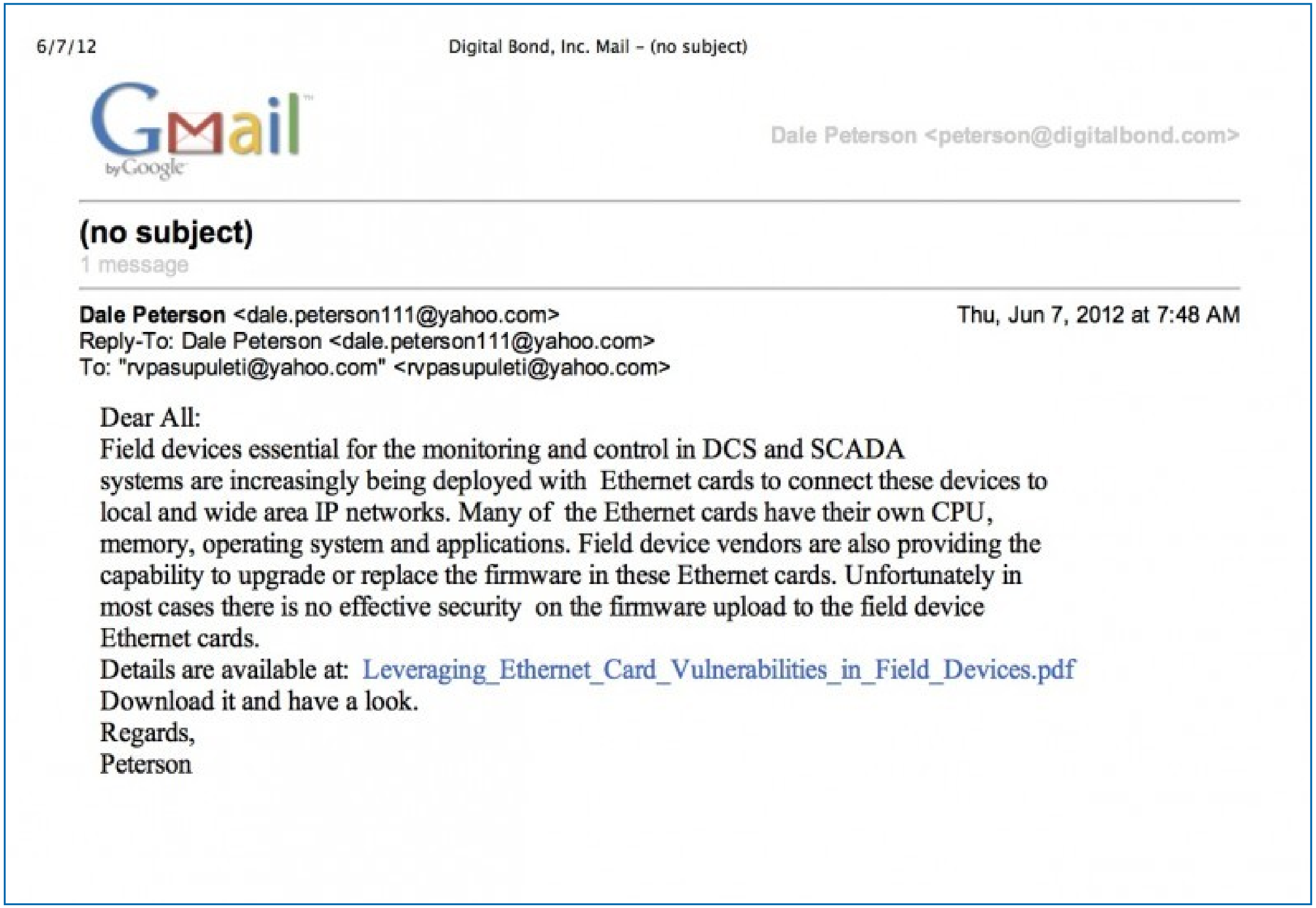
Spear Phishing -- Focus on Industrial Control Systems

ICS-CERT Incident Response Summary Report – 2011 Example

ICS-CERT deployed an incident response team to a bulk electric power organization that had been the victim of a broader **spear-phishing campaign** against the nuclear/energy sectors.

- The point of entry appeared to have been an employee opening a PDF attachment of a **spoofed industry-specific newsletter**, which contained malware.
- **Command and control was positively identified** as part of this analysis.
- ICS-CERT provided indicators and mitigation strategies to this organization to detect further infections on their network and take appropriate defensive measures to combat the threat.
- The recommendations given to this organization also included security recommended practices and mitigation techniques specific to the threat actors.

Spear Phishing -- Focus on Industrial Control Systems



6/7/12 Digital Bond, Inc. Mail - (no subject)

Gmail by Google

Dale Peterson <peterson@digitalbond.com>

(no subject)

1 message

Dale Peterson <dale.peterson111@yahoo.com> Thu, Jun 7, 2012 at 7:48 AM
Reply-To: Dale Peterson <dale.peterson111@yahoo.com>
To: "rvpasupuleti@yahoo.com" <rvpasupuleti@yahoo.com>

Dear All:
Field devices essential for the monitoring and control in DCS and SCADA systems are increasingly being deployed with Ethernet cards to connect these devices to local and wide area IP networks. Many of the Ethernet cards have their own CPU, memory, operating system and applications. Field device vendors are also providing the capability to upgrade or replace the firmware in these Ethernet cards. Unfortunately in most cases there is no effective security on the firmware upload to the field device Ethernet cards.
Details are available at: Leveraging_Ethernet_Card_Vulnerabilities_in_Field_Devices.pdf
Download it and have a look.
Regards,
Peterson

How do we respond?

SCOTT'S GREAT SNAKE.
IOWA
HAWK-EYE MARKSMEN
ILLINOIS
INDIANA
OHIO
NEW YORK
PENSYLVANIA
N. JERSEY
MD.
MISSOURI
KANZAS
INDIAN TERRITORY
ARKANSAS
KENTUCKY
ARMED NEUTRALITY
VIRGINIA
TENNESSEE
NORTH CAROLINA
GEORGIA
SOUTH CAROLINA
ALABAMA
MISSISSIPPI
TEXAS
LOUISIANA
FLORIDA
Division of Maps
NOV 30 1946
Library of Congress

How do we respond?

Layers of security that focus on:

- **People**
- **Technology**
- **Operations**

Critical Infrastructure and Emergency Preparedness

- In February, OCS, Taxation and Finance, OTDA, OCFS, and OFT participated in the DHS National Cyber Security Division’s national cyber exercise, Cyber Storm IV.
- Cyber Storm IV tested communications and incident response plans within New York in the event of a coordinated cyber attack against elements of the state government.
- The exercise featured an ongoing series of cyber events, some of which resulted in physical consequences.

Critical Infrastructure and Emergency Preparedness

- FEMA National Level Exercise (NLE) 2012 -- examined the Nation's ability to coordinate and implement prevention, preparedness, response, and recovery plans and capabilities pertaining to a significant cyber event or a series of related cyber events.

- NLE 2012 encompassed four exercises over a three month period (March – June).

- OCS, in conjunction with OEM and OCT, participated in NLE 2012 to test plans and capabilities pertaining to a cyber event with physical consequences.

Critical Infrastructure and Emergency Preparedness

- **OCS supports OCT in the preparation of the statutorily required reviews of critical infrastructure, including this year's review of energy generating and transmission facilities.**

- **OCS is conducting a survey of State agencies to identify industrial control systems maintained by those agencies.**

QUESTIONS?

Thank you!

Karen Sorady
Assistant Deputy Director for Cyber Programs
Office of Cyber Security

NYS Division of Homeland Security
and Emergency Services (DHSES)

Contact: 518-242-5200
E-mail: ksorady@dhses.ny.gov