NationalCouncil of ISACs

Information Sharing

Denise Anderson

Executive Director

National Health Information Sharing & Analysis Center (NH-ISAC)

Chair, National Council of ISACs

Agenda

- What is an ISAC?
- Overview of NCI
- Information Sharing - What and How
- Threats Seen
- Case Studies

National Council of ISACs

What is an ISAC?

Why ISACs?

Why ISACs?

❖ Trusted entities established by CI/KR owners and operators.

❖ Comprehensive sector analysis aggregation / anonymization

❖ Reach-within their sectors, with other sectors, and with government to share critical information.

❖ All-hazards approach

❖ Threat level determination for sector

❖Operational-timely accurate actionable

ISACs

- Aviation ISAC
- Communications ISAC
- Defense Industrial Base ISAC
- Downstream Natural Gas ISAC
- Electricity ISAC
- Emergency Management & Response ISAC
- Financial Services ISAC
- Information Technology ISAC
- Maritime ISAC
- Multi-State ISAC
- National Health ISAC

ISACs

Real Estate ISAC Information Sharing and Analysis Center

ONG-ISAC

- Oil and Natural Gas ISAC (ONG)
- Over the Road & Motor Coach ISAC
- Public Transit ISAC
- Real Estate ISAC
- Research and Education ISAC
- Retail ISAC
- Supply Chain ISAC
- Surface Transportation ISAC
- Water ISAC

SC ISAC

REN-ISAC

R-CISC RETAIL CYBER INTELLIGENCE SHARING CENTER

WaterISAC

APTA

ST-ISAC

Other Operational Entities and Upcoming ISACs

- **Automotive**
- Chemical
- Food & Ag
- Nuclear
- Critical Manufacturing

National Council of ISACs

What is the National Council of ISACs?

National Council of ISACs

- Began meeting in 2003 to address common concerns and cross-sector interdependencies

- Volunteer group of ISACs who meet monthly to develop trusted working relationships among sectors on issues of common interest and work on initiatives of value to CI/KR

NCI Structure

- National Council of ISACs: four designated operational representatives from each ISAC sit on the Council.
- ISAC Plus: all other entities/representatives such as operations centers who participate in information sharing
- Leadership:

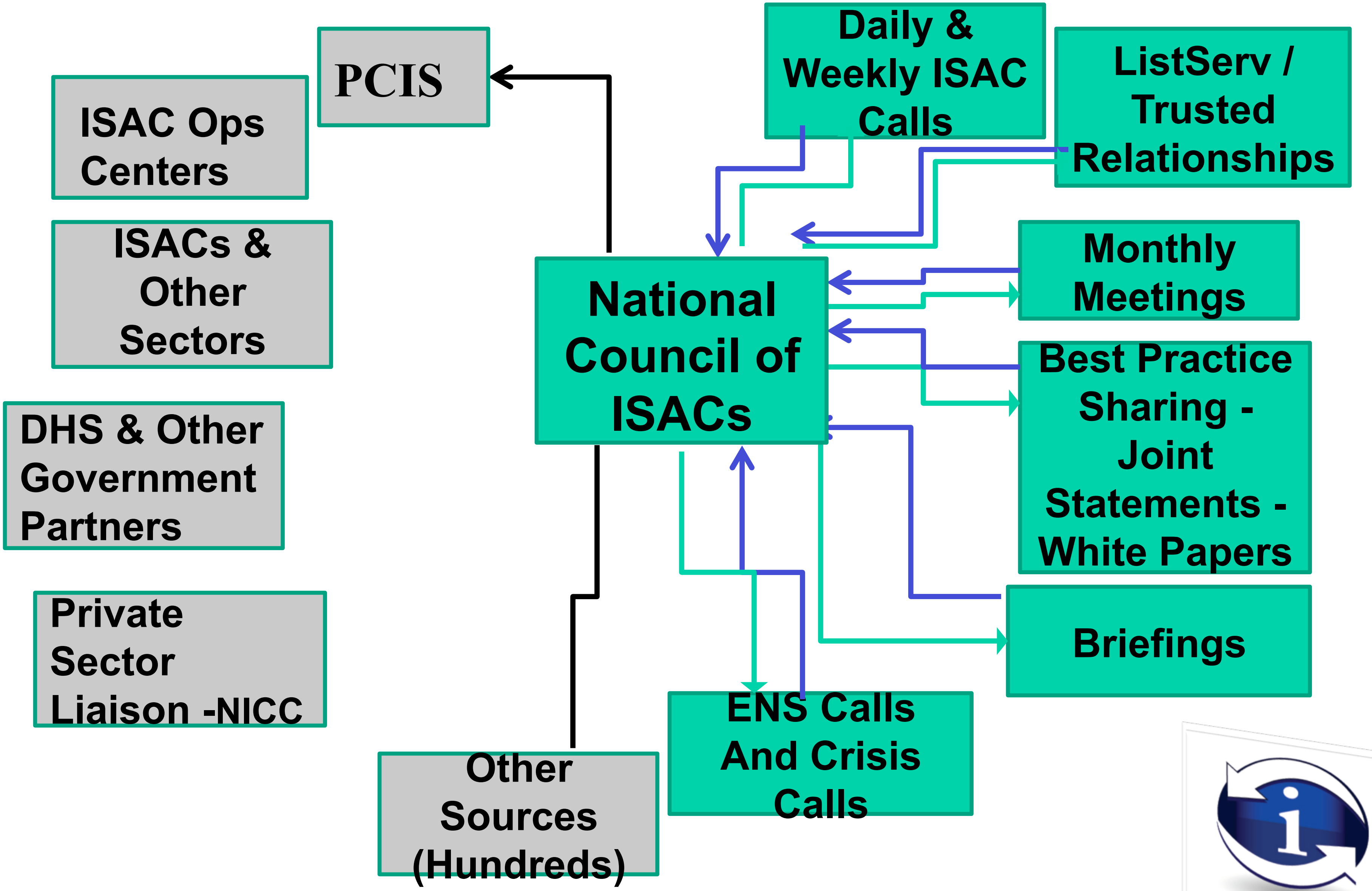
Chair: Denise Anderson-FS-ISAC

Vice-Chair: Scott Algeier-IT-ISAC

Secretary: Josh Poster-ST-ISAC

Information Sources

Communications



PCIS

ISAC Ops Centers

ISACs & Other Sectors

DHS & Other Government Partners

Private Sector Liaison -NICC

Other Sources (Hundreds)

National Council of ISACs

Daily & Weekly ISAC Calls

ListServ / Trusted Relationships

Monthly Meetings

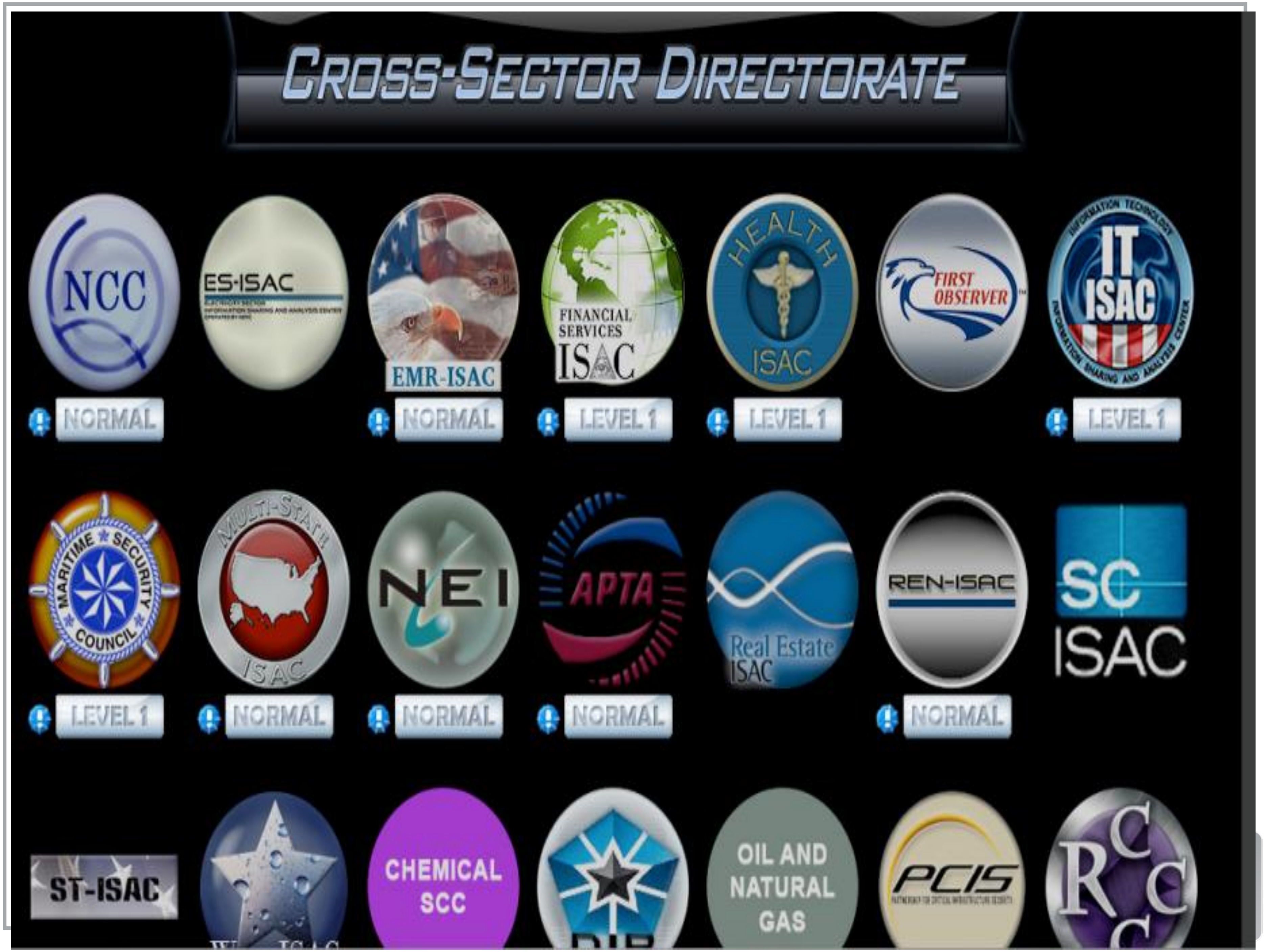
Best Practice Sharing - Joint Statements - White Papers

Briefings

ENS Calls And Crisis Calls

Examples of Activities

- Increase involvement of sectors without ISACs
- Daily, Weekly, Monthly and Crisis calls
- **Cross Sector Information Sharing Portal**
- **Private Sector Liaison with the NICC**
- Drills/Exercises Such as NLEs, Cyber Storm
  - OCF
- Implement Real-Time sector Threat Level Reporting
  - Directorate


CROSS-SECTOR DIRECTORATE
NCC
NORMAL
ES-ISAC
ELECTRICITY SECTOR INFORMATION SHARING AND ANALYSIS CENTER OPERATED BY NERC
EMR-ISAC
NORMAL
FINANCIAL SERVICES ISAC
LEVEL 1
HEALTH ISAC
LEVEL 1
FIRST OBSERVER
INFORMATION TECHNOLOGY IT ISAC INFORMATION SHARING AND ANALYSIS CENTER
LEVEL 1
MARITIME SECURITY COUNCIL
LEVEL 1
MULTI-STATE ISAC
NORMAL
NEI
NORMAL
APTA
NORMAL
Real Estate ISAC
REN-ISAC
NORMAL
SC ISAC
ST-ISAC
CHEMICAL SCC
OIL AND NATURAL GAS
PCIS
PARTNERSHIP FOR CRITICAL INFRASTRUCTURE SECURITY
RCCC

Points of Engagement

- National Infrastructure Coordinating Center (NICC)
- National Cybersecurity and Communications Integration Center (NCCIC)
  - DHS-led Unified Operations Watch & Warning Center
  - Operates 24 hours/day, 7 days/week, 365 days a year
- Unified Command Group-composed of private and public sector representatives
  - Meet monthly and during an incident as needed
  - Advise Assistant Secretary of CS&C on cybersecurity matters, provide subject matter expertise and response as necessary during an incident that requires national coordination

National Council of ISACs

www.nationalcouncilofisacs.org

nationalcouncilofisacs@natlisacs.org

NationalCouncil of ISACs

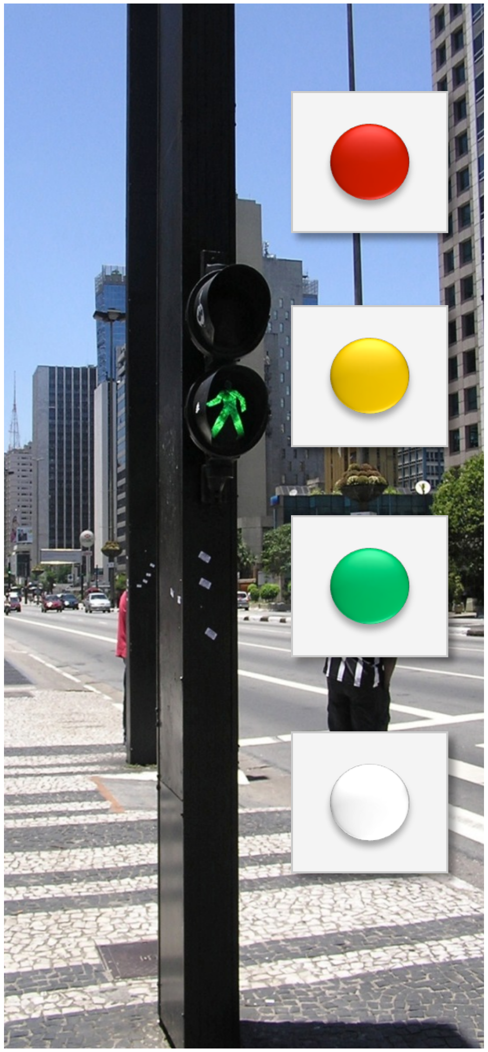
Information Sharing

Valu
e

Trust

Structur
e

Information Sharing: Traffic Light Protocol



- Restricted to a defined group (e.g., only those present in a meeting.) Information labeled RED should not be shared with anyone outside of the group

- This information may be shared with FS-ISAC members.

- Information may be shared with FS-ISAC members and partners (e.g., vendors, MSSPs, customers). Information in this category is not to be shared in public forums

- This information may be shared freely and is subject to standard copyright rules

NationalCounciloFISACs

Types of Information Shared

Cyber Threats, Vulnerabilities, Incidents

- ✓ Malicious Sites
- ✓ Threat Actors, Objectives
- ✓ Threat Indicators
- ✓ TTPs, Observables
- ✓ Courses of Action
- ✓ Exploit Targets
- ✓ Denial of Service Attacks
- ✓ Malicious Emails: Phishing/ Spearphishing
- ✓ Software Vulnerabilities
- ✓ Malicious Software
- ✓ Analysis and risk mitigation
- ✓ Incident response

NationalCouncil of ISACs

Primary Ways Information Is Shared

✓Portal/Alerts

✓Listservers

✓Automation

Sample of Sharing Thread

Received close to 500 so far and still coming in, 90 made it through to employees before being blocked by perimeter as spam

Subject:
Important message from BANK
Sender:
youraccount@BANK.message.com
URL: hxxp://www2.webmasterradio.fm/FanPagePro/css/Logon.html

0 hits last 7 days

We've had about 50 hits; so far all are discarded

BANK: Submitted a takedown request for the phishing site

TLP AMBER
PROPRIETARY INFORMATION

Sample of ISAC Sharing

Indicators of Compromise

IP Address, Subject Line, MD5, TTP, Malware

Ask a question

Anyone else seeing?...

What do you do in this situation?....

How do you handle?…………

Share a Best Practice

Here’s how we……

Share a Mitigation Strategy

Here’s a script you can use……

We did this……

A Common Language

STIX™

- **Structured Threat Information Expression is a common language a way for all to speak the same**

Trusted Automated eXchange of Indicator Information (TAXII)

- **The goal of TAXII is to facilitate the exchange of structured cyber threat information**
  - Designed to support existing sharing paradigms in a more automated manner
- **TAXII is a set of specifications defining the network-level activity of the exchange**
  - Defines services and messages to exchange data
  - Does NOT dictate *HOW* data is handled in the back-end, *WHAT* data is shared or *WHO* it is shared with
  - TAXII is NOT a sharing program
- **TAXII is a protocol over which STIX can be transported**

What is Cyber Threat Intelligence?
8 Constructs of STIX

Atomic

Observable

What threat activity are we seeing?

Tactical

Indicator

What threats should I look for on my networks and systems and why?

Operational

Incident

Where has this threat been seen?

Course of Action

What can I do about it?

ExploitTarget

What weaknesses does it exploit?

Strategic

ThreatActor

Who is responsible for this threat?

Campaign

Why do they do this?

TTP

What do they do?

National Council of ISACs

Threats Seen

Cyber Threat Environment

- **Actors:**
  - Nation States
  - Terrorists
  - Criminals
  - Insiders
  - Activists/Hacktivists
  - Media
  - Vendors

National Council of ISACs

Seen Last Week…..

Nuclear Exploit Kit

Open VAS Scanning

Dridex

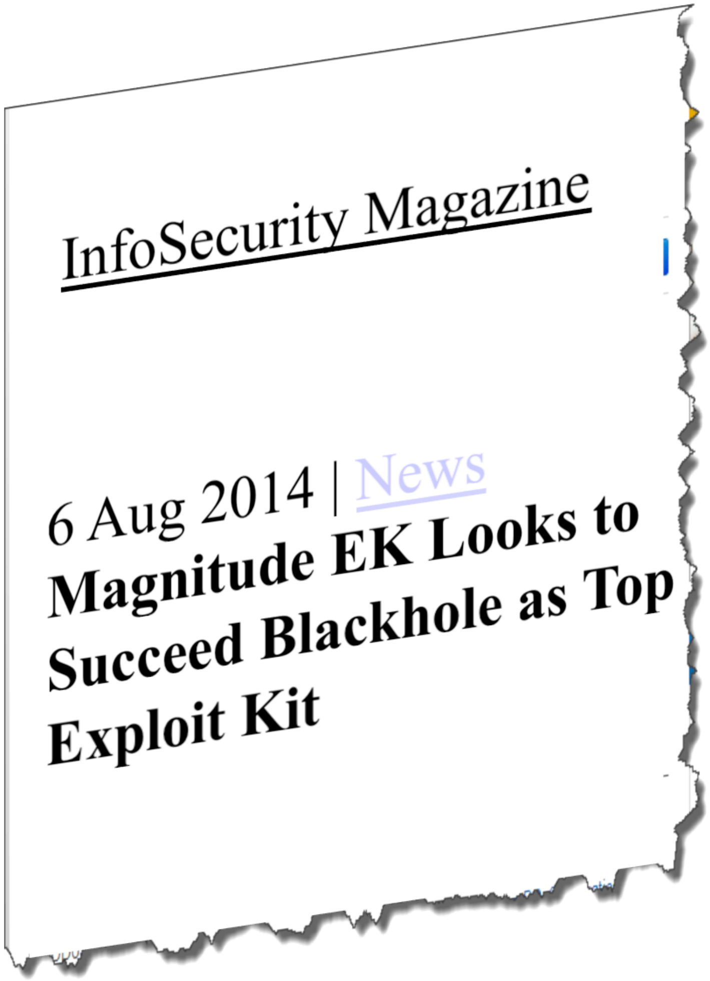
PlugX

Upatre/Dyre

Angler/Neutrino

DDoS

Malware-Exploit Kits



InfoSecurity Magazine

6 Aug 2014 | News

Magnitude EK Looks to Succeed Blackhole as Top Exploit Kit

Top Exploit Kits Seen

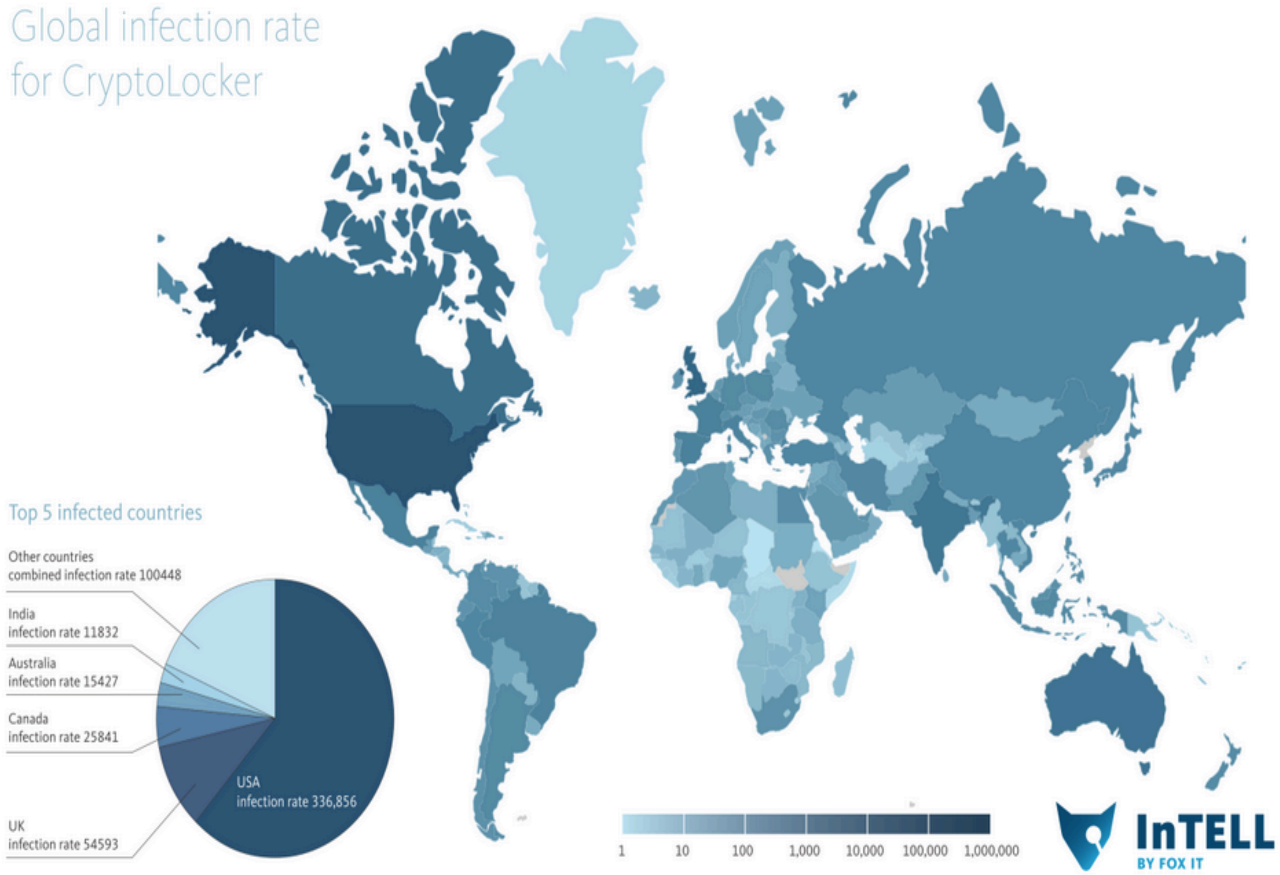
Blackhole EK *– Paunch 10/13*
Infinity EK*: Flash player exploit*
Neutrino EK*: Mixes legitimate non-legitimate requests to obsfuscate the code.*
Magnitude EK*: - Ransomware*
Sweet Orange EK*: - Website*
Fiesta EK*: - Silverlight*
Angler EK*: hides behind legitimate web code*
Crimeboss EK*: Java exploits*

NationalCouncil of ISACs

Ransomware

-Crytolocker
-CryptoWall
-CryptoDefense
-Torrent Locker
-Darkleach

Top infections:
US
AU
Canada
UK
India
Also saw Singapore trend


Global infection rate for CryptoLocker
Top 5 infected countries
Other countries combined infection rate 100448
India infection rate 11832
Australia infection rate 15427
Canada infection rate 25841
UK infection rate 54593
USA infection rate 336,856
1
10
100
1,000
10,000
100,000
1,000,000
InTELL
BY FOX IT

NationalCouncil of ISACs

Delivery Mechanisms:
Phishing/Spearphishing

Court Notice

Invoice/Statament

Shipping Themes: DHL, Fedex, UPS

EZ Pass

Bank Phish – Swift Transfer

Dhgate invoice

eFax

Salesforce

Reward themes

Airline – Delta

WhatsApp – You’ve got a voicemail

Malware: Banking Trojans

Top Trojans Seen

Citadel

Kronos

Kulouz – Asprox

Carperb

Zeus

Zberp - hybrid

Game-over Zeus (GOZ) - P2P (.arj) 9/14

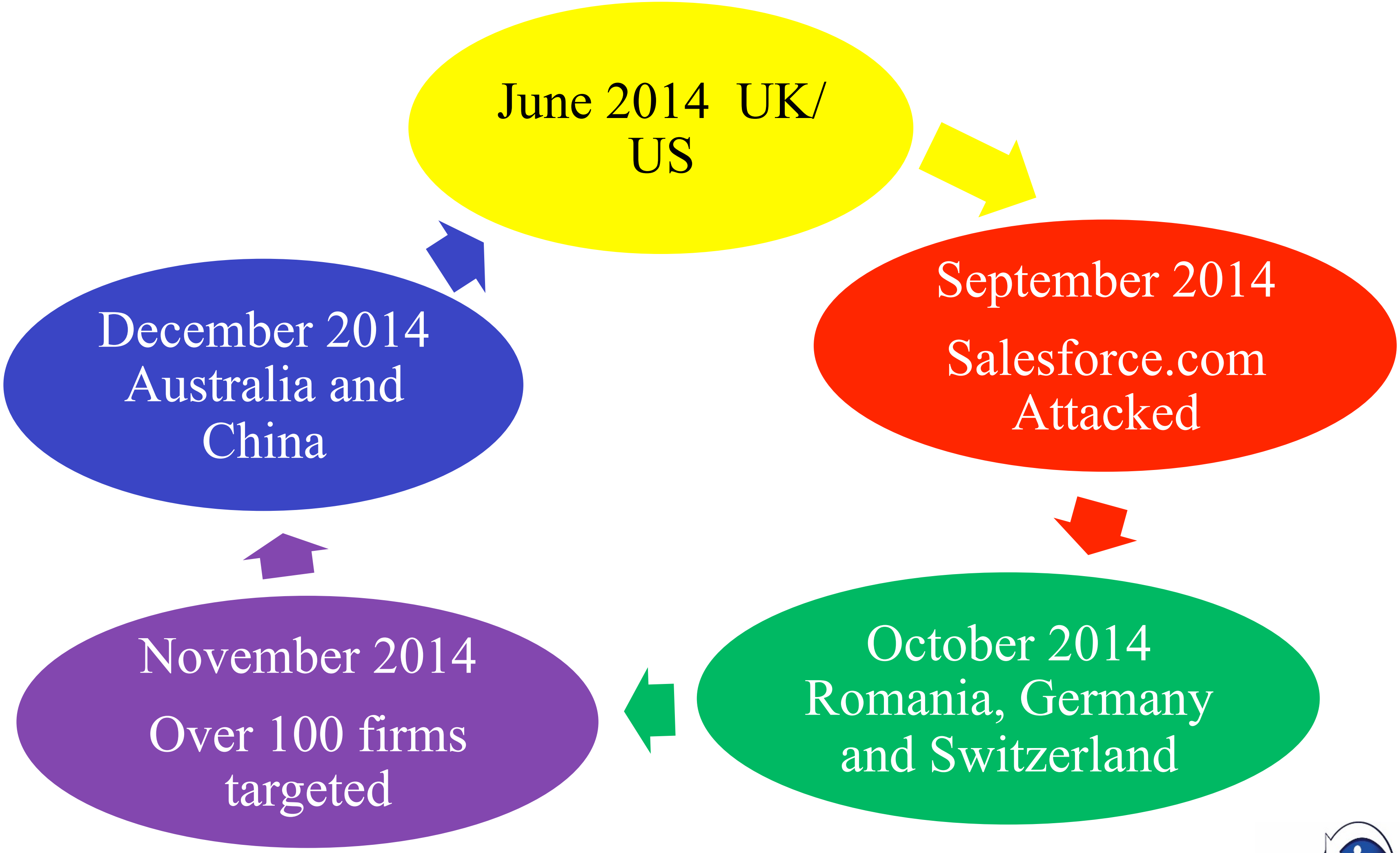
Cridex – Bugat, Feodo

Dridex

Dyre

Shylock – July 2014 Takedown

Dyre Spreads Like A Global Virus…



June 2014 UK/ US

September 2014

Salesforce.com Attacked

October 2014 Romania, Germany and Switzerland

November 2014

Over 100 firms targeted

December 2014 Australia and China

NationalCouncilofISACs

Delivery Mechanisms:
Drive-by Downloads and Watering Holes

Forbes.com
Energystar.com
AusPost-tracking.com
VA.gov
NBC.com – Citadel 2013

Vulnerability Scanning

- *Port Scans – Open ports*
- *Vulnerability Scans   - Wordpress, Joomla, Java, Flash, Open SSL*
- *Infrastructure*

Vulnerabilities

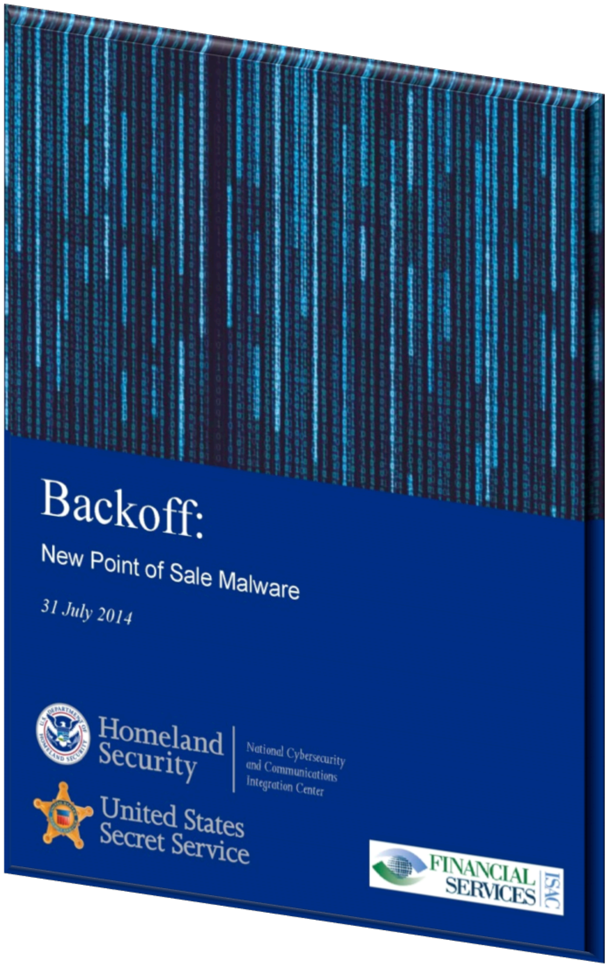
- *OpenSSL/Heartbleed*
  - *Old vulnerability*
  - *Allows more data than allowed to be read*
  - *Website vulnerability*
  - *Banks took rap unfairly*

- *GNU Bash/Shellshock*
  - *Old vulnerability 1994*
  - *Unix based: Linux, Apple Mac OX*
  - *Went public Wednesday 9/24*
  - *Exploits and scanning seen almost immediately*

Breaches

Malware: ChewBacca, Dexter, Black POS, Backoff

- ➢ *Target: 70 million - 2013*
- ➢ *OPM: 21.5 million*
- ➢ *Primera BC/BS: 11.2 million*
- ➢ *Community Health Systems: 4.5 million*
- ➢ *Anthem BC/BS: 80 million*
- ➢ *Sony/Hacking Team*



Backoff:

New Point of Sale Malware

31 July 2014

Homeland Security | National Cybersecurity and Communications Integration Center

United States Secret Service

FINANCIAL SERVICES ISAC

2015 Breaches Identified by the ITRC as of: 8/11/2015

•Total Breaches: 5,500 approx

•Total Records Exposed: 818,004,561

•Identity Theft Resource Center

NationalCouncil of ISACs

DDoS

- *Sony PlayStation – Lizard Squad*
- *Operation Ababil*
- *Las Vegas – Gaming Industry*
- *Israel*
- *DD4BC*
- *World Cup*

<u>Q1 2015 Compared to Q4 2014</u>

15 % decrease in avg. attack time

35 % increase in total DDoS attacks

42 % increase in SSDP DDoS attacks (routers)

22 % increase in aplication layer DDoS attacks

7 % decrease in average attack bandwidth (170 Gbps)

37 % increase in infrastructure layer DDoS attacks

Akamai

NationalCouncil of ISACs

Wiper Malware

- *Shamoon – 2012*
  - *Attack on 30,000 Saudi Aramco Workstations*
  - *Corrupts files and wipes devices*
- *South Korean Attacks– 2013*
  - *2 banks, media company and insurance company*
  - *Patch systems targeted and used to infect*
  - *Wiped windows, Linux and UNIX OS*
- *Las Vegas Casino– 2014*
  - *Wiped and destroyed files with VB bomb*
- *Sony – 2014*
  - *SMB Worm Tool, listening implant, backdoor, proxy tool, destructive hard drive tool, destructive targeted cleaning tool, network propogation wiper*
  - *Financial data destroyed, financial system still inoperable – asks for delay in filing*

The Media and Vendors

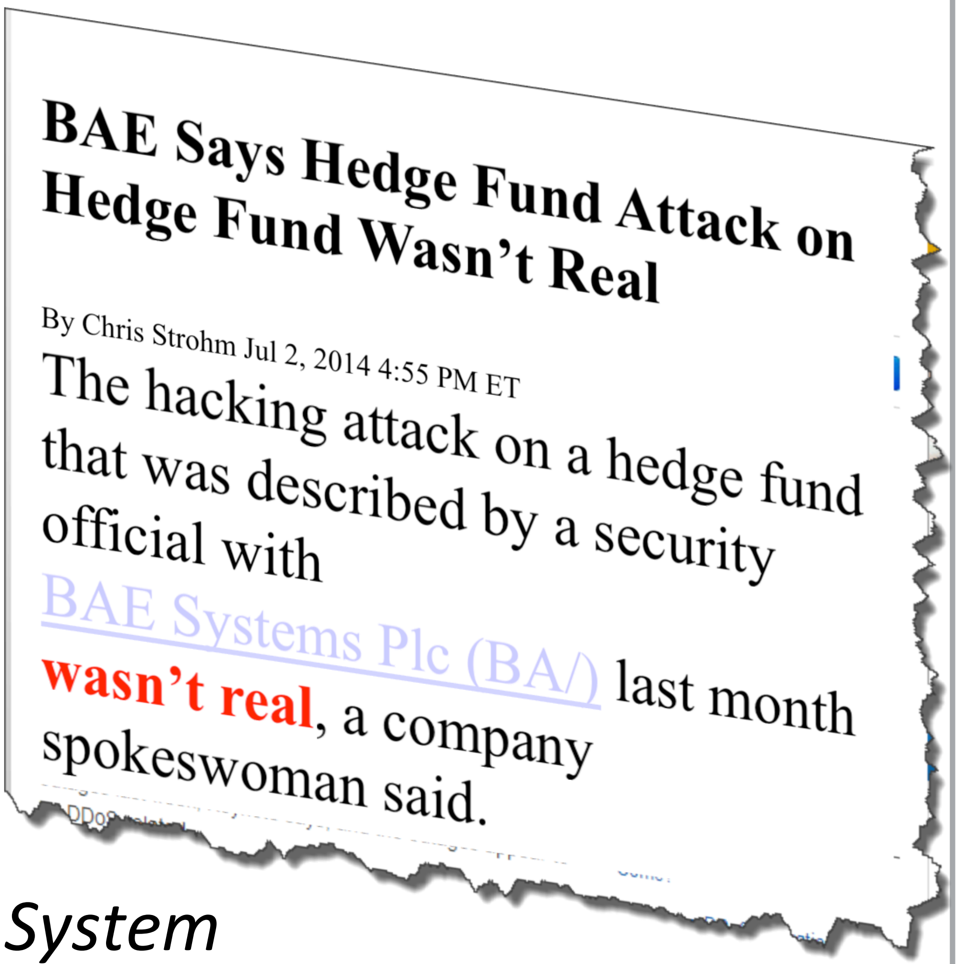
Malvertising

Watering Holes

Syrian Electronic Army

Media/
Vendor Spin Incidents:

- *HeartBleed, Open SSL*
- *Hedge Fund Attack - BAE*
- *Russians Attack Financial System*
- *Russians Hack 1.4 Billion Passwords - Hold Security*



BAE Says Hedge Fund Attack on Hedge Fund Wasn't Real

By Chris Strohm Jul 2, 2014 4:55 PM ET

The hacking attack on a hedge fund that was described by a security official with BAE Systems Plc (BA/) last month **wasn't real**, a company spokeswoman said.

NationalCouncil of ISACs

Other Threats

- *Call Center – Phishing*
- *Mobile*
- *Social Media – Sony Executive on American Airlines*
- *Industrial Control Systems - Havex*
- *Espionage – VirusTotal testing for malware*

NationalCouncil of ISACs

NationalCouncil of ISACs

Case Studies

DDoS – DD4BC

Since: April 2015
•*Subject Line:*

•From: From: DD4BC Team <d4bct[AT]gmail[.]com>

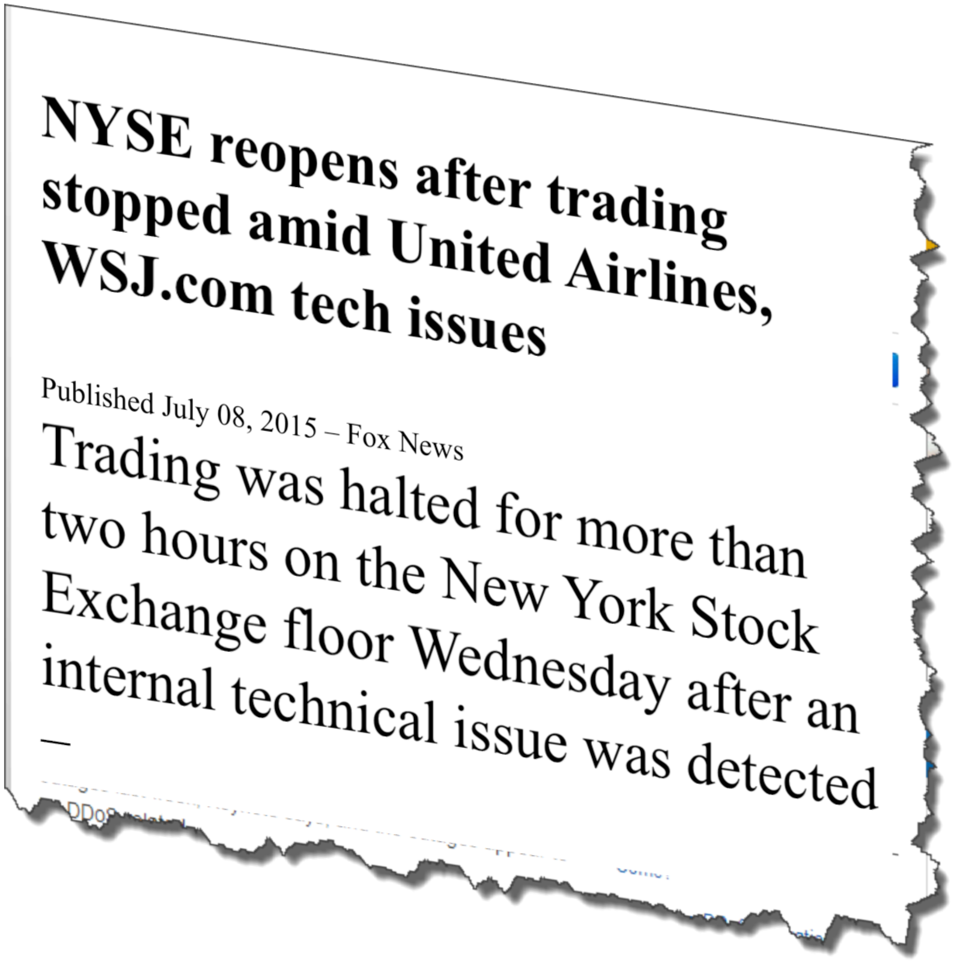
•Subject: DDOS ATTACK!

Size: 500 Mbps to 50 Gbps
Duration: Up to 1 hour
Ransom Demand: 25-40 BTC

United/NYSE

NYSE: July 8, 2015 11:32am
11:45am chatter
Noon definitive word

UNITED: 8:26 am
Reservation System



NYSE reopens after trading stopped amid United Airlines, WSJ.com tech issues

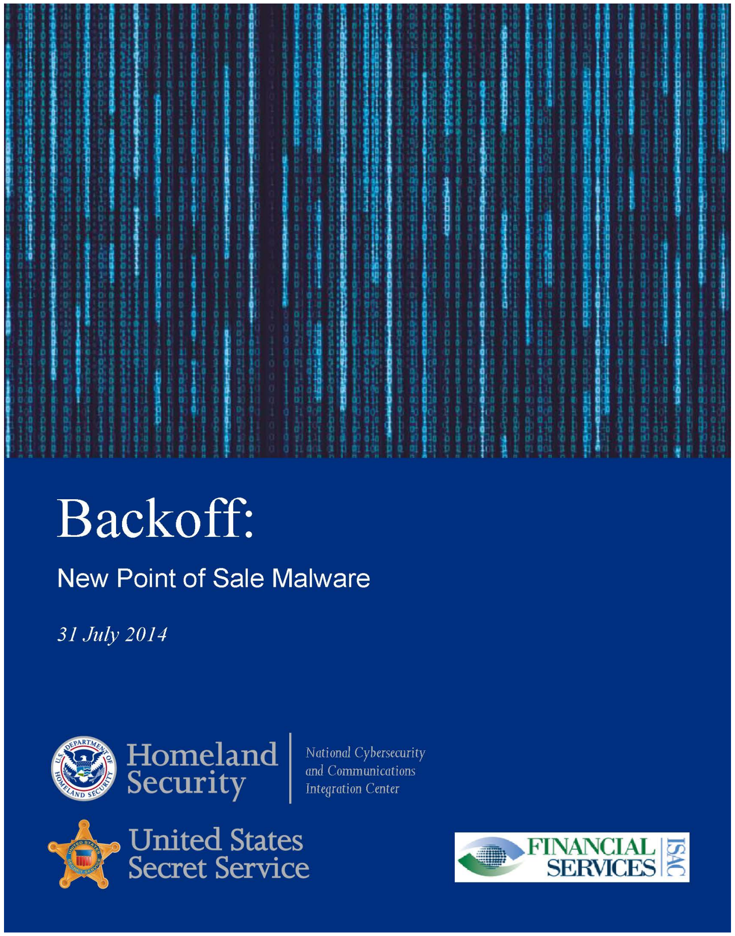
Published July 08, 2015 – Fox News

Trading was halted for more than two hours on the New York Stock Exchange floor Wednesday after an internal technical issue was detected

—

United Parcel Service

- **USSS, NCCIC, FS-ISAC –** Collaborate to release malware analysis and risk mitigation recommendations
- **Shared with Retailers Association**
- **UPS Detected and used to mitigate Malware**



Backoff:

New Point of Sale Malware

31 July 2014

Homeland Security | National Cybersecurity and Communications Integration Center

United States Secret Service

FINANCIAL SERVICES ISAC

Questions?