Collaborative Information Sharing, Current and Future Threats

- Charles Bretz
- 1-205-790-0248
- cbretz@fsisac.us

FS-ISAC Overview

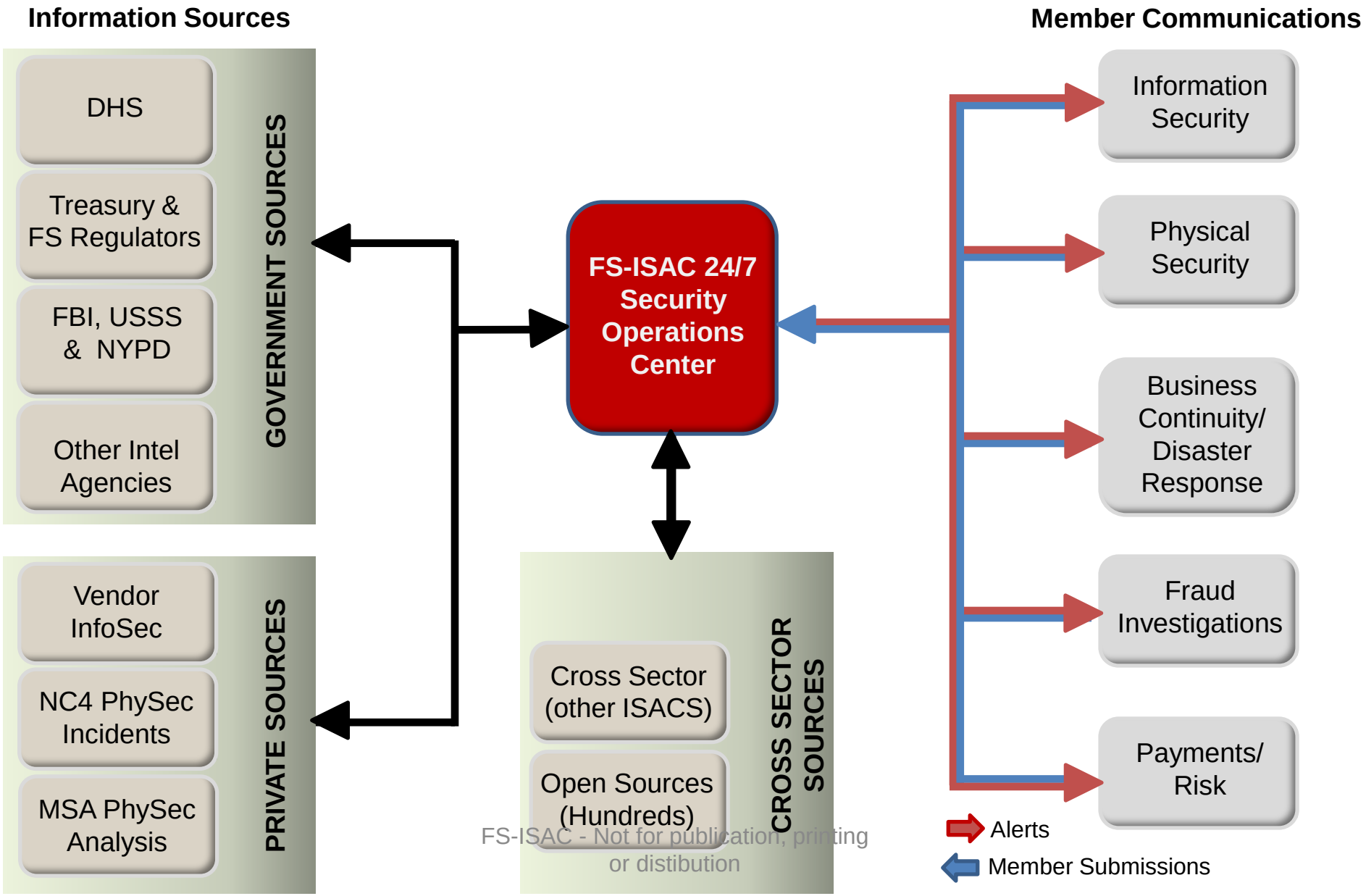
Financial Services Information Sharing & Analysis Center

FS-ISAC Background and Goal

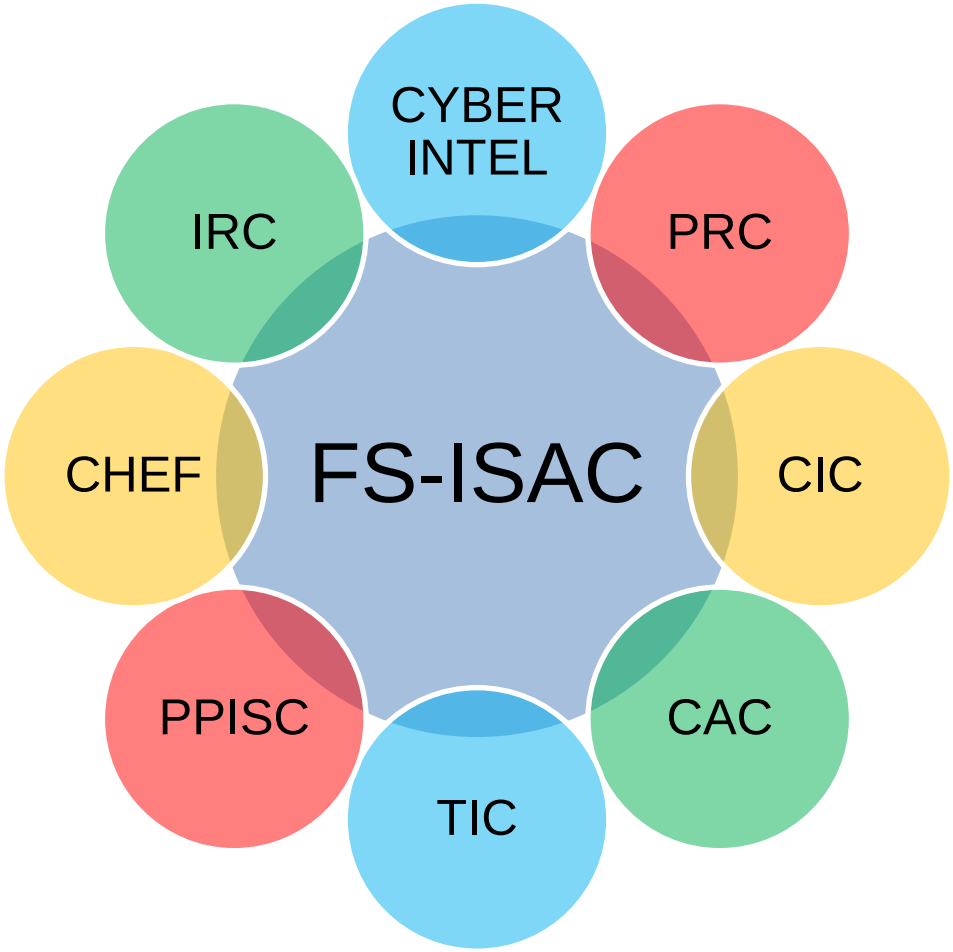
The Financial Services Information Sharing and Analysis Center is:

- A nonprofit private sector initiative
- Designed/developed/owned by financial services industry
- Lead agency: U.S. Treasury
- Goal:
  - Provide a single source for sharing physical and cyber security information…
  - to protect the critical US Financial System…
  - including critical payment systems.

FS-ISAC 24/7 Security Operations Center



FS-ISAC Circles of Trust

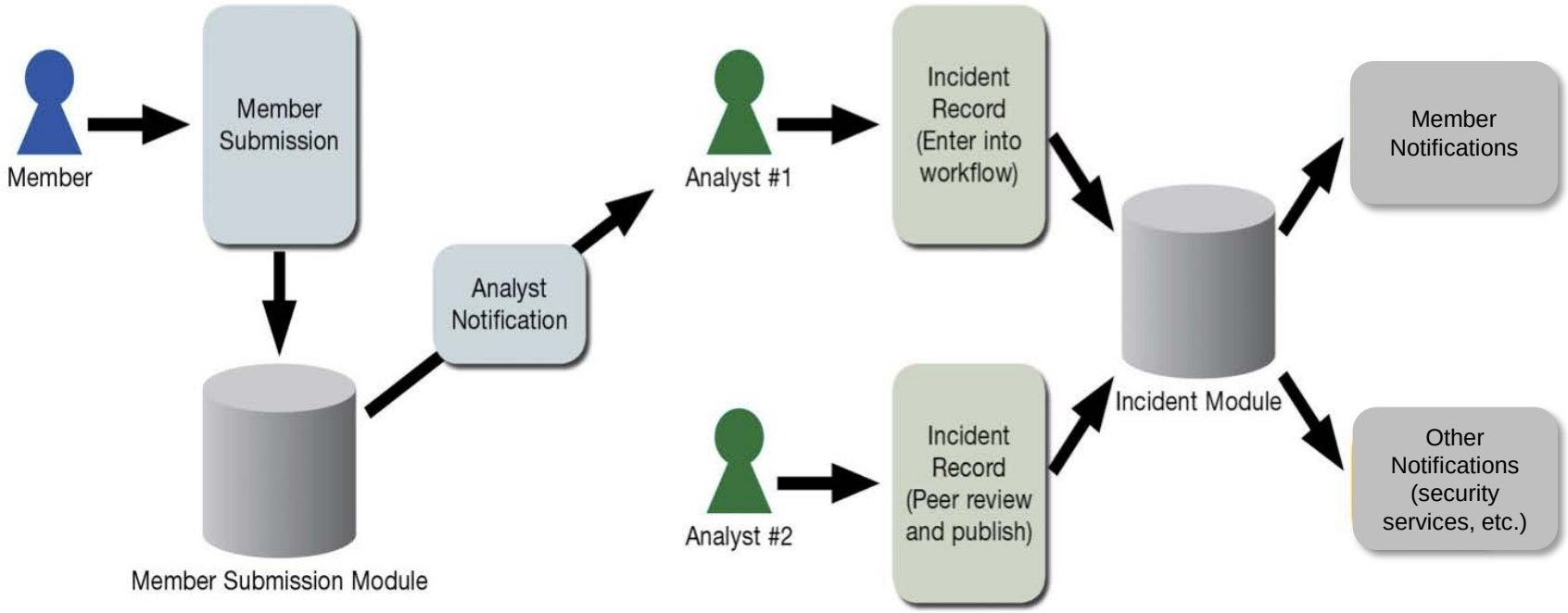


FS-ISAC Traffic Light Protocol (TLP)

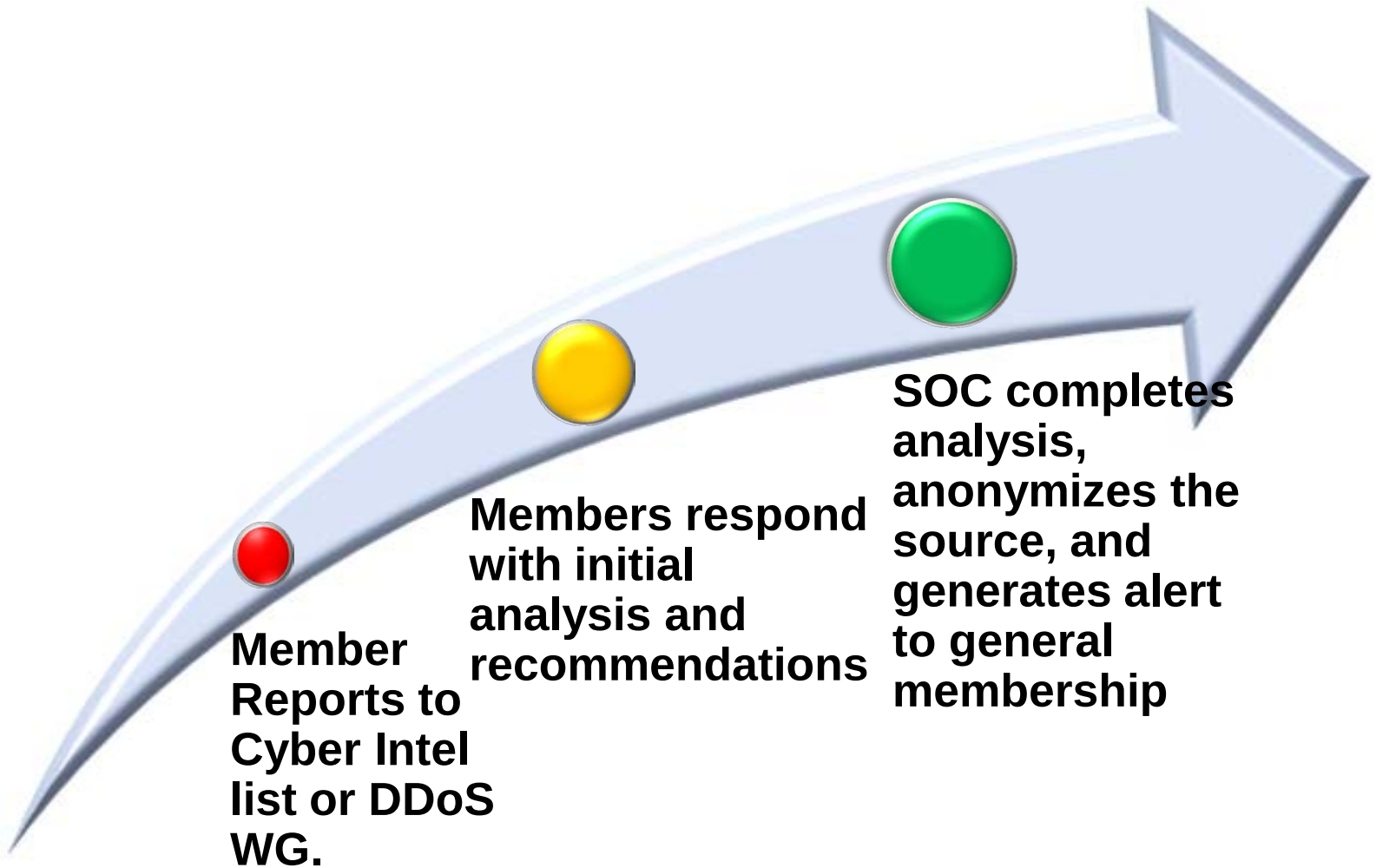
Classification	Target Audience
+ **FS-ISAC Red**	+ **Restricted to a defined group (e.g., only those present in a meeting.) Information labeled RED should not be shared with anyone outside of the group**
+ **FS-ISAC Amber**	+ **This information may be shared with FS-ISAC members.**
+ **FS-ISAC Green**	+ **Information within this category may be shared with FS-ISAC members and partners (e.g., Government Agencies and ISACs). Information in this category is not to be shared in public forums**
+ **FS-ISAC White**	+ **This information may be shared freely and is subject to standard copyright rules**

Member Submissions via Portal

Anonymous or Attributed
Submission Types: Cyber Incident, Physical Incident or Document Upload



Typical Process Utilizing Circles of Trust



Current Threats

Transnational Organized Crime and Attributed Nation State Attacks

Financial Services Information Sharing & Analysis Center

Worldwide Threat Assessment of the
US Intelligence Community Senate Select Committee on Intellige
James R. Clapper Director of National Intelligence
March 12, 2013

Cybercriminals also threaten US economic interests. They are selling tools, via a growing black market, that might enable access to critical infrastructure systems or get into the hands of state and non-state actors.

In addition, a handful of commercial companies sell computer intrusion kits on the open market. These hardware and software packages can give governments and cybercriminals the capability to steal, manipulate, or delete information on targeted systems.

Worldwide Threat Assessment
of the
US Intelligence Community
Senate Select Committee on Intelligence

Transnational Organized Crime Transnational (TOC) networks erode good governance, cripple the rule of law through corruption, hinder economic competitiveness, steal vast amounts of money, and traffic millions of people around the globe. (Cybercrime, an expanding for-profit TOC enterprise, is addressed in the Cyber section.) TOC threatens US national interests in a number of ways:

Corruption. Corruption exists at some level in all countries; however, the interaction between government officials and TOC networks is particularly pernicious in some countries. Among numerous examples, … in Russia, the nexus among organized crime, some state officials, the intelligence services, and business blurs the distinction between state policy and private gain.

Examples of Transnational Criminal Activity

Bank Muscat hit by $39m pre-paid card fraud

27 February 2013 | 3815 views | 1

Oman's Bank Muscat says crooks have managed to compromise a dozen pre-paid travel cards, racking up RO15 million (US$39 million) in fraudulent transactions.

No customers have suffered any financial loss and no other credit or debit cards issued by the bank have been affected, says a statement published on the Muscat Securities Market site.

Domino's guy a key player in bank-fraud scheme: feds

By MITCHEL MADDUX
Last Updated: 2:40 PM, March 30, 2013
Posted: 1:03 AM, March 30, 2013

This pizza guy really knew how to make some dough.

A Domino's Pizza employee was a key player in a bank-fraud scheme that netted a New York crime ring millions of dollars, the feds said yesterday.

Elvis Rodriguez, 24, of Yonkers, was slapped with federal bank-fraud charges after he and his accomplices allegedly used phony debit cards to withdraw millions in cash from ATMs in Manhattan and Brooklyn.

Secret Service agents say the New York ring paid Russian and Romanian mobsters for confidential financial information that had been hacked from the computers of banks in the United Arab Emirates and Oman.

Rodriguez and his pals then used the stolen data to make the counterfeit cards.

The feds say they have bank surveillance photos of Rodriguez wearing a black Domino's Pizza cap withdrawing cash with the stolen cards. He also listed the restaurant as his employer on a passport application.

The suspect and two cohorts flew from JFK to Romania in January to deliver $300,000 to the gang that provided the hacked bank data, prosecutors said at his Brooklyn federal court Thursday appearance.

INVESTMENT BANKING | LEGAL/REGULATORY | JULY 25, 2013, 10:19 AM | 112 Comments

U.S. Says Ring Stole 160 Million Credit Card Numbers

BY NATHANIEL POPPER AND SOMINI SENGUPTA

United States District Court
District of New Jersey

UNITED STATES OF AMERICA
v.

VLADIMIR DRINKMAN, [redacted]

ALEKSANDR KALININ, [redacted]

ROMAN KOTOV, [redacted]

MIKHAIL RYTIKOV, [redacted]

and DMITRIY SMILIANETS, [redacted]

INDICTMENT FOR
18 U.S.C. §§ 371, 1030, 1343, 1349, and 2

A True Bill,

DVKRK Indictments
Companies Alleged to be Attacked

- NADDAQ
- Jet Blue
- Carrefour
- Heartland
- WetSeal.com
- Commidea
- Hannaford
- Dexia
- Dow Jones
- Euronet
- Global Payments
- Bank A
- Visa – Jordon
- Dinners Singapore
- Ingenicard (Cash out)
- 7-Eleven

Attributed Nation State DDoS Attacks

Financial Services Information Sharing & Analysis Center

THE WALL STREET JOURNAL.

U.S. EDITION ▾ Friday, October 12, 2012 As of 7:38 PM EDT

WORLD NEWS | Updated October 12, 2012, 7:38 p.m. ET

Iran Blamed for Cyberattacks

U.S. Officials Say Iranian Hackers Behind Electronic Assaults on U.S. Banks, Foreig Firms

Article | Stock Quotes | Comments (166)

By SIOBHAN GORMAN And JULIAN E. BARNES

A A

WASHINGTON—Iranian hackers with government ties have mounted cyberattacks against American targets in recent months, escalating a low-grade cyberwar, U.S. officials say.

The Iranian effort culminated in a series of recent attacks against U.S. banks as well as electronic assaults this year on energy companies in the Persian Gulf. The attacks bore "signatures" that allowed U.S. investigators to trace them to the Iranian government, the officials said.

A Litany of High-Tech Assaults

Incidents have escalated in recent months.

- January 2012: Potent but smaller-scale denial-of-service attacks against U.S. banks.
- July 2012: Cyberattack at Saudi Arabian Oil Co. unleashes a virus called 'Shamoon,' destroying data on 30,000 computers.
- August 2012: Cyberattack at Rasgas, a Qatari natural gas company, disabled websites and email system.
- September 2012: A group called "Qassam Cyber Fighters" announced plans for cyberattacks on U.S. banks. Powerful denial of service strikes hit Bank of America Corp, J.P. Morgan Chase & Co., U.S. Bancorp, PNC Financial Services Corp. and Wells Fargo & Co.
- October 2012: The Qassam Cyber Fighters issued announcements, followed by cyber strikes, involving other U.S. banks, slowing or interrupting consumer websites

- (U//FOUO) Since September 2012, US financial institutions have been under coordinated and timed DDoS attacks.
- To date, 46 U.S. financial institutions have been targeted with DDoS attacks, with various degrees of impact, in over 200 separate DDoS attacks.
- These attacks have utilized high bandwidth webservers with vulnerable content management systems.
- Typically a customer account is compromised and attack scripts are then uploaded to a hidden directory on the customer website.
- To date the botnets have been identified as “Brobot” and “Kamikaze/Toxin.”

Future Concerns

Financial Services Information Sharing & Analysis Center

The New York Times

Asia Pacific

Computer Networks in South Korea Are Paralyzed in Cyberattacks

NYT Reporting about Korean Attacks

"The attacks, which left many South Koreans unable to withdraw money from A.T.M.'s…"

"The malware is called "DarkSeoul"…It is intended … to render computers unusable."

"Two banks…, NongHyup and Jeju, reported that operations at some of their branches had been paralyzed after computers were infected with viruses and their files erased.."