SearchFinancialSecurity.com
INFORMATION SECURITY
FINANCIAL
INFORMATION SECURITY DECISIONS

Cybercrime and the Financial Sector: The Growing Link

Erez Liebermann
Seth Kosto
Assistant United States Attorneys
Computer Hacking and Intellectual Property Section
District of New Jersey

Laws and Penalties

- Computer Fraud and Abuse Act
- Identity Theft
- Access Device Fraud
- Wire Fraud

Cyber Crimes

- Hacking
- Data Breaches
- Phishing
- Malicious Attacks

The Most Sophisticated?

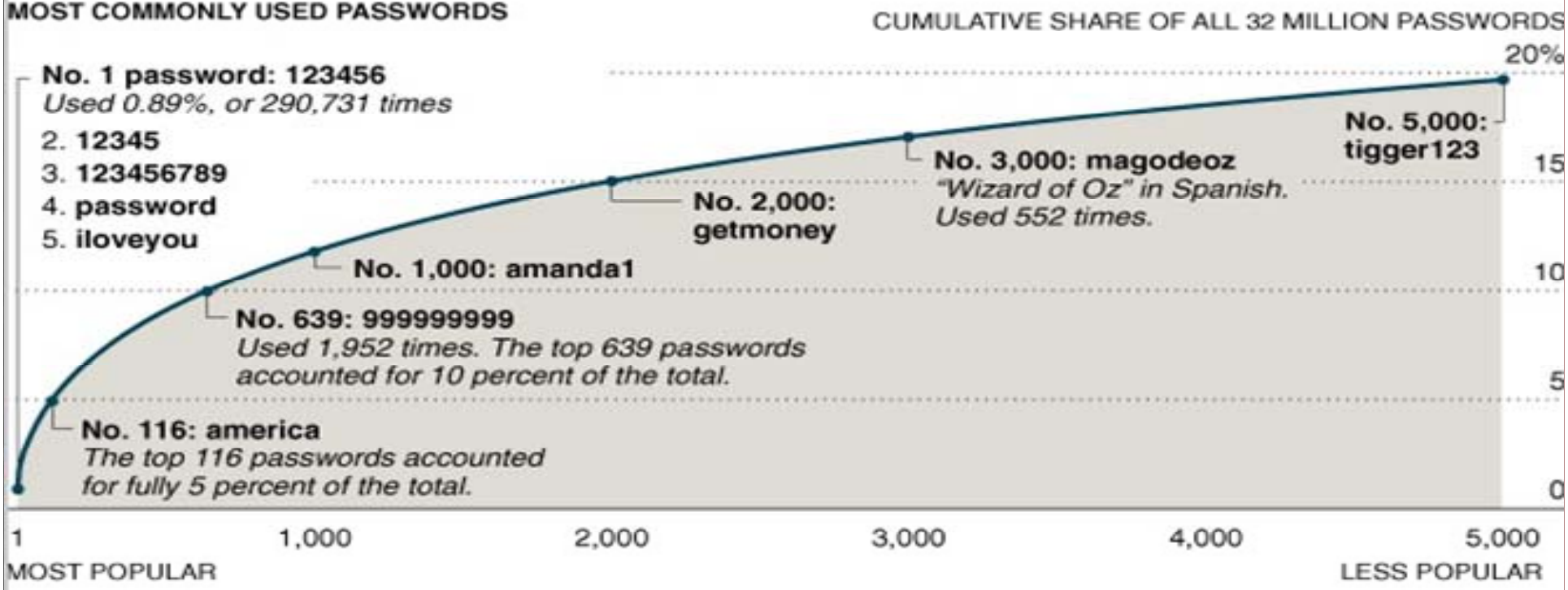
- SQL Injections?
- WiFi Breaches?
- Botnets?
- Trojans?

They Learned…

- The path of least resistance:
- Social Engineering

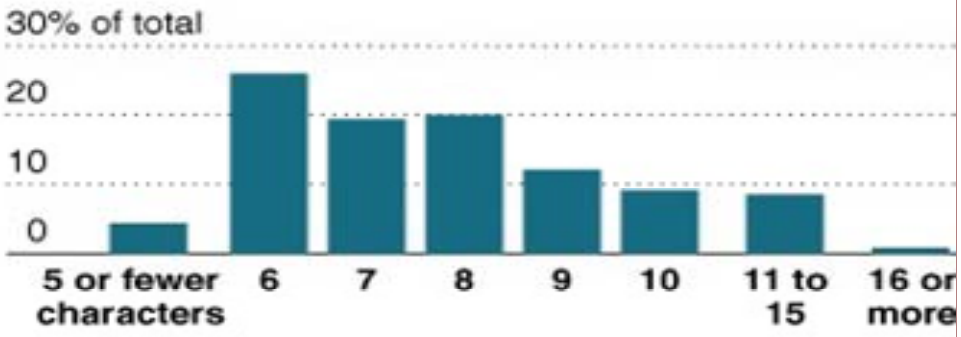
The Risks of Keeping It Simple

In December, security researchers discovered that a list of 32 million passwords and e-mail addresses were stolen from RockYou, a site that sells advertising and makes applications for social networking sites like Facebook and MySpace. An analysis found that nearly 20 percent of the accounts — some 6.4 million — used only 5,000 different passwords, most short and very simple.



PASSWORD LENGTH

Long passwords mixing letters, numbers and symbols are tough to crack. As the number of characters increases, the possible combinations rise exponentially, making it harder for a hacker to try all the possibilities. The best passwords are memorable but hard to type, like **()hmy1stuBBedmyt0e.**



Source: Imperva

Common Defense

- SODDI
- Some Other Dude Did It

Evidence Typically Recovered

- Internet Protocol Logs
- E-mail Searches
- Social Networking Sites / Forums (Facebooks/Myspace)
- Data analysis via pen registers
- Wire Intercepts

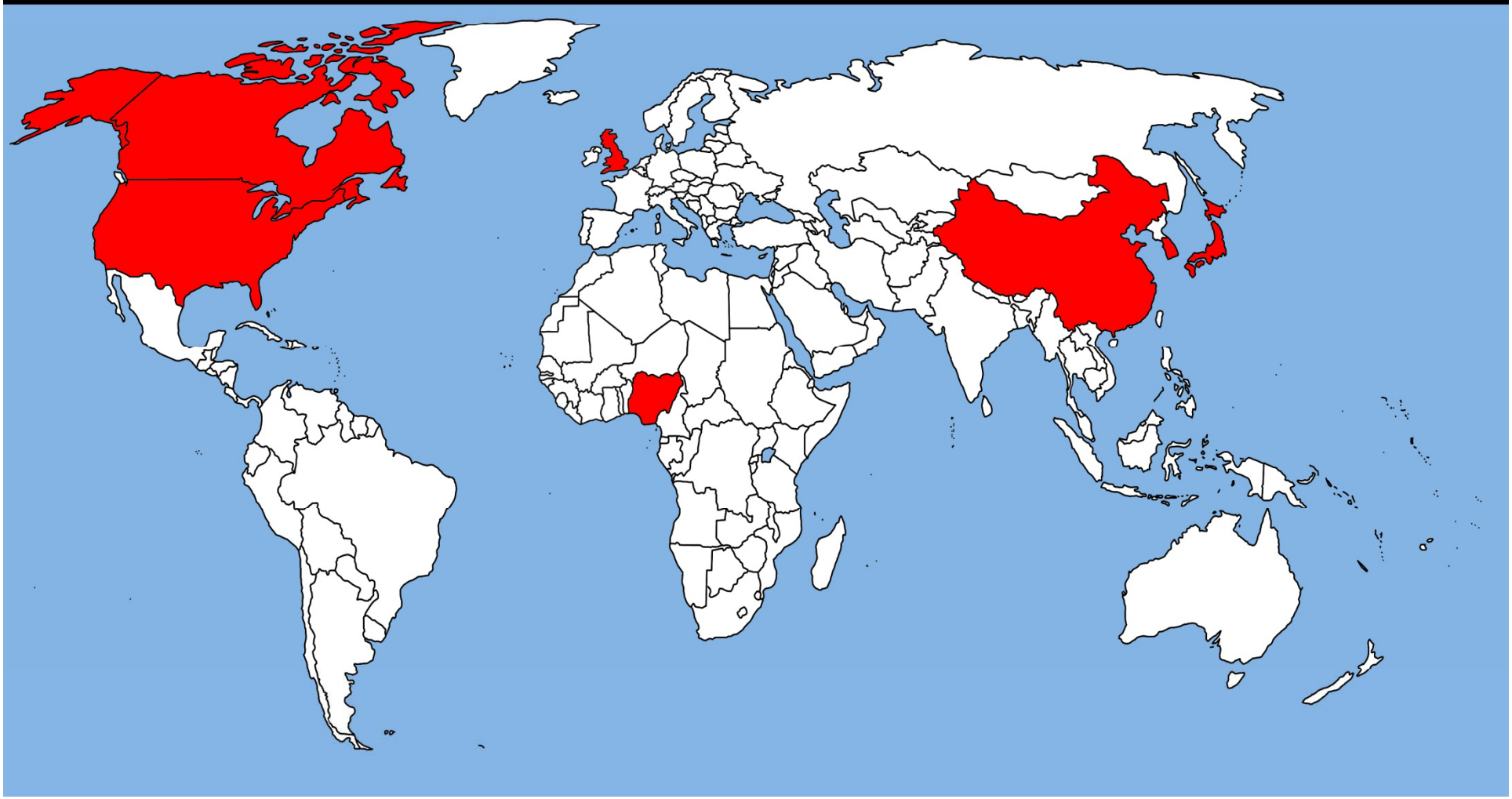
HELOC

- Fraud
- Identity Theft
- New? Same stuff, but…
  - Using computers (beyond spam)

Tracking the Fraud

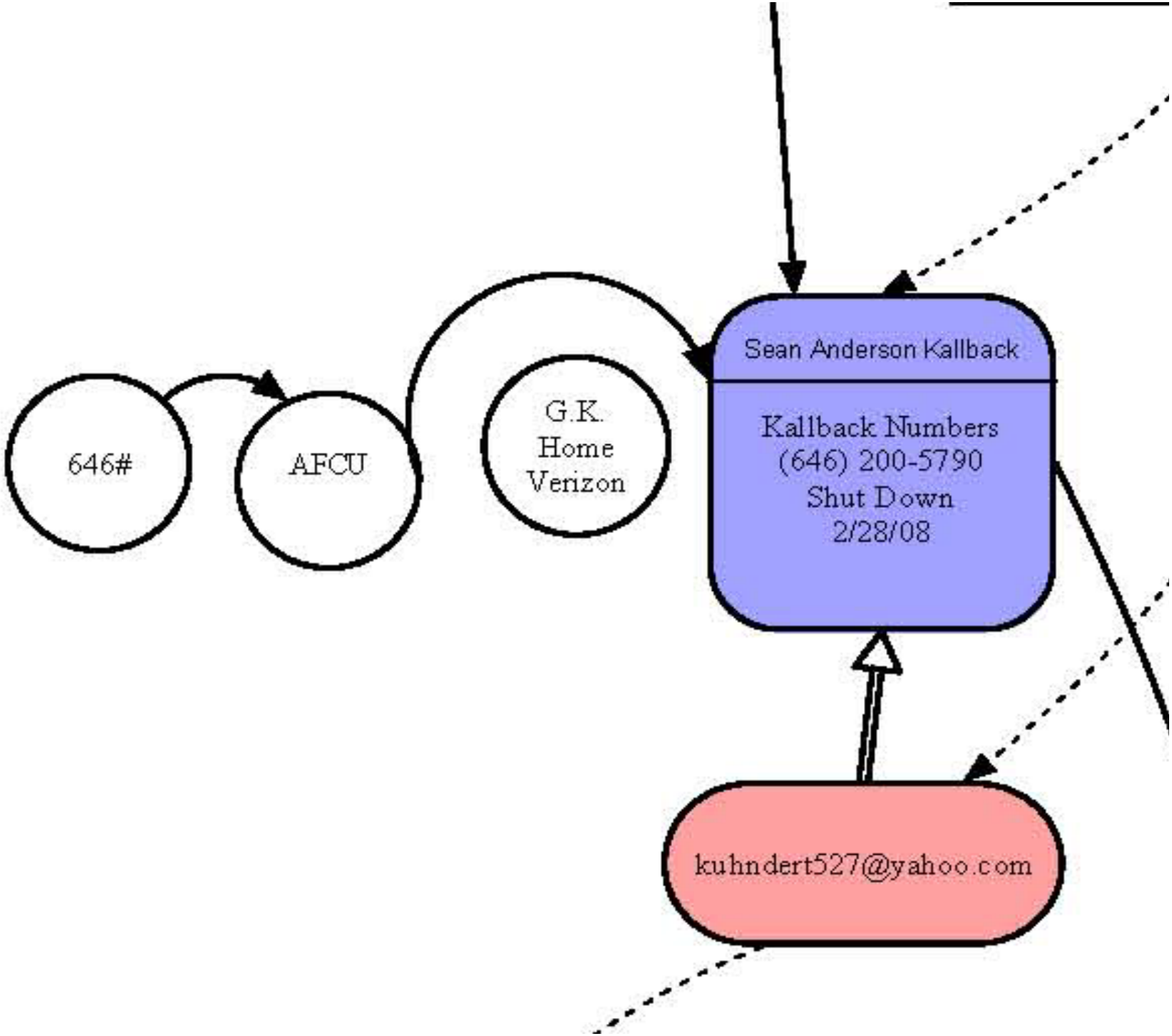
- Hear from victim bank about loss… Now what?
  - Traditional: Follow the Money
  - New: Follow the Phones
  - New: Follow the IPs

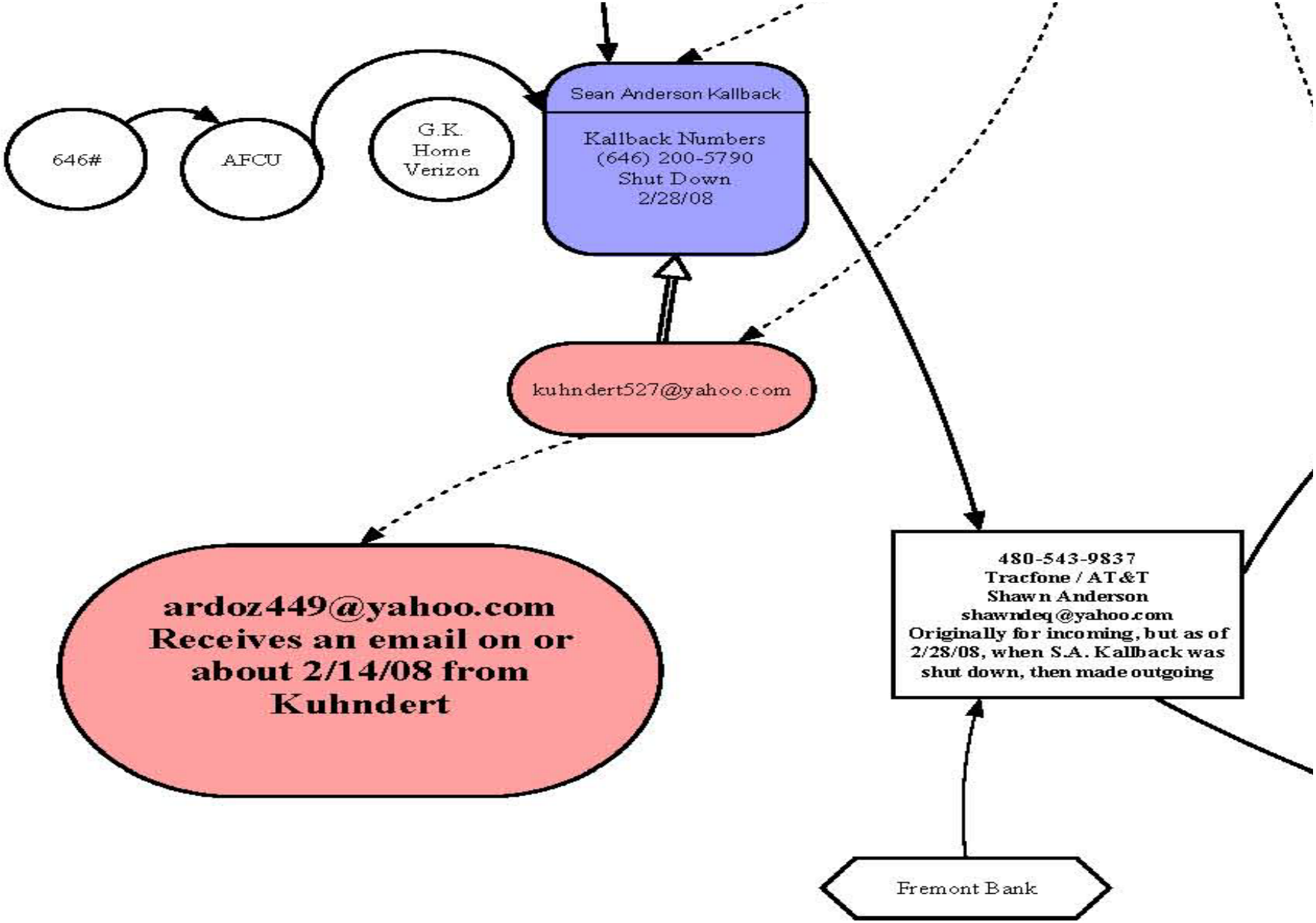
United States v. Hakeem Olokodana - HELOC Fraud Ring



New & Improved Criminals

- Phone in other names
  - Switching Phones
- Hiding IP Addresses
- Working away from the house


646#
AFCU
G.K.
Home
Verizon
Sean Anderson Kallback
Kallback Numbers
(646) 200-5790
Shut Down
2/28/08
kuhndert527@yahoo.com


646#
AFCU
G.K.
Home
Verizon
Sean Anderson Kallback
Kallback Numbers
(646) 200-5790
Shut Down
2/28/08
kuhndert527@yahoo.com
ardoz449@yahoo.com
Receives an email on or
about 2/14/08 from
Kuhndert
480-543-9837
Tracfone / AT&T
Shawn Anderson
shawndeq@yahoo.com
Originally for incoming, but as of
2/28/08, when S.A. Kallback was
shut down, then made outgoing
Fremont Bank

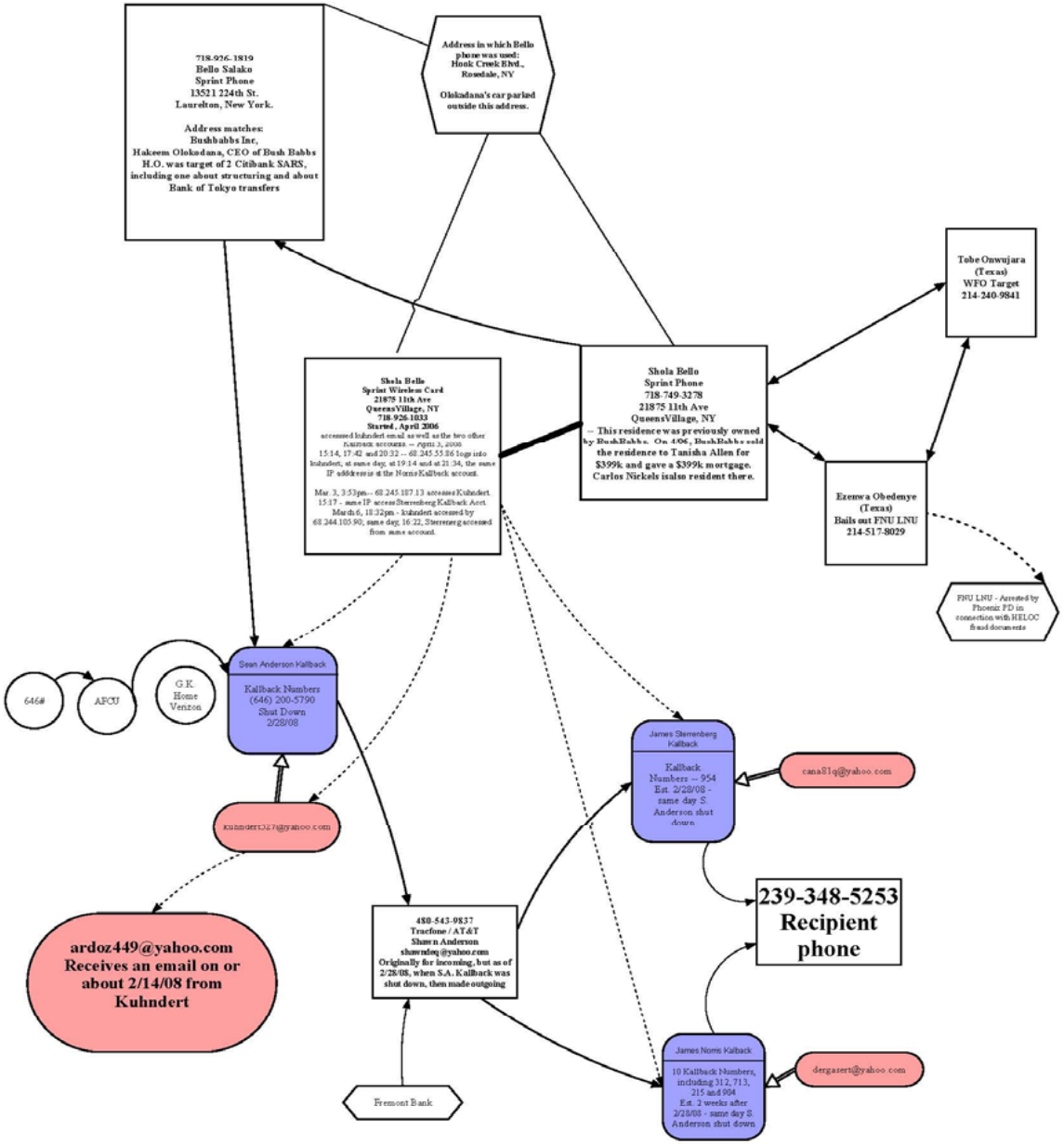
AHA!

=

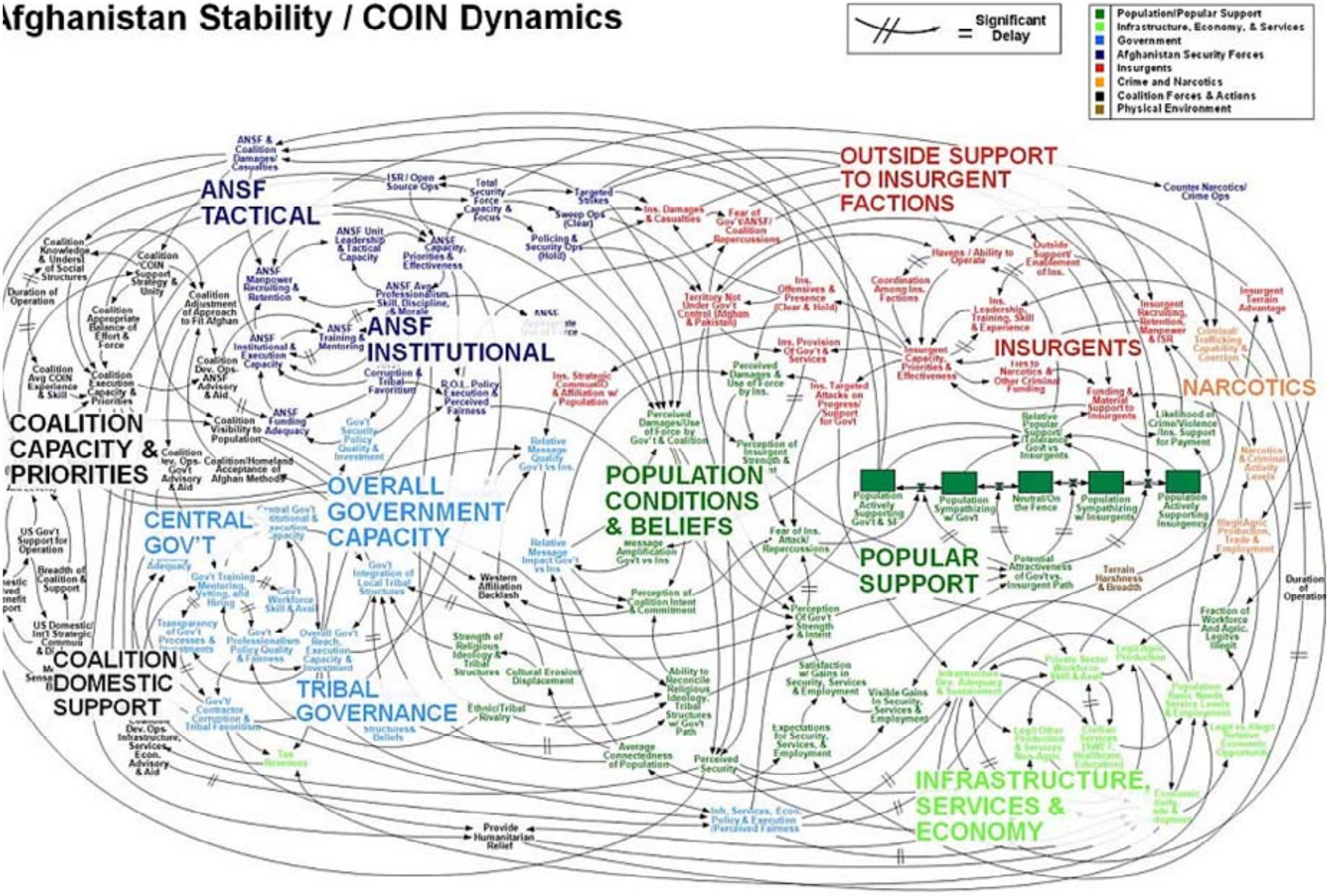
718-926-1819
Bello Salako
Sprint Phone
13521 224th St.
Laurelton, New York.

Address matches:
Bushbabbs Inc,
Hakeem Olokodana, CEO of Bush Babbs H.O. was target of 2 Citibank SARS, including one about structuring and about Bank of Tokyo transfers

HELOC FRAUD PHONE CALLS AND CONNECTIONS



Afghanistan Stability / COIN Dynamics



WORKING DRAFT – V3


CALIFORNIA
DRIVER LICENSE
B3354888
SUNTRUST
210C
Copy
Fax
Scan
SONY


VISA
VISA SIGNATURE
Cirrus
WorldPoints
Bank of America
World Points
SUNTRUST
MasterCard
PLATINUM PLUS


LG
cingular

Did Someone Lose a Cellphone?

Is it a Conspiracy?

- One large ring?
- Independent Operators?
- How far does a conspiracy extend?

Results?

- 8 Arrested
- No Bail
- 8 Convicted
- Sentences: Up to 12 years

Know Your Customer & Trust Your Systems

- "To Err is Human...."
- Anti-Fraud Measures are Pro-Customer
- Fraudsters Know Your Rules Too!


COOP LAUNCH
OFF
LAUNCH


THE
HUNT
FOR
RED
OCTOBER


CRIMSON TIDE

Data Breaches

- Challenges:
  - International in scope.
    - > 70% from overseas
  - Victim Cooperation
  - Sophistication & Patience

Corporate Fear: $$$

- Cost of Data Breach Report:
  - Per Record Cost: $142
- Stock Price Rebound:
  - Approx. 60 days
  - Victims of massive breaches?

U.S. v. Albert Gonzalez

- Where we meet Albert Gonzalez?
  - Arrested for ATM Fraud
  - 2003
- Shadowcrew
  - Landmark Carding Case
  - Indictment October 2004
  - 21 Arrested in U.S.; Others Overseas

ShadowCrew

http://www.shadowcrew.com/

Google

Design News ...cture news The Lair of t... will to live Publisher Unabashed U...shing Tool BUDGET News

United States Secret Service

WWW.SECRETSERVICE.GOV

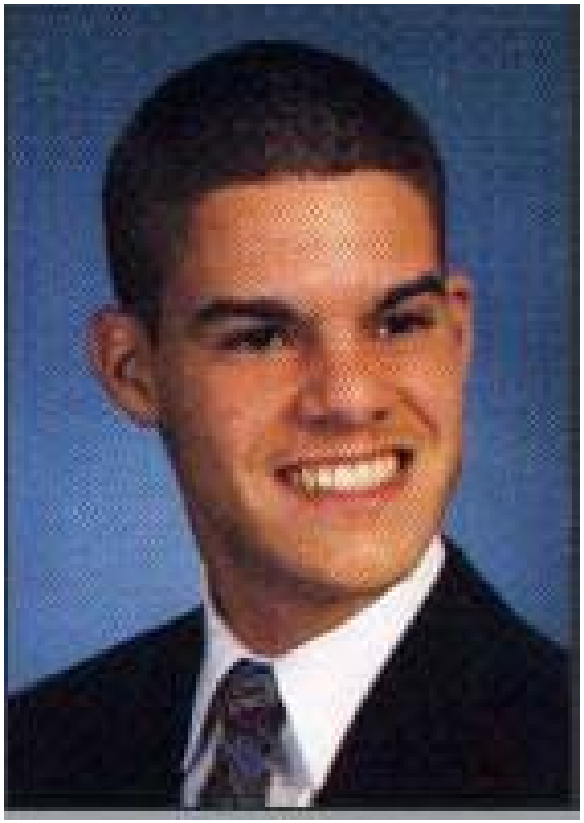
SHADOWCREW

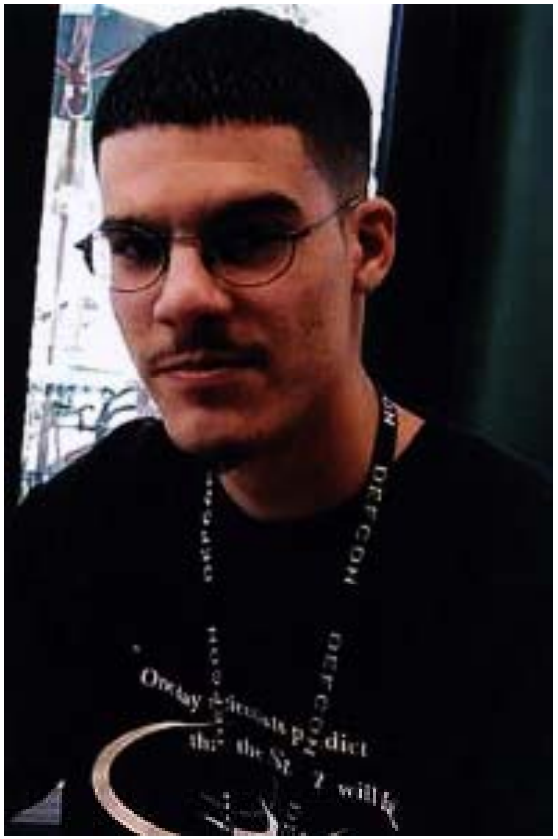
"FOR THOSE WHO HAVE TO PLAY IN THE SHADOWS....."

ACTIVITIES BY SHADOWCREW MEMBERS ARE BEING INVESTIGATED BY THE

UNITED STATES SECRET SERVICE

Gonzalez





TJX Hacking Investigation

- 2003 to 2008:
  - TJX
  - BJ's Wholesale Club
  - OfficeMax
  - Boston Market
  - Barnes & Noble
  - Sports Authority
  - Forever 21
  - DSW
- USSS & D. Massachusetts

Heartland and Others

- Continuing investigation…
- More Victims:
  - Heartland Payment Systems
  - 7-Eleven / Citi
  - Hannaford / Food Lion
  - JCPenney
  - Wetseal

Picking the Targets

- List of Fortune 500
- Visit stores – Identify POS Terminals
- Visit Websites

Executing Attacks

- SQL Injections
  - Foreign Servers
- Malware
- Network Recon
- Exfiltration

Hiding the Attacks

- Foreign Proxies
- Disabled logging by victims
- Testing against AV programs
- Erasing Evidence

Piecing Together

- 5 Victims
- Connected?
  - SQL Injection Strings (Hash)
  - Infiltration IP
  - Exfiltration IP

Chat Fragments

- “Planning my second phase against Hannaford”
- “Core still hasn’t downloaded that Wetseal shit”

Indictments

- Gonzalez Indicted
  - 3 Districts
- Longest Sentence for a Hacker:
  - 20 years (and 1 day)

Gonzalez' Statement

- "I'm fearful of what the DOJ's reaction may be if I go on record with the events of the past 10+ years... The motherfu_kers have already proven to be untrustworthy and vindictive."
  - Rolling Stone, June 10, 2010

Sentencing

- Loss Calculations
- Attempt vs. Successful
- Remedial Efforts

Our Best Practices

- Protect the rights of the victim.
- Consult with senior management.
- Consult with IT staff.
- Minimize disruption to the company.
- Coordinate media releases.
- Keep the company informed.
- Build relationships before an intrusion.

Preparedness

- Cultivate Relationships Now
- Before: Have a Response Plan
  - Accountability and Authority
  - Independence – Call Someone Else
  - Logs

Incident Response

- Assess Damage Remotely
  - Limit Access
- NO E-MAILS! (None. Really.)
- Preserve Logs
- Record Keeping

Steps to Protect

- Separation of Powers
- Immediate Cut-off
- Extra Vigilance

“Who you gonna call?”

Questions???

- Contact Info:
  - Erez Liebermann
    - 973-645-2874
    - erez.liebermann@usdoj.gov
  - Seth Kosto
    - 973-645-2737
    - Seth.kosto@usdoj.gov