RSA Conference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

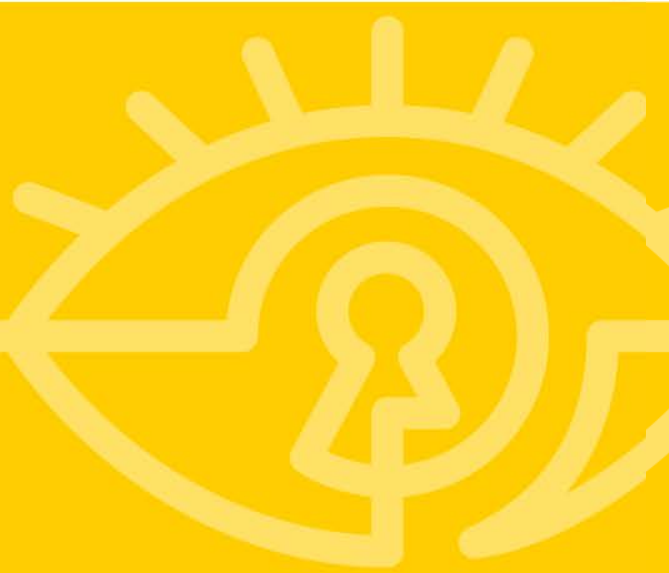
SESSION ID: PNG-R03F

Confronting Cybercrime: Exploring the Legal and Investigative Challenges

David J. Hickton

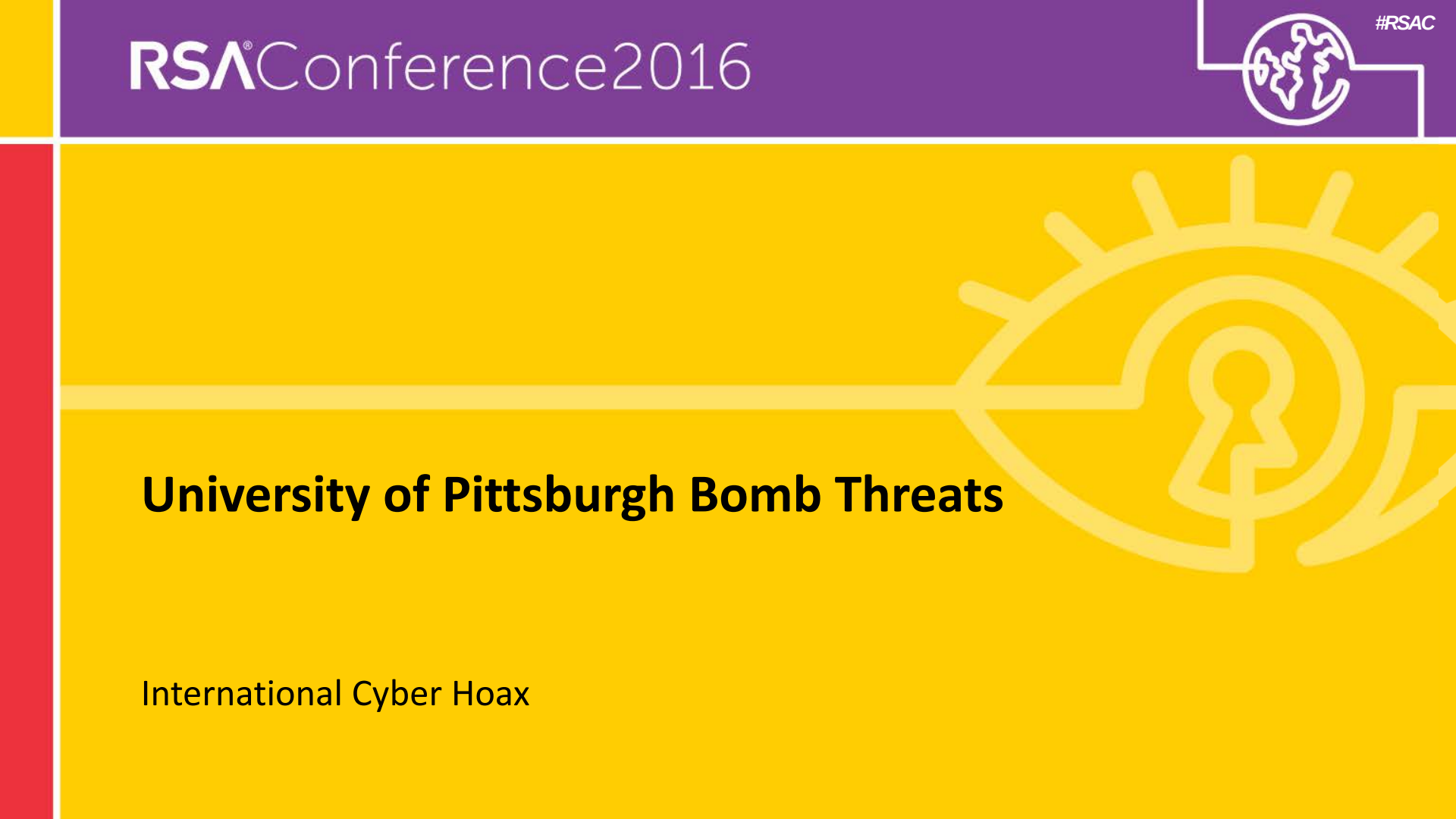
United States Attorney
Western District of Pennsylvania
@WDPANews

#RSAC



Why Pittsburgh?

Pittsburgh:
Uniquely Positioned for the Cyber Fight



University of Pittsburgh Bomb Threats

International Cyber Hoax

University of Pittsburgh Bomb Threats

March/April 2012

- 40+ bomb threats sent through anonymizers
- 100+ evacuations of buildings and students
- $300K in additional security costs to University

University of Pittsburgh Bomb Threats

Hoax Investigation

- JTTF investigates
- Overcame use of anonymizers/email remailers
- Full cooperation of Pitt's IT department
- International partners: England, Ireland and Scotland

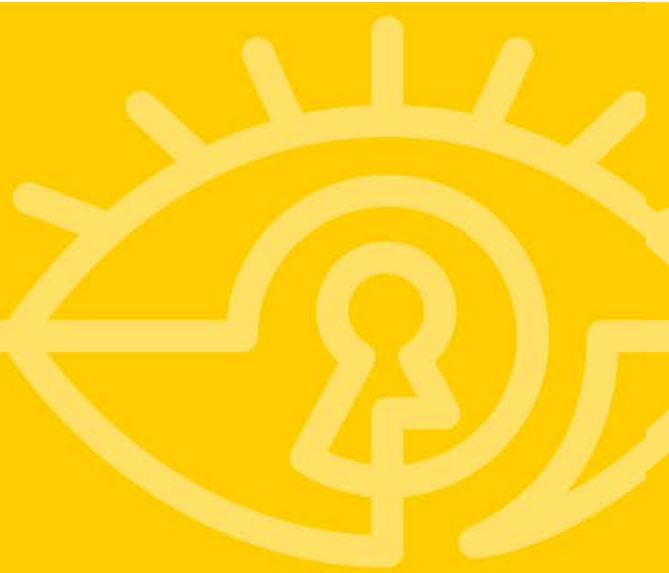
"Tell the Pitt police that bombs are in Litchfield Towers, the Cathedral of Learning, Salk, Scaife, PA and Ruskin Halls."

April 21, 2012 Email

University of Pittsburgh Bomb Threats

Adam Stuart Busby

- Indicted for email threat campaign against University of Pittsburgh, U.S. Attorney and three Federal Courthouses
- Scottish separatist living in Dublin, Ireland
- Wanted by Scotland for similar conduct
- Presently in hospital in Scotland



Chinese Economic Espionage

Industrial Hacking by a Nation State

Chinese Economic Espionage

PLA Military Hackers

- First time the United States has leveled cyber espionage charges against the military of a foreign country
- 31-count indictment charging five members of Chinese military with theft of technological secrets and communications

Chinese Economic Espionage

U.S. Entities Attacked

Chinese Economic Espionage

Westinghouse Electric Company, LLC

- Westinghouse in negotiations with Chinese Nuclear Power Corporation regarding AP1000 reactor Construction in China
- May 2010: pipe support engineering documents stolen
- 2010-2012: emails of top executives stolen

Chinese Economic Espionage

United States Steel Corporation

- Between 2009-2012, US Steel was engaged in trade cases against Chinese steel manufacturers
- Two weeks before a decision in one of the disputes, an employee working in a relevant division of US Steel received a spearphishing e-mail message
- At about the same time, names and descriptions of thousands of US Steel servers were stolen

Chinese Economic Espionage

Allegheny Technologies, Inc.

- Partner in a joint venture with major Chinese Steel Company and, between 2009 and 2012, was engaged in a trade case against the same Chinese firm
- The day after a board meeting for the joint venture in Shanghai, the network credentials for virtually every employee were stolen

Chinese Economic Espionage

United Steelworkers

- In 2012, USW's President issues a "call to action" against Chinese policies
- The next day, emails containing strategic discussions from senior union employees were stolen
- Two days after the union publicly advocated for duties on Chinese imports, more email messages containing strategic discussions were stolen

Chinese Economic Espionage

Alcoa

- In 2008, Alcoa announced a partnership with a major Chinese Aluminum company to acquire a stake in another foreign company
- Three weeks later, senior Alcoa managers received spearphishing email messages

Chinese Economic Espionage

SolarWorld USA

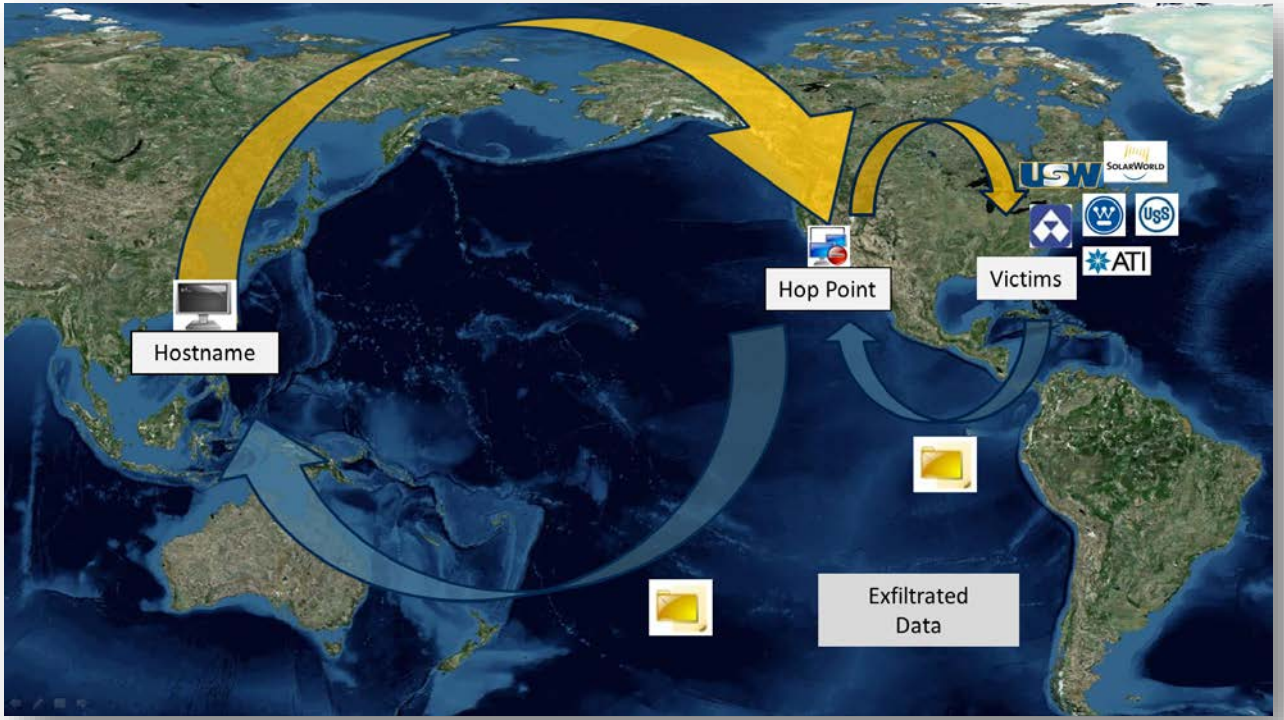
- May 2012 - September 2012: thousands of employee emails and attachments were stolen
- During the same timeframe, SolarWorld was engaged in trade cases against Chinese solar manufacturers

Chinese Economic Espionage

What Did They Steal?

- Credentials
- Intellectual property
- Strategic plans
- Cost and price data
- Trade case strategy

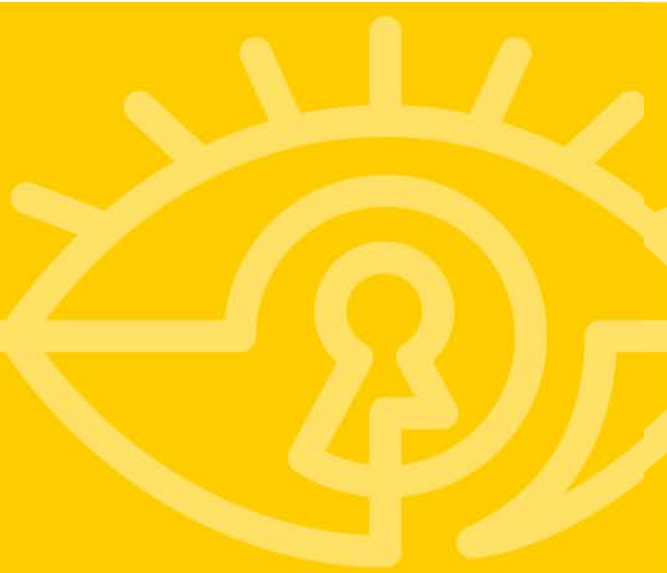
Chinese Economic Espionage



Chinese Economic Espionage

PLA Unit 61398

- Employs hundreds, perhaps thousands of personnel
- Requires personnel trained in computer security and computer network operations
- Has large-scale infrastructure and facilities in the “Pudong New Area” of Shanghai



GameOver Zeus/Cryptolocker

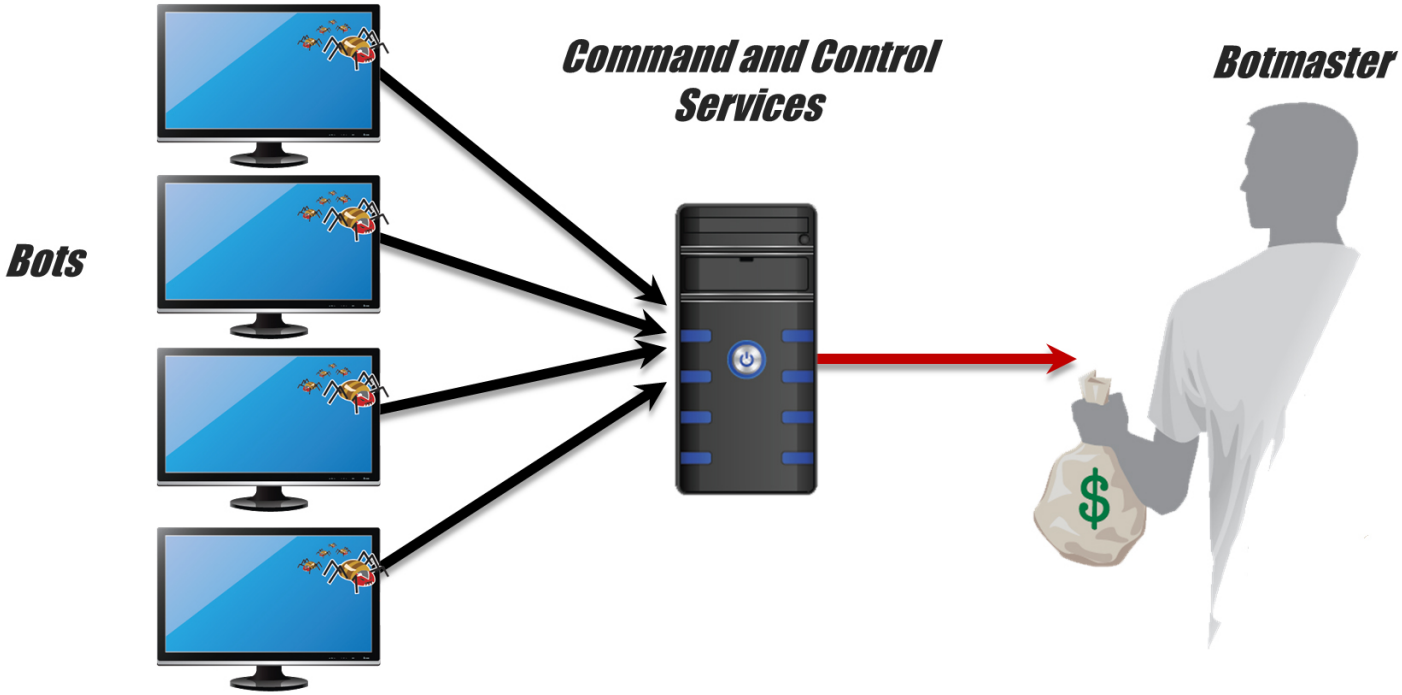
Malware Intrusion by Foreign Actors

GameOver Zeus Malware

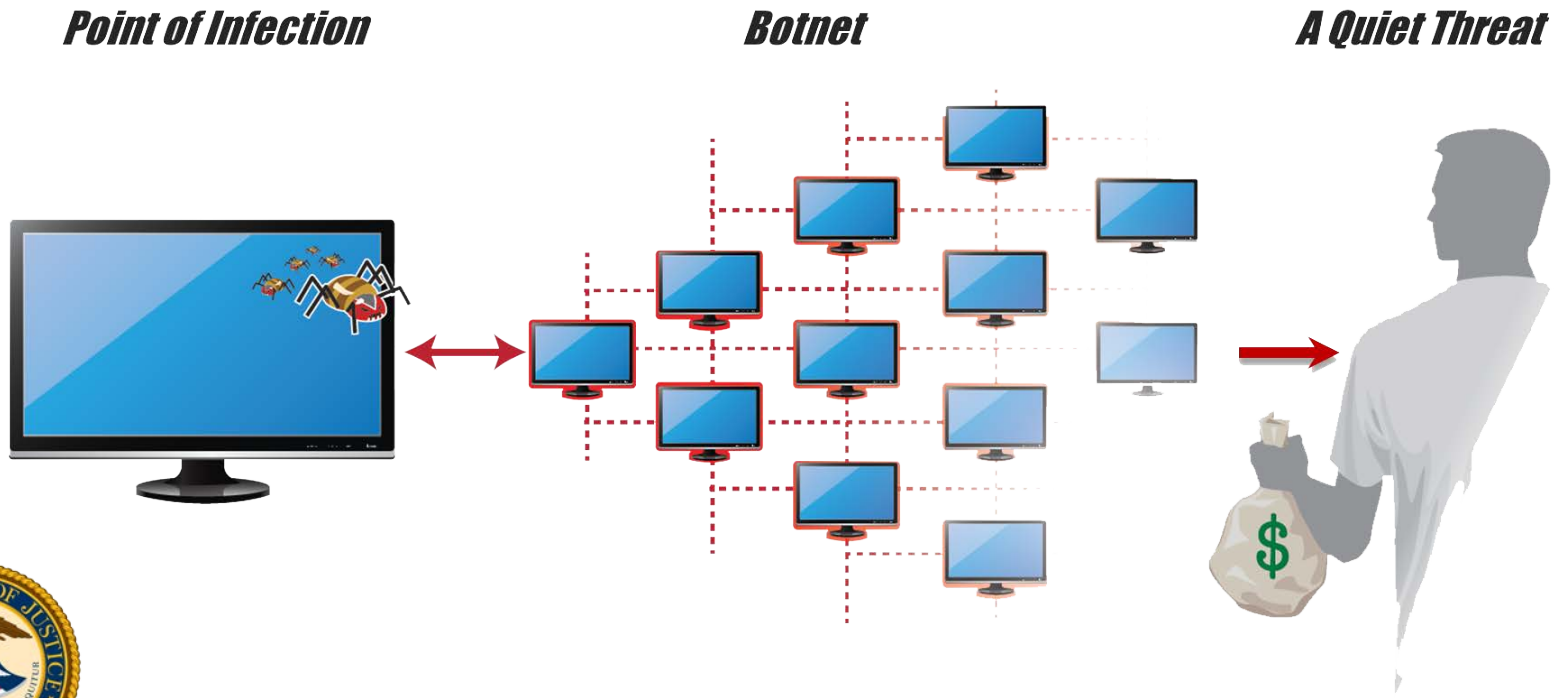
GameOver Zeus Malware

- 1 Million infected computers worldwide; 25% in the United States
- $100M+ wire transferred from compromised computers to cyber criminals overseas
- Haysite Reinforced Plastics of Erie, Penn. bilked of $375K in October 2011

Zeus Malware



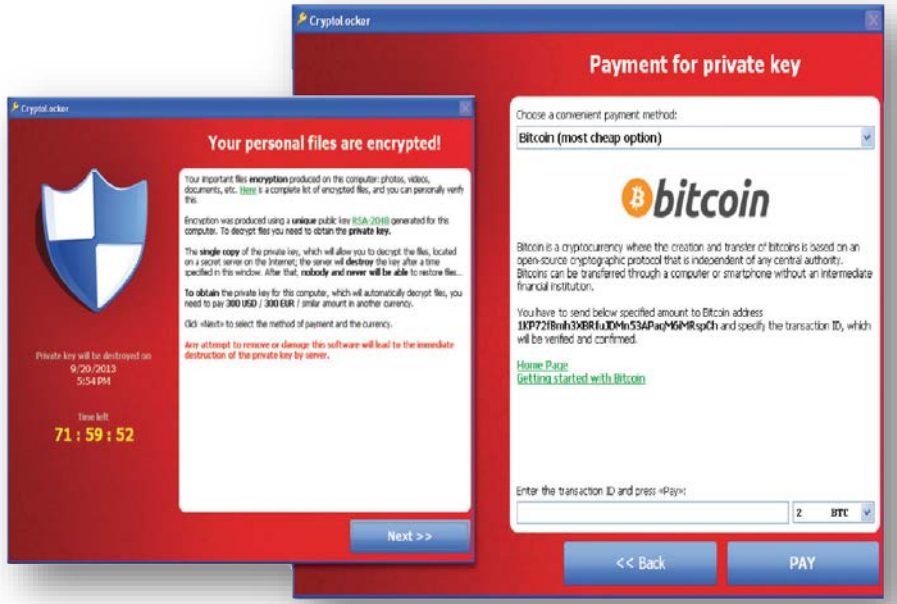
GameOver Zeus Malware



Cryptolocker

Cryptolocker “Ransomware”

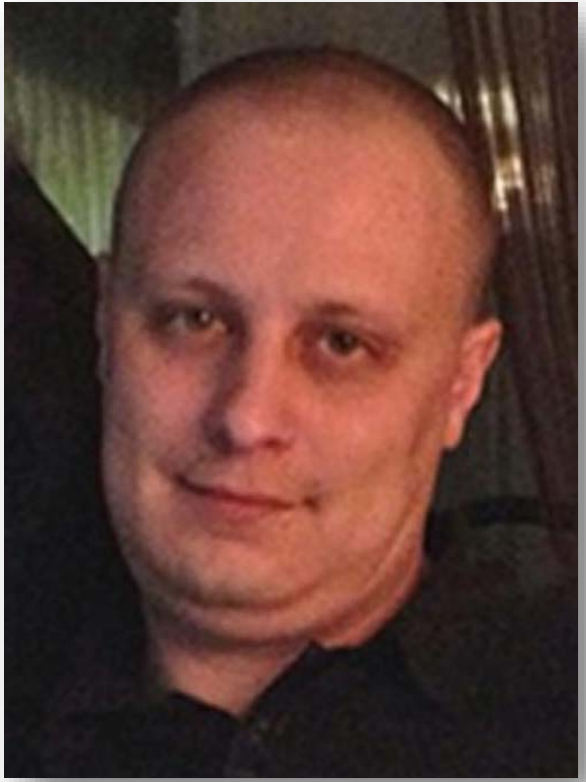
- Spread through GameOver Zeus
- Encrypts computer files, decrypting upon payment of ransom
- Computers infected: 234,000+
- Estimated losses: $27M+ in first two months of operation

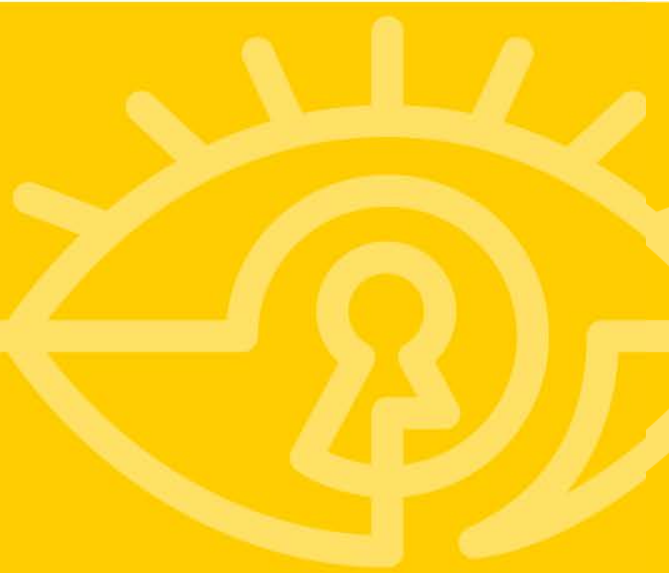


GameOver Zeus/Cryptolocker

All Tools Approach

- Criminal indictment
- Civil injunction to dismantle botnet
- International partners
- Private business partners
- $3M reward/FBI Cyber Most Wanted





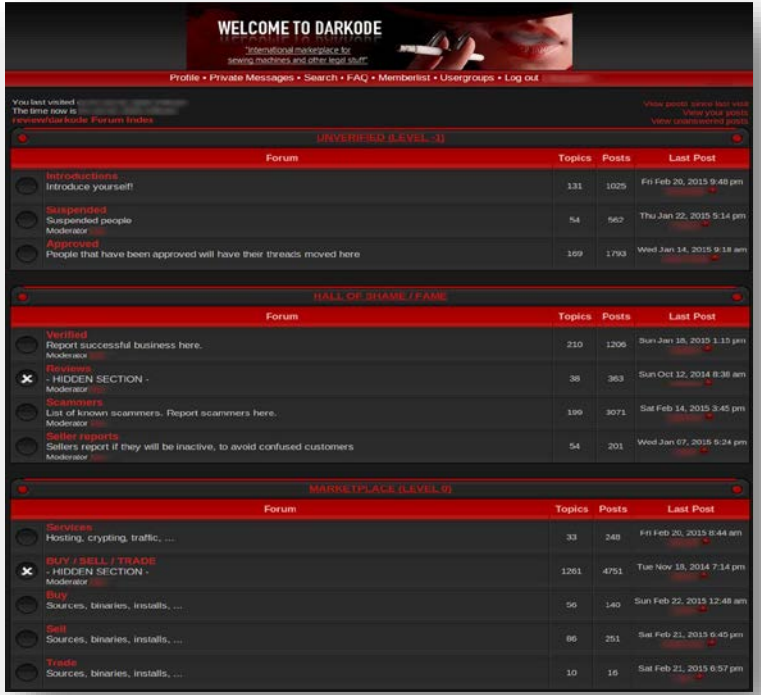
Darkode

Cybercrime Forum

Darkode

Global Cybercrime Marketplace

- Largest, most sophisticated English language forum
- Buy, sell, trade, share cybercrime products
  - Malware, botnets, passwords, Facebook Spreader, Dendroid
- Invitation only; apply with hacking resume



Darkode

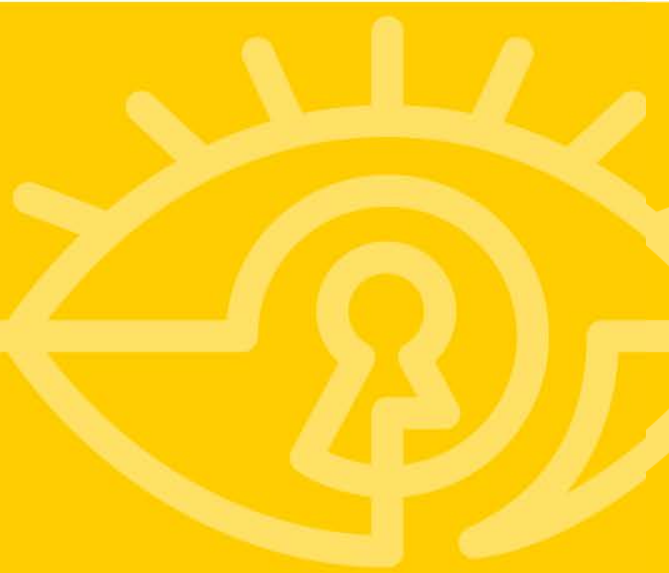
Malware example

- Dendroid: created by CMU student Morgan Culbertson, aka “Android”
- Control Android phones, place/record phone calls, intercept texts, open apps, take photos/videos, infect Android applications
- $65,000 to purchase; $300/month to lease

Darkode

Operation Shrouded Horizon

- Multi-year investigation, infiltrated forum at high level
- Seized domain
- 70 members and associates searched or arrested globally
- U.S. charges 12 criminally in U.S., Sweden, Pakistan, Spain and Slovenia



Future of Cybercrime Fighting

Future of Cybercrime Fighting

Challenges

- Privacy/Security balance
- Improved risk management
- Greater deterrence
- Resiliency

Future of Cybercrime Fighting

Opportunities

- Forge relationships with the private sector that are appropriate, lawful and effective
- Improve reporting of cyber intrusions
- Centralize intelligence and sharing regarding cyber intrusions

Future of Cybercrime Fighting

Opportunities

- Enhance development and distribution of cyber intelligence products to private sector and across government
- Increase and expedite international cooperation
- Improve victim outreach and cooperation