UAB’s Interdisciplinary Approach to Fighting Cybercrime

Richard Marchase, Ph.D.
Vice President for Research
University of Alabama at Birmingham

UAB is a National Security Agency & Department of Homeland Security credentialed Center of Academic Excellence in Information Assurance Research (CAE-R)
The Operational Model

- Address cyber crime from multiple disciplinary perspectives (e.g., criminology, psychology, computer science, information systems)
- Become a central, trusted advisor for law enforcement (international/federal/state), business, and industry
- Play a support role in solving cyber crime and deterring cyber criminals
The beginning (c. 2007)

- Blocking SPAM and taking down phishing sites – not finding the “bad guys” responsible – primary focus of industry (“whack-a-mole model”)

  - Problem: criminals know that industry is not especially interested in catching them
  - Result: without real threat of arrest and sanction, there is no deterrence and criminals will continue attacking computing systems and assets
Effective deterrence requires

- Successful investigations leading to arrests or civil sanctions
- Recovery of quality evidence available for use in civil and criminal litigation

Solution:

- Develop accurate, actionable intelligence on Spam, Phishing, and Malware attacks and provide that information to law enforcement and impacted industries and assist them in generating evidence
Implementing the Solution
The Center for Information Assurance and Joint Forensics Research (“The Center”)

- Provides information assurance-based research, development, and outreach to help ensure a safer, more productive world
- Develop state-of-the-art solutions for government, business, and institutional partners
- Offer practical computer science and social science-based research, scholarship, services, and products to enhance integrity of global cyber-infrastructure
- Outreach to community, government and industry
- “In-reach” within UAB to grow capacity
Center Origins and Evolution

Interdisciplinary partnership begun in 2006

- Departments of Computer and Information Sciences and Justice Sciences
- Focus: address cyber crime with the rigor of “mature science”

2006-2011: successes with *Fortune* 500 companies to address cyber crime

2011: Center officially approved by UA System as UWIRC
The Center

- 30+ professors and many students
- Members from computer science, justice science, business, health professions, and others
- Contracts for service
- Federal funding (e.g., NSF; DARPA)
- Targeted initiatives from government
Fighting Cyber Crime

Partners:

facebook
Microsoft
ups
Bank of America
Yahoo!
twitter
BBVA Compass
Regions
LinkedIn
NACHA
Google
United States Postal Inspection Service
NASA
Treasury
Internal Revenue Service
Alabama Bureau of Investigation
FDIC
Targeting Cyber Crime
Fighting Cyber Crime

- Interdisciplinary coordination of Center affiliates to address cyber crime and security issues
  - Information assurance and security
    - Focus: managing risks related to the use, processing, storage, and transmission of information
  - Intelligence analytics
    - Focus: information gathered from non-classified, non-secret sources including news media, the Internet, and commercial databases (e.g., Whois)
  - Human-computer interaction
    - Focus: understanding how user/computer interactions creates opportunities for cyber criminals to engage in illegal activities
  - Intersection of computer science, behavioral sciences, and design
  - Imagery and geospatial analytics
    - Focus: applying statistical analysis and other informational techniques to data which has a geographical or geospatial aspect.
Multidisciplinary Focus of Center in Cyber Crime Arena
Center focus in fighting cyber crime

- Identify attack commonalities on different brands
- Evaluate scope and nature of impact to prioritize response
- Recognize trails attackers leave behind and link to specific incidents
- Exploit open source intelligence including social media, Twitter, “chat rooms,” etc.
- Connect key people and enable them with actionable intelligence
Serve as a common, trusted clearing-house that allows competitors to legally cooperate and safely address common problems

- Data are “pre-enforcement” and not subject to same constraints as that of evidence involved with litigation or as proprietary information
Domains:

“Big Data”: datasets with sizes beyond the ability of commonly used software tools to capture, curate, manage, and process within tolerable elapsed time (e.g., UAB Spam Datamine (~600 million archived emails))

Knowledge discovery/data mining: interdisciplinary focus on methodologies for extracting useful knowledge from existing data that draws on research in statistics, pattern recognition, machine learning, data visualization and optimization, and high-performance computing

Machine learning: construction and study of systems that can learn from data (e.g., designing systems to learn to distinguish spam and non-spam messages to then route incoming messages into spam and non-spam folders)
Domains (contd.)

- **Development of new tools and processes**: 7 Steps to Phishing Investigations; Emerging Threats by Email Report
- **Human-computer interaction** and how it facilitates problems
- Internet-based **victimization** (e.g., fraud, cyberstalking, cyberbullying, etc.)
- **Security threats**: existing and emerging
Fighting Cyber Crime

IP Developed by Center
7 Steps for Phishing Investigations

- Analyze spam and related messages sent by same source to reveal clues about sender’s identity
- Analyze phished site to mine intelligence about its construction
- Analyze “kit files” used to create phishing site (“kits” contain important clues in the comments and source code, including email addresses of criminal(s))
- Perform cluster analysis using automated techniques to compare closely related phishing sites to determine if additional information may be found on other sites created by same criminal(s)
- Conduct analyses of logs at the compromised servers that host the phish and those of the client (these contain a wealth of information about the criminal, victims, and the techniques favored by the criminal)
- Engage in analysis of open source intelligence including forums, chat rooms, Facebook pages, etc. to gather additional information
- Provide affidavits of probable cause for search warrants related to phishing scheme
Emerging Threats by Email Reports

- Daily report that contains analysis of top malware and related attacks based on analysis of UAB Spam Data Mine
- Sent to subscribing companies including UPS, Bank of America, and PayPal
- Sent to the FBI and other law enforcement and computer security groups at no charge
- Funded by grant from the UPS Foundation
Fighting Cyber Crime

Spinoff: Malcovery Security, Inc.
Malcovery Security

- IT and IS related security and business solutions
- Focus: application of data mining principles and powerful analytic techniques to large evidentiary data sources to provide unique intelligence that will significantly enhance the process of identifying cybercriminals, prioritizing cybercrime investigations, and protecting consumers, corporations, and governments from online fraud and cyberattacks
- Strategic partnerships with Radiance Technologies, Internet Identity, and IBM
- Location: Innovation Depot
Center Kudos: Some Examples
Thanked on page one of the FBI.gov website for help with “Operation Ghost Click”

Stories

Home • News • Stories • 2011 • November • International Cyber Ring That Infected Millions of Computers Dismantled

Operation Ghost Click
International Cyber Ring That Infected Millions of Computers Dismantled

11/09/11

Six Estonian nationals have been arrested and charged with running a sophisticated internet fraud ring that infected millions of computers worldwide with a virus and enabled the thieves to manipulate the multi-billion-dollar internet advertising industry. Users of infected machines were unaware that their computers had been compromised—or that the malicious software rendered their machines vulnerable to a host of other viruses.

Details of the two-year FBI investigation called Operation Ghost Click were announced today in New York when a federal indictment was unsealed. Officials also described their efforts to make sure infected users’ internet access would not be disrupted as a result of the operation.

New York Field Office

Manhattan U.S. Attorney Charges Seven Individuals for Engineering Sophisticated Internet Fraud Scheme That Infected Millions of Computers Worldwide and Manipulated Internet Advertising Business

Malware Secretly Re-Routed More Than 4 Million Computers, Generating at Least $4 Million in Fraudulent Advertising Fees for the Defendants

National Press Releases

International Cooperation Disrupts Multi-Country Cyber Theft Ring

October 01, 2010

The FBI and international law enforcement, working in an unprecedented partnership, have disrupted a large-scale, international organized cybercrime operation active in several countries that resulted in numerous search warrants and arrests.

Operation Trident Breach began in May 2009, when FBI agents in Omaha, Nebraska, were alerted to automated clearing house (ACH) batch payments to $46 separate bank accounts throughout the United States. Agents quickly realized the scope of the crime and partnered with local, state, and federal partners, cybercrime task forces, working groups, and foreign police agencies in the Netherlands, Ukriane, and the United Kingdom to bring those responsible to justice.
NBC's *Rock Center* features UAB's Computer Forensics Research Laboratory

Facebook donates recovered money to UAB cyber crime group
Summary

- The Center seeks multidisciplinary solutions to pressing cyber-related issues and problems
- Create critical mass of collaborating scientists and researchers
- Focus on Research and Development to assist partners to better identify criminals, enhance the efficiency and efficacy of their investigations, and successfully pursue legal action against those violating civil or criminal laws
- Key to success is partnering with government, business, and industry
- http://thecenter.uab.edu
THANK YOU!