London Action Plan
International spam enforcement network

CNSA
The EU Contact Network of Spam Authorities

TRAINING WORKSHOP: ONLINE THREATS INVESTIGATIONS FOR LAW ENFORCEMENT AGENCIES

With the help of the Messaging Anti-Abuse Working Group (MAAWG) and international enforcement experts, the London Action Plan (LAP) and the European Union Contact Network for Spam Authorities (CNSA) are conducting a collaborative **Training Workshop: Online Threats Investigations for Law Enforcement Agencies.**

This training workshop is an integral part of the overall ***3rd Joint LAP/CNSA Workshop: Collaborative Ventures to Fight Online Threats.***

Objectives

This workshop is intended to provide Law Enforcement Agencies with an opportunity to:

- Understand the global nature of the malware industry
- Learn how to extract, analyse and leverage evidence for successful prosecution
- Reinforce networking in order to develop professional inter-relationships with Law Enforcement Agencies and public/private sector stakeholders
- Create better cooperation and synergy
- Build trust to share knowledge, information and expertise, and to
- Maintain momentum acquired so far.

Dates/Times

Wednesday, October 10, 2007 (Location: Marriott Crystal Gateway Salon 3)

08:45am – 09:45am	Training Session 1 - Basic Spam Forensics
09:45am – 10:45am	Training Session 2 - Network-Based Methods for e-Crime

Thursday, October 11, 2007 (Location: Marriott Crystal Gateway Salon A & B)

08:30am – 10:00am	Training Session 3 - Chasing the Spammers: Legal Aspects
10:15am – 11:15am	Training Session 4 - Get a Grip on Malware

London Action Plan
International spam enforcement network

CNSA
The EU Contact Network of Spam Authorities

LAP/CNSA Training Workshop: Online Threats Investigations for Law Enforcement Agencies

Wednesday, October 10, 2007	
8:45 – 9:45am	Serge Presseau, Senior Policy Advisor, Industry Canada (Moderator) **Session 1 - Basic Spam Forensics** John Levine, MAAWG Senior Technical Advisor This session introduces the basic techniques of analyzing e-mail messages. Participants will learn the structure and relevant parts of messages, and how determine which parts are authentic or forged. They also will learn about online resources such as WHOIS and DNS useful in message analysis.
9:45 – 10:45am	**Session 2 - Network-Based Methods for e-Crime Investigations** Patrick Peterson, V-P Technology, IronPort Systems Netflow, packet-level captures, destination IP addresses, source & destination ports…do you understand how these and other network issues can assist you in your investigation? This session will demonstrate how some networks can be instrumented with passive monitoring, allowing the collection of these flow level summary data. Other tools and techniques will also be explored.
Thursday, October 11, 2007	
8:30 – 10:00am	**Session 3 - Chasing the Spammers: Legal Aspects** Chris Duffy, Senior Investigator, Anti Spam Team, Australian Communications and Media Authority (ACMA) Thomas X. Grasso, Supervisory Special Agent, Federal Bureau of Investigation (FBI) Steven Wernikoff, Staff Attorney, Federal Trade Commission (FTC) The session will provide an overview of the legal issues encountered in investigating and prosecuting spammers and their operations. The session will explore the legal issues agencies face in conducting an investigation, including obtaining information from Internet service providers and sharing information with foreign counterparts. The session will also consider the various civil and criminal legal theories available to prosecute or sue spam operations.

10:00 – 10:15am	Refreshment Break
10:15 – 11:15am	**Session 4 - Get a Grip on Malware** Marcel van den Berg, Digital Investigator, Dutch OPTA This training will teach you how to get a grip on malware and make a rapid analysis. This hands-on course will provide an introduction into the tools and methodologies used to perform analysis of malware. If possible bring a laptop with WindowsXP running in VMware with an internet connection. Conclusion/Closing Remarks - Neil Schwartzman, Executive Director, CAUCE