The ILLBuster project

http://www.illbuster-project.eu

Fabio Roli
University of Cagliari, Italy
DG-HOME – Call ISEC: *Prevention of and Fight Against Crime*

**Priorities:** *Projects on sexual exploitation of children, illegal use of Internet and cybercrime*

1. Supporting prevention and fight sexual exploitation and abuse of children, in particular but not exclusively in the online environment
2. Promoting cooperation between law enforcement, private sector and civil society for that purpose.
3. Supporting co-operation, including training, between experts, private sector and law enforcement authorities on understanding and combating fraud (including identity fraud) and illegal trade on the internet and other types of illegal activities
4. Co-operation to develop and exchange efficient methods of detecting illegal contents
Partners roles

Academic partners
- University of Cagliari, Italy
- University of Milano Bicocca, Italy
- Tech and Law Center, Italy
- University of Georgia, USA

LEAs
- Polizia di Stato, Italy
- Guardia di Finanza, Italy

Technological partners
- NASK, Poland
- NetClean, Sweden
- Tiscali, Italy
- DBI, Denmark
Project scenario

- Analysis of illegal contents on the web is often a Sisyphus task for LEA analysts
  - **2013 INHOPE figures** ([http://www.inhope.org](http://www.inhope.org))
    - 1,210,893 reports processed
    - by 170 analysts worldwide
    - serving 2.7 billion of internet users

- Discovery of illegal contents by hotlines reports and analysts’ investigations is extremely difficult when contents are hosted on botnets just to hide such contents
Project goals

1) Computer-assisted hotline for automatic report of suspicious web sites
2) Computer-assisted inspection of suspicious web sites
3) Computer-assisted discovery of suspicious web sites hosted on fast-flux networks
Targeted illegal web contents

1) Computer-assisted hotline for automatic report of suspicious web sites
2) Computer-assisted inspection of suspicious web sites
3) Computer-assisted discovery of suspicious web sites hosted on fast-flux networks

• Malware
• CSAM - Child Sexual Abuse Material
• Phishing
• Counterfeit medicines
Project goals

1) Computer-assisted hotline for automatic report of suspicious web sites
2) Computer-assisted inspection of suspicious web sites
3) Computer-assisted discovery of suspicious web sites hosted on *fast-flux networks*
• **Fast flux** is a DNS technique used by botnets to hide illegal web sites behind an ever-changing network of compromised hosts acting as proxies

  ✓ each node is a compromised computer with public IP address (fast flux agent)
  ✓ a single Fast Flux Domain Name may resolve to thousands of different nodes scattered around the world

**Project goal:** The ILLBuster system should allow LEA analysts to perform a computer-assisted discovery of suspicious web sites hosted on fast-flux networks
The ILLBuster project builds on FluxBuster.

Flux Buster is a research prototype developed by PRA Lab for the automatic detection of Fast flux networks through passive analysis of DNS traffic in large networks.

Project organization and timing

**Project Duration:** 24 Months

- **Start Date:** February 1st, 2014
- **End Date:** January 31, 2016

**Project activities are organized along 5 work-packages**

- **WP1** – Management (from M1 to M24)
- **WP2** – ILLBuster Platform Development (from M1 to M12)
- **WP3** – Legal and Ethical Compliance (from M1 to M12)
- **WP4** – Training and Testing with LEAs (from M13 to M24)
- **WP5** – Dissemination (from M1 to M24)
The ILLBuster project idea

FluxBuster
Network Analysis

flux URLs

blacklisted
URLs

URLs

Job
Manager

Content
Extractor

CSAM
Detection

NetClean
ICAP

Phishing Detection

Malware Detection

Fake Medicines

Computer-assisted hotline

Legal compliance

ILLBuster interface
The ILLBuster project idea

FluxBuster Network Analysis

- flux URLs
- blacklisted URLs

URLs

LEA URLs

ILLBuster Dashboard

Malicious Domain 3 - http://maldomain.xxx3.mal

- Malicious URLs
  - URL1
    - Malware
    - Inspect
  - URL2
    - Phishing
    - Inspect
  - URL3
    - Pharmacy
    - Inspect
  - URL4
    - CSAM
    - Inspect

Confidence

Feedback

- Is malicious?
- Send Report

ILLBuster interface

Computer-assisted hotline
ILLBuster logical architecture

- **FluxBuster**
  - fast flux networks
- **PageFinder**
  - flux URLs
- **N6**
  - blacklisted URLs
- **LEAs data sources**
  - LEAs URLs
- **ILLBuster interface**
- **CSAM Detection**
- **HSN2**
- **Counterfeit Medicine Detection**
- **Low-interaction Client Honeypot**
- **Malware Detection**
- **Phishing Detection**
- **High-interaction Malware Detection**

Computer-assisted hotline
CSAM detection module

- All traffic that flows from the infrastructure of ILLBuster is inspected by a Netclean appliance
  - works as a ‘proxy’, and if suspicious material is found,
    - the connection is dropped (no CSAM material will be hosted within the ILLBuster platform)
    - the related URL is marked as being related to CSAM
      - to be further inspected by law enforcement personnel
Malware Detection

- Detection is performed by
  - looking at known malicious patterns by rules; e.g., a specific ActiveX instantiation, files written on disk, registry modifications
  - exploiting machine learning algorithms developed by PRA Lab (e.g., algorithms for JavaScript malware detection)
Phishing and counterfeit medicines

- PRA Lab is developing tools based on machine learning for the detection of phishing and counterfeit medicine webpages.

- They learn automatically from a set of known webpages, as well as the related legitimate targets.

Input features for detection:
- Web page contents
- Network source data

- Logo violations
- Trademark violations
- Use of product pictures
Where we stand now…

HW infrastructure just settled in

First versions of SW modules are going to be deployed

Preliminary results on CSAM and malware detection expected in October 2014
Contacts

Project website
http://www.illbuster-project.eu

PRA Lab website
http://pralab.diee.unica.it

Fabio Roli rol@diee.unica.it