

# **CYPRUS POLICE**

**Office for Combating Cyber Crime  
and  
Digital Forensic Laboratory**

**Cyprus Police Headquarters**



28/11/2016

Γραφείο Καταπολέμησης Ηλεκτρονικού Εγκλήματος

# Agenda

- Establishment of Office Combating Cybercrime and Digital Forensic Lab and responsibilities
- Type of cases we are facing in Cyprus
- Main legislation
- Cooperation
- Reporting

# Establishment of the Office for Combating Cyber Crime

- The Office for Combating Cyber Crime was established in September 2007 based on the Police Order 3/45.
- The Digital Forensic Laboratory (D.F.L.) is under the same administration and was established in 2009.
- There are six (6) investigators working at the Office for Combating Cyber Crime and nine (9) forensic analysts working at the D.F.L. on shift basis.

# Duties

- Investigation of serious offences held via the internet and offences related to computers and data
- Cooperation with officers from other organizations
- Organizing training sessions
- Statistics preparation
- Participation in events and lectures
- Observing the evolution of technology

# DIGITAL FORENSIC LAB (D.F.L)

- D.F.L was established on 2009 and falls within the effective examination of electronic evidence. D.F.L is staffed with specialized personnel for collection of evidence and digital forensic analysis of electronic devices
- It's the only Government Computer Forensic Lab in Cyprus

# D.F.L

- **Mission**: Collection and forensic analysis of digital devices as well as the presentation of scientific testimony as expert before the court
- **Responsibilities**
  - Collection of e-evidence at crime scenes
  - Forensic examination of e-evidence and presentation of scientific testimony before the court
  - Training (police staff and other organization's staff)

# D.F.L

- **Capabilities**

- Forensic Imaging of e-evidence
- Forensic Analysis of e-evidences (FTK, EnCase, IEF, Atola, Virtualization)
  - Index search
  - Data Recovery
  - Export
  - Data analysis
  - Data verification

# E-evidence admissibility

The basic principle of forensic examination of electronic evidence is the integrity of the original evidence, except in such circumstances where the action is fully justified



# Types of cases

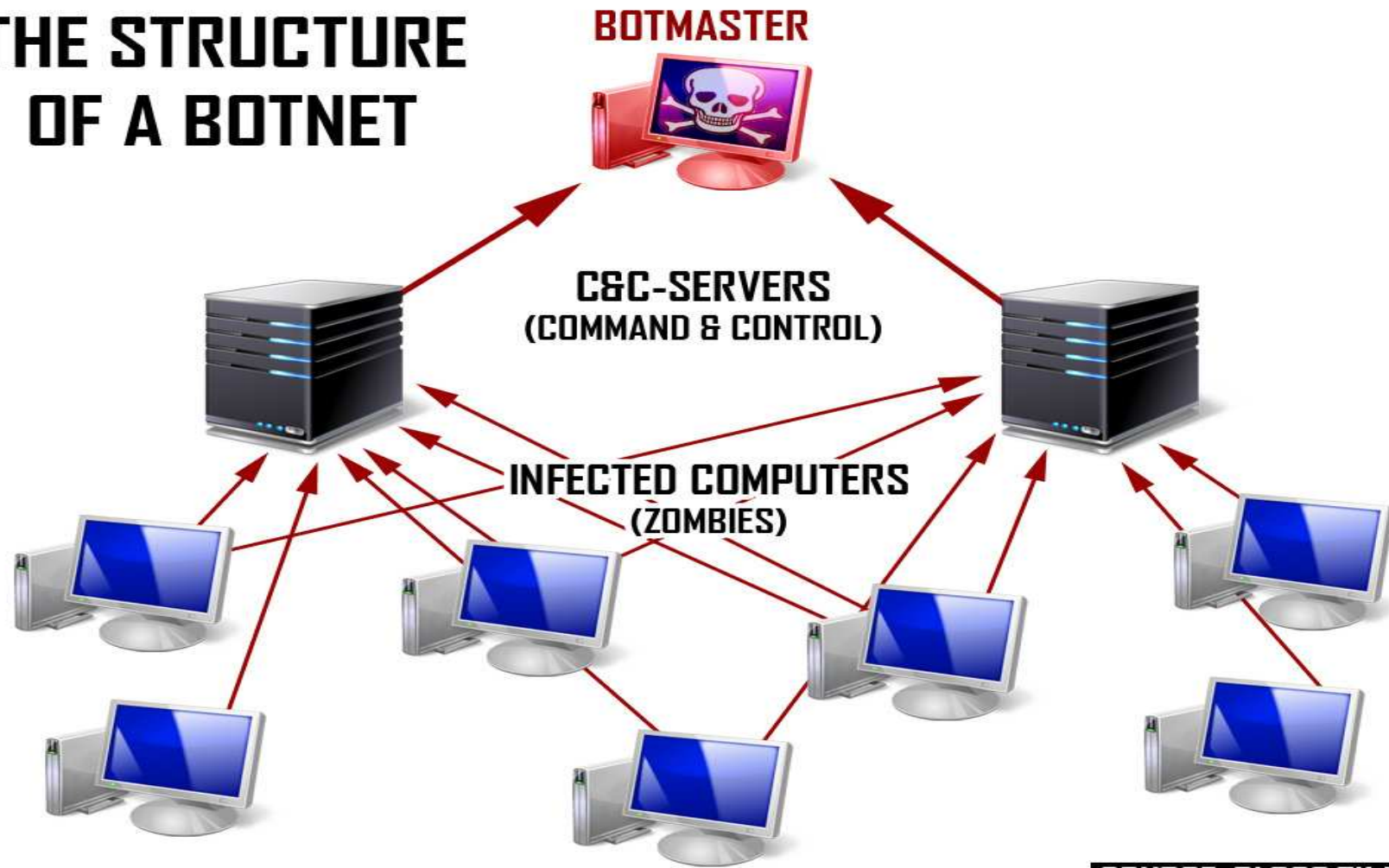
- Child pornography (content related crimes)
- Attacks on information systems (hacking)
- Computer related forgery (phishing sites)
- Malwares
- Gambling
- Requests from other countries (Mutual Legal Assistance Treaty MLAT).

# Hacking



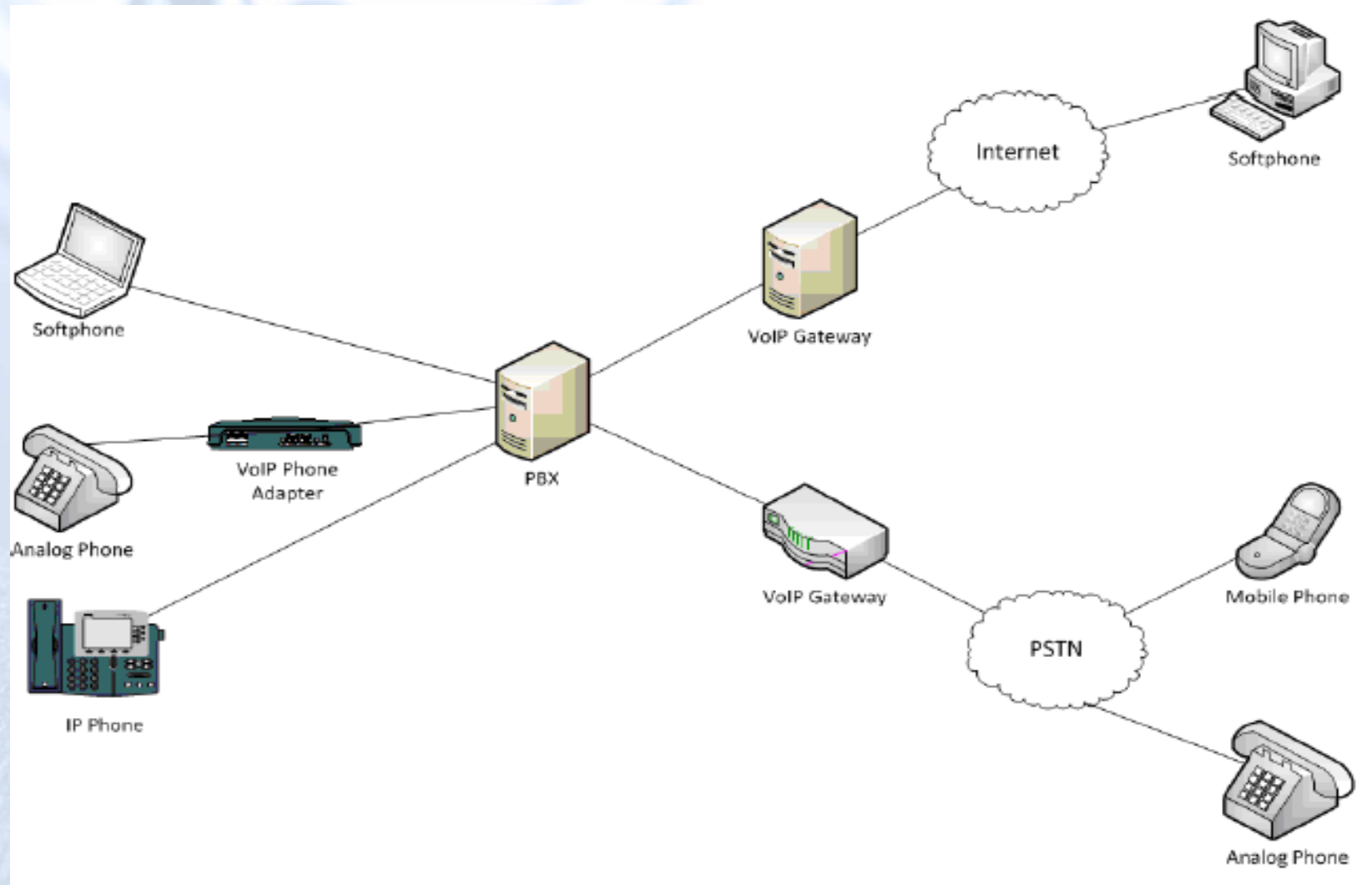
# Hacking

## THE STRUCTURE OF A BOTNET



SOURCE: BLOGG.TKJ.SE

# Hacking



# Phishing

The image shows a browser window with a yellow address bar displaying the URL <http://www.rfiimports.com/cpg146/albums/home/>. A warning icon in the address bar indicates a "Suspicious Website". A modal dialog box is overlaid on the page, titled "Suspicious website" with a warning icon. The dialog contains the following text:

This might be a phishing website.

Phishing websites impersonate trustworthy websites for the purpose of obtaining your personal or financial information.

Microsoft recommends that you do not give any of your information to such websites.

Report whether or not this is a phishing website.

At the bottom of the dialog is a link: [What is Phishing Filter?](#)

The background page is a PayPal login page. It features the PayPal logo at the top, followed by "Welcome" and "Send" buttons. Below this is a "Member Log-In" section with input fields for "Email Address" and "Password", and a "Forgot" link. At the bottom of the page is a banner for "Shop Without Sharing Your Financial Information" with the text "PayPal. Privacy is built in." and a "Learn more" link.

# **The Law on the Retention of Telecommunication data for the investigation of serious offences, L. 183(I)/2007**

- This Law forces the ISPs to store telecommunication and traffic data (ip addresses, calling numbers and emails) for the purpose of investigation for the period of six months
- The police is able to access these data (court warrant) during the investigation of serious crimes that are punishable by the given legislation with imprisonment more than 5 years

## **Law on the protection of the privacy of the communication and access to written communication content, Law 92(i)/1996 and 216(i)/2015**

- No possibility of tampering with private communication up until now
- Possibility to access written communication content (emails, chats etc)
- The police is able to access these data (court warrant) during the investigation of serious crimes as described within the article 17b of the constitution of the Republic of Cyprus (murder, trafficking of humans beings, child pornography, drugs and corruption)

# Cybercrime Legislation-Acts unique to information systems, in particular those related to cyber attacks

- Illegal **access** to a computer system L. 22(III)/2004, article 4
- Illegal **interception** of computer data L. 22(III)/2004, article 5
- Illegal **data interference** L. 22(III)/2004, article 6
- Illegal **system interference** L. 22(III)/2004, article 7
- Misuse of devices L. 22(III)/2004, article 8 (Malware)
- Computer related **forgery** L. 22(III)/2004, article 9



# **Cybercrime Legislation-Acts unique to information systems, in particular those related to cyber attacks**

- **Illegal data interference L. 147(I)/2015, article 5**

Whoever intentionally and without right destroys, deletes, alters or conceals computer data or interrupt the access to such data commits an offense punishable with imprisonment not exceeding five years or a fine not exceeding 34,172 euro or by both penalties.

# Office for Combating Cyber Crime

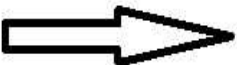

## **Activities/Cooperation(cont.)**


- Participation to Europol EC3:  
F.P Twins, Cyborg and Terminal 24/7 service
- Participation to EMPACTS  
Child Sexual Exploitation (CSE) and Cyber Attacks
- Europol Malware Analysis (EMAS)
- Cooperation with O.C.E.C.P.R (Cyber security strategy)
- Active member of EUROPOL, INTERPOL, EUROJUST, FBI
- ECTEG (European Cybercrime Training and Education Group)
- Also O.C.C is in close cooperation with
  - ENISA (European Union Agency for Network and Information Security)
  - CEPOL
  - CERT EU
  - European Commission
  - VCACITF (Violent Crimes Against Children International Task Force)
  - Council of Europe (T-CY)

# Reporting

The screenshot shows the Cyprus Police website (www.police.gov.cy) with the following elements:

- Header:** "ΑΣΤΥΝΟΜΙΑ ΚΥΠΡΟΥ" (Cyprus Police) with navigation links for "Κινηματογραφικό Αρχείο", "Φωτογραφικό Αρχείο", "Έντυπα και Αιτήσεις", "Εκστρατείες", and "Εκδηλώσεις & Διαλέξεις".
- Left Sidebar:** A menu with categories such as "Αστυνομία Κύπρου", "Ενημέρωση", "Αναζητούμενα και Καταζητούμενα Πρόσωπα", "Κλοπιμαία/Αναζητούμενα Οχήματα", "Κλοπιμαίες Πινακίδες Εγγραφής", "Προσλήψεις", "Προσφορές", "Τμήματα/Υπηρεσίες", "Μονάδες", "Διευθύνσεις", "Αστυνομικές Διευθύνσεις Επαρχιών", "Χρήσιμα Τηλέφωνα", "Ηλεκτρονικές Διευθύνσεις", "Στατιστικά Στοιχεία", "Κώδικας Αστυνομικής Δεοντολογίας", "Χάρτης Δικαιωμάτων του Πολίτη", "Έντυπα και Αιτήσεις", "Ετήσια Έκθεση της Αστυνομίας", "Ενημερωτικό/Διαφωτιστικό Υλικό", "Αστυνομικοί Σύνδεσμοι & Οργανώσεις", and "Μουσείο Αστυνομίας".
- Main Content Area:**
  - Section: "Καλώς Ήλθατε στο Διαδικτυακό μας Τόπο"
  - Advertisement for the "Αστυνομία Κύπρου" mobile app, available on Google Play and the App Store, with a QR code for download.
  - Section: "Δελτία Τύπου" (Press Releases) with a list of recent news items:
    - 22/11/2016 Δελτίο Τύπου 2 - Ληστεία
    - 22/11/2016 Δελτίο Τύπου 1- Φωτιά σε αμαξώματα αυτοκινήτων
    - 21/11/2016 Δελτίο Τύπου 5 - Σύλληψη - Προσωποκράτηση 24χρονου Φέρεται να ενέχεται σε 5 υποθέσεις διαρρήξεων και κλοπών
    - 21/11/2016 Δελτίο Τύπου 4 - Ποινική καταδίκη 8 χρόνων για ανθρωποκτονία
    - 21/11/2016 Δελτίο Τύπου 3 - Συνομοσία προς διάπραξη κακούργηματος και πλημμελήματος, παράνομη κατοχή και μεταφορά πυροβόλου όπλου, οπλοφορία προς διέγερση τρόμου, πρόκληση
- Right Sidebar:**
  - Social media links for Facebook and Twitter.
  - Section: "Ομιλίες Αρχηγού Chief Speeches"
  - Section: "Εξώδικα Τροχαίας Εντάλματα Προστίμων"
  - Section: "Καταχώρηση Καταγγελιών/Πληροφοριών Cyber Crime για ηλεκτρονικό έγκλημα" (highlighted with a red circle)
  - Section: "Γραφείο Χειρισμού Θεμάτων Ιδιωτικών Υπηρεσιών Ασφαλείας"
  - Section: "Συγκροματοδοτούμενα"

Πρόσωπα	Κατηγορία Παραπονού *	Παρακαλώ Επιλέξτε
Κλοπιμαία/Αναζητούμενα Οχήματα		Παρακαλώ Επιλέξτε Παιδική Πορνογραφία Παράνομη Επέμβαση (Hacking)/Παρέμβαση σε δεδομένα Η/Υ Απάτη μέσω Διαδικτύου Ξενοφοβία/Ρατσισμός
Κλοπιμαίες Πινακίδες Εγγραφής		Περιγραφή Παραπόνου /Πληροφορίας*
Προσλήψεις		
Προσφορές		
+ Τμήματα/Υπηρεσίες		
+ Μονάδες		
+ Διευθύνσεις		
+ Αστυνομικές Διευθύνσεις Επαρχιών	URL / Σύνδεσμος	
Χρήσιμα Τηλέφωνα	Όνομα *	
Ηλεκτρονικές Διευθύνσεις	Επώνυμο *	
Στατιστικά Στοιχεία	Ηλικία	
Κώδικας Αστυνομικής Δεοντολογίας	Δελτίο Ταυτότητας	
Χάρτης Δικαιωμάτων του Πολίτη	Χώρα Έκδοσης Δελτίου Ταυτότητας	CYP - ΚΥΠΡΟΣ
Έντυπα και Αιτήσεις	Αριθμός Εγγραφής Αλλοδαπού	
Ετήσια Έκθεση της Αστυνομίας	Διαβατήριο	
Αστυνομική Ανασκόπηση	Χώρα Έκδοσης Διαβατηρίου	Παρακαλώ Επιλέξτε
Ενημερωτικό/Διαφωτιστικό Υλικό	Διεύθυνση	
Αστυνομικοί Σύνδεσμοι & Οργανώσεις	Επάγγελμα	
Μουσείο Αστυνομίας	Σταθερό Τηλέφωνο	
	Κινητό Τηλέφωνο	
	Ηλεκτρονική Διεύθυνση (email)	
	IP Address	



# Mobile Application



28/11/2016

Γραφείο Καταπολέμησης Ηλεκτρονικού Εγκλήματος



Constantinos Anastasiou  
Police Officer  
Digital Forensic Laboratory  
C.E.E.C.S  
BSc Computer Science  
MSc Business Administration  
[canastasiou@police.gov.cy](mailto:canastasiou@police.gov.cy)  
Tel. 22808988  
Fax. 22808465