PUBLIC MINISTRY
Prosecutor's Office attached to the High Court of Justice

Directorate for the Investigation of Organized Crime and Terrorism (D.I.O.C.T)

Service for Countering Cyber Criminality (CC.U)

Ioana Albani, chief prosecutor
www.diicot.ro

D.I.O.C.T – CC.U

Typology of crime

- Collecting of confidential data – phishing/vishing (credit card information, online banking, usernames, passwords etc.)
- Fraudulent computer auctions-selling (computer forgery, escrow fraud, use of fake documents/identity, blind mules or affiliated to the network etc.)
- Unauthorized access to computer systems/ illegal interception of computer communications
- VoIP fraud (PBX attacks)
- ATM manipulation (skimming)
- Forgery of electronic payment instruments/fraudulent withdrawals

D.I.O.C.T – CC.U

Objective & subjective factors that have favoured proliferation of Cybercrime

- Increasingly and wide access to fast/modern equipment/connections
- Anonymous connections
- Difficulties in cooperation with service providers, cyber cafés, university campus networks or small networks;
- The relative easiness with which one is able to carry out some of the acts specific of Cybercrime;
- The delay in the response by the authorities,
- Lack of predictability in prosecution and also within courts procedures
- Migration of some organized criminal groups to cyber crime
- Freedom of movement
- Maximum profits at lower costs

D.I.O.C.T – CC.U

Common evidence vs electronic evidence

General definition on evidence any factual element that serves :

- to establish the existence or non existence of a crime;
- to identify the perpetrator and to know the necessary circumstances for a just solution

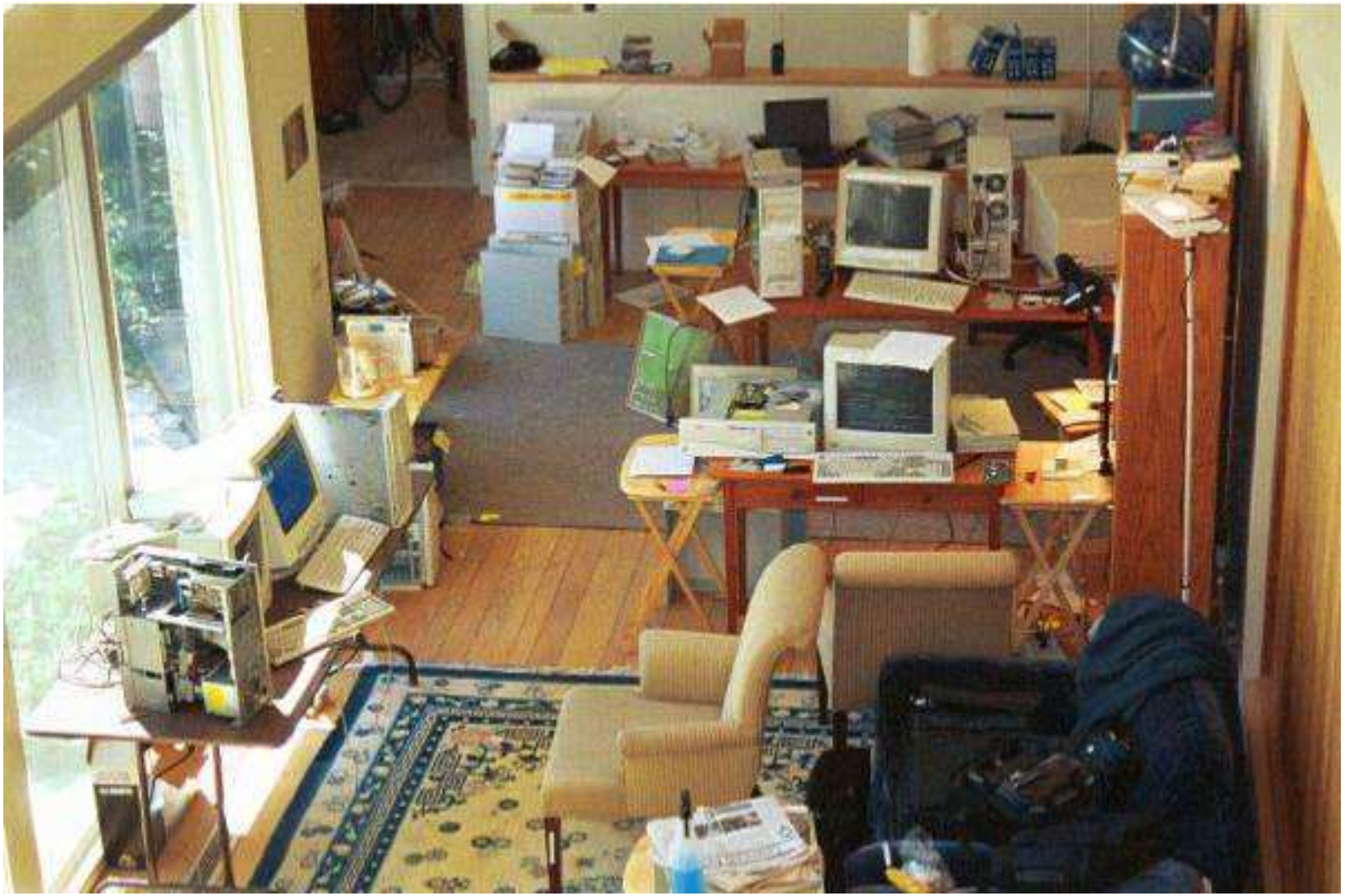
Electronic evidence = any factual element **created or revealed in a digital environment** that serves :

- to establish the existence or non existence of a crime;
- to identify the perpetrator and to know the necessary circumstances for a just solution

Computers create evidence as well as they can record or produce evidence: files content; meta data; system files; logging data; backup files; deleted files; recovered files

Conditions for admissibility :

- » To be pertinent
- » Conclusive
- » Utility for the case
- » Not forbidden by the law



Case I

D.I.O.C.T – CC.U

Notification/complaint – FBI Legal attaché

Victim – Discover, 20 pharmacies, Brandi Inc.

Offence 1 – illegal access to computer systems, illegal interception of computer communication, illegal operation with credit card data

Offence 2 – money laundering, organized crime

Description of facts

- A fraudulent scheme involving compromised computers at retail pharmacies with the purpose of stealing credit card information
- Maintenance common software products used at each pharmacy, service LogMeIn, to allow remote access to POS machines located in the pharmacies
- The computer systems at the pharmacies were compromised by malware
- Fortunately - log created, thus the analysis revealed IP address, user account created

D.I.O.C.T – CC.U

Information provided by US authorities

- affidavit /case agent FBI Chicago
- evidence collected in US under subpoena, legal documents, logs for email addresses, forensic analysis, financial analysis/WU transfers

Track back the facts

Malicious software update scheme/phishing /successful

Account created on a compromised computer: gestapo09@gmail.com

Traceable IP 89.42.137.9 – Skynet Telecom network , Bucharest

Hi5 profile *pictures, car plate led to the offender/nicknames

FTP server identified / information collected – HTML files provided by a Keylogger software/credit card information, logs

Other email accounts and logs : **grimvm@yahoo.com; bastardvm@yahoo.com**

ICQ account by the name of the offender

AOL account by the name of Grim

D.I.O.C.T – CC.U

IP address verification led to several ISPs:

- RDS&RCS, Constanta
- UPC Romania, Bucharest , Blvd. Banu Manta
- Bucharest, G-ral Vladoianu (rented apartment girlfriend)
- Wireless network (neigh borough)
- Zapp modems (anonymous)

Forensic analysis on compromised computers

- Forensic company/Cybertrust
- Carnegie Mellon CERT / alg.exe and update9823.exe

KEYLOGGER ANALYSIS

D.I.O.C.T – CC.U

- **Name given by the offender: “Grim Keylogger added PWS”**
- **What it can do:**
  - **Firewall Bypass**
  - Persistence Option (Impossible to Remove)
  - **Colored HTML Log**
  - Works on Non admin Accounts
  - 2 FTP Servers Support
  - Passive mode for FTP Upload (works behind routers and LANs)
  - Organized FTP Upload (Dir for Each User , Logs Sorted with Date and time)
  - When the Keylogger starts , it Checks for Internet Connection and try to send the current Log directly , then after that it sleeps the number of hour chosen in the editor and send when the time passes
  - Should be Undetected by 90 % of avs
- **Customization:**

KEYLOGGER ACTIVITY

- **Server.exe** :
  - Changes Windows Registry
  - Creates the following files on the computer:
    - C:\Documents and Settings\user\Application **Data\windows\alg.exe (adds an Win Reg Key "alg.exe")**
    - C:\Documents and Settings\user\Application Data\windows\gp2007.dll
    - C:\Documents and Settings\user\Application Data\windows\sql2005.dll
    - C:\Documents and Settings\user\Application Data\ tmp6sfsa.sql **(contains HTML logs)**
    - C:\Documents and Settings\user\Application Data\ **ppx123.txt (contains passwords)**
    - C:\WINDOWS\uninstall\rundl132.exe (imitates OS "rundll32.exe")
  - Accesses Windows Functions: WriteFile , CreateFileA , GetTempPathA;
  - Once executed it initiates a connection **to www.google.com using port 80 and also to IP : 200.115.173.65 using FTP port 21 ;**

Panama FTP Server

D.I.O.C.T – CC.U

host-200-115-173-65.ccipanama.com (200.115.173.65

200.115.173.0 - 200.115.173.255
Cyber Cast International, S.A.
Addison House Plaza Suite 20, 507, 264-0852
6-3783 - Panama - PA
Panama
Brazil
+507 264-0852 []
Created on 19-11-2008
Last updated on 19-11-2008

Cyber Cast International, S.A.
info@CCIPANAMA.COM
Addison House Plaza Suite 20, 507, 264-0852
6-3783 - panama - pa
Panama
Brazil
+507 264-0852 []
Created on 05-04-2005
Last updated on 23-09-2008

Please wait while you are redirected to the gateway you chose to make payment...

Loading

Western Union Transfer Instructions:

Send the Western Union to:
Receiver First Name: Jorge
Receiver Last Name: Moreno
Receiver Country: Panama
Receiver City: Panama
Receiver Province: Panama

When the transfer is completed send us an email to billing@offshore-web-hosts.com with the following information:
- Sender's Name
- Sender's Country
- Total Amount Sent
- Your 10 digit Western Union order number

Intercepted email

D.I.O.C.T – CC.U

tuesday, march 17, 2009 6:08 am
from:
"billing@offshore-web-hosts.com" <billing@offshore-web-hosts.com>
add sender to contacts
to:
grimvm@yahoo.com
dear client,

regarding western union

please make the payment to:

receiver first name: jorge
receiver last name: moreno
receiver country: panama
receiver city: panama
receiver province: panama

when the payment has been done please send us an email to billing@offshore-web-hosts.com with the following information:

- full name
- address
- amount of your transaction. $
- your 10 digit western union order number.

if you need any further information, feel free to contact us. is always a pleasure to assist you.
thank you to trust cyber cast international.
best regards,

elisa vado
billing department
cyber cast intl
panama, panama

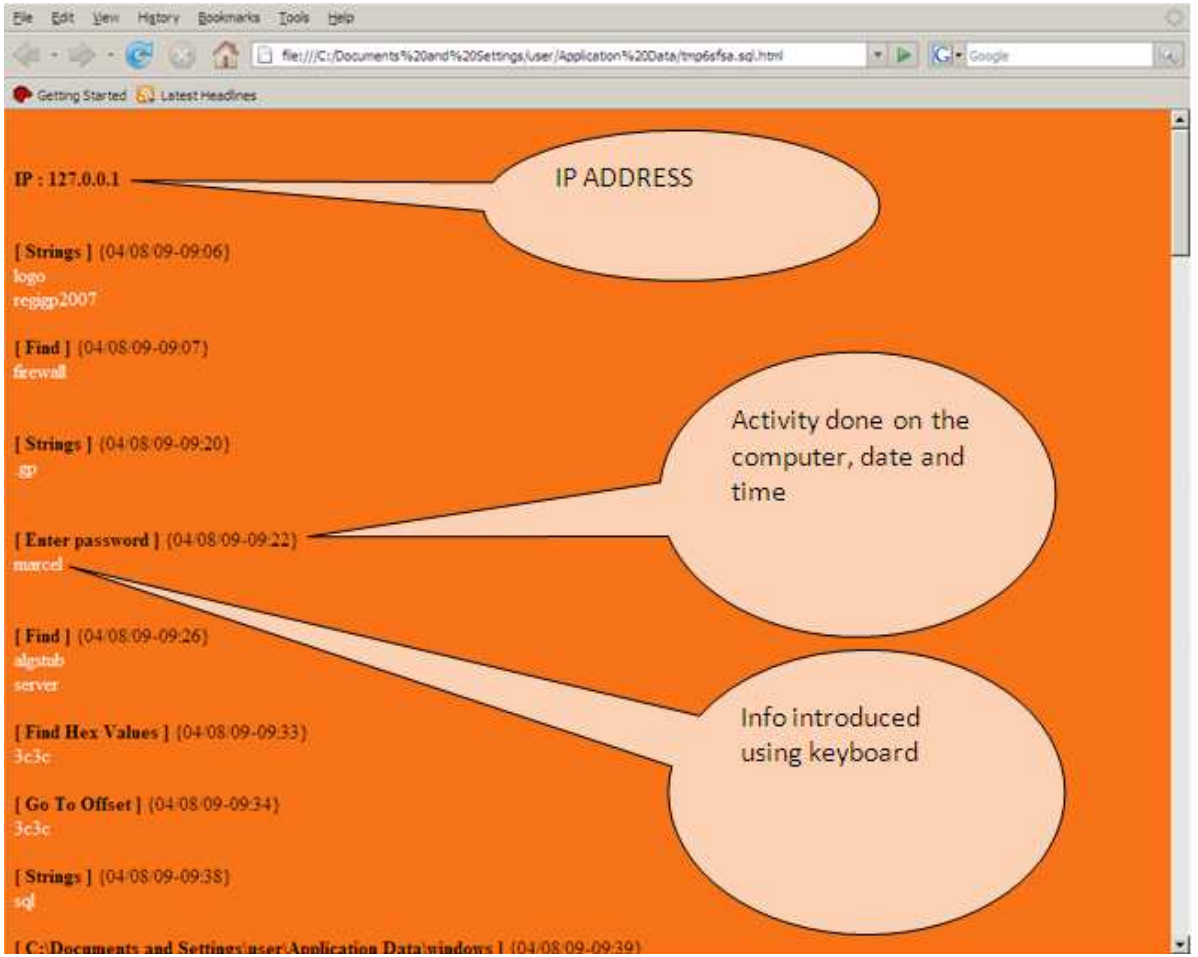
---
email: billing@offshore-web-hosts.com
phone: +507 264-0852
fax: +507 264-2978

ticket details

ticket id: pmp-704832
department: billing
priority: low
status: closed

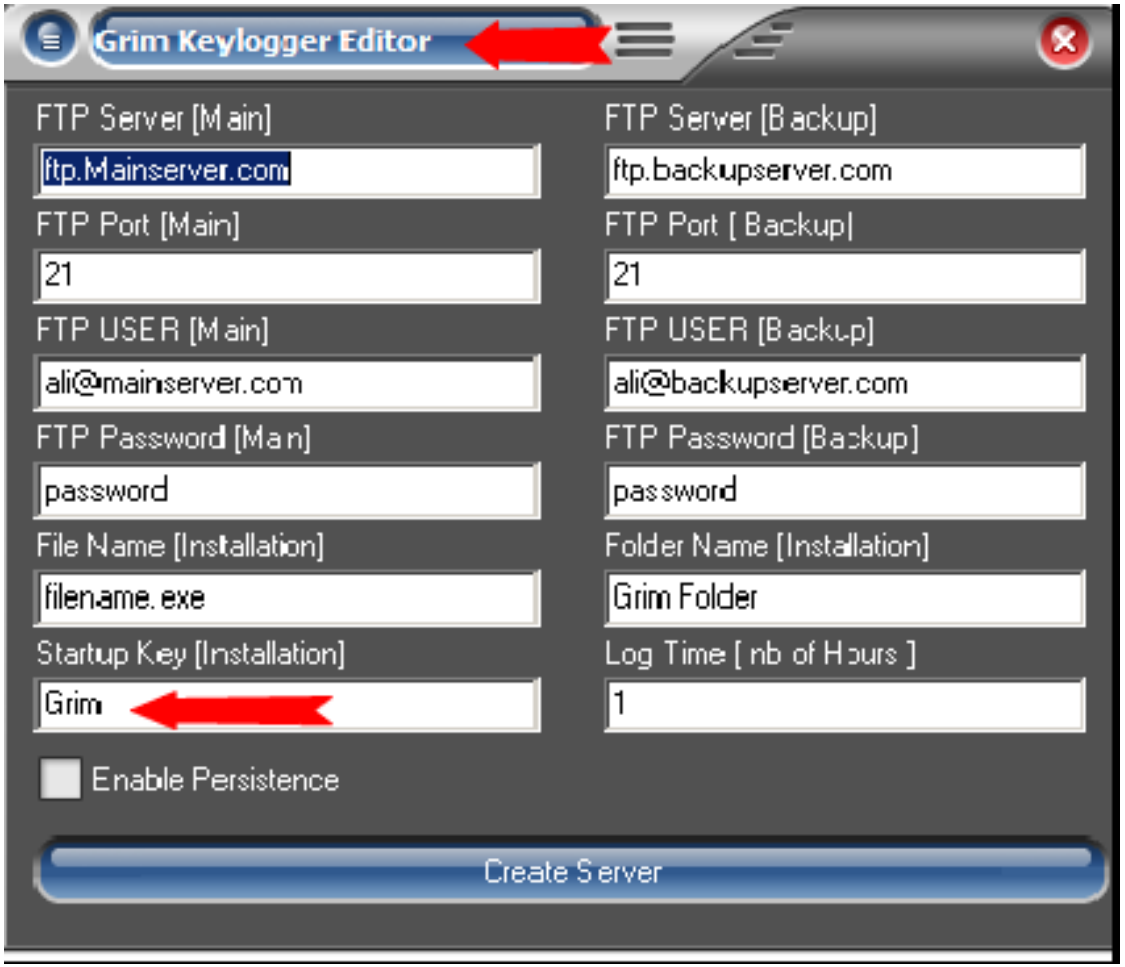
COLORED HTML LOG

D.I.O.C.T – CC.U



GRIM KEYLOGGER EDITOR

D.I.O.C.T – CC.U



Internet/Phone Intercepts

D.I.O.C.T – CC.U

- Phones used to comunicate with individuals from USA and Bulgaria
- Emails addresses used by RE to comunicate with individuals from USA, Bulgaria and Romania :
  - **gestapo09@gmail.com**
  - **bastardvm@yahoo.com**
  - **grimvm@yahoo.com**
- WebMoney nr. on **www.trainexservice.com** : WMZ: Z188516
- WebMoney nr. on **www.wmtransfer.com** : WMId 998970028670

Search warrants
Forensics on RE computers

D.I.O.C.T – CC.U

- **Identified:**
  - Keylogger HTML logs containing CC data from pharmacies;
  - Keylogger installation kit
  - References to maintenance software
  - References to IP's used in the illegal access;
  - 43786 unique credit card numbers (VISA, MASTERCARD, DISCOVER , AMERICAN EXPRESS);
    - 3957 reported to have been compromised.
    - WU transfers from

Financial investigation

D.I.O.C.T – CC.U

- WU documents for receiving money corroborated with the information obtained from intercepts and computer forensic (around 200.000 USD within one year)
- Web money transactions couldn't be verified
- Parallel investigation in the US on the persons identified in fraudulent transaction with forged credit cards
- 120.000 USD seized on the house search
- Investigation on legal subsistence (the offenders/no job and their family, estate, other goods/cars)
- No match between the personal legal earnings and the expenditure

Indictment I/conviction
September 2010

D.I.O.C.T – CC.U

RE and one of his accomplices (CE) have been indicted and then convicted for committing :

- Illegal access to a computer system (aggravated)
- Illegal interception of computer data (aggravated)
- Misuse of device
- Fraudulent operation with credit cards data
- Money laundering

Total - RE imprisonment 4 years and 6 months

- CE (accomplice) suspended sentence

- **No sufficient evidence to indict other accomplices** (preventive measures on MC – not to leave the country by the end of the investigation)
- **Spontaneous release of information regarding the US participants**

D.I.O.C.T – CC.U

THANK YOU FOR YOUR ATTENTION

Ioana Albani

Chief prosecutor

Head of the Cybercrime Unit

Directorate for the Investigation of Organized Crime and Terrorism

Prosecutor's Office attached to the High Court of Justice

Phone/fax 0040 21 319 39 30

Mobile 0040 742 923 585

i_albani@yahoo.com

albani_ioana@mpublic.ro