Responses to the challenge of cybercrime

Experience of Romania
Directorate for Investigating Organized Crime and Terrorism

Tunis
22 MARCH 2018

GENERAL VIEW

- ✓ **Acknowledgement and necessity of countering organized crime phenomenon**

- ✓ **Harmonization of the Romanian legislation**
  - 2000 Romania signed UNTC; ratification 2002;
  - 2001 Romania signed the CCC; 2004 ratification;
  - 2000 Law on Trafficking in Drugs;
  - 2001 Law on Trafficking in Human Beings;
  - 2002 Law on Combating Money Laundering;
  - 2003 Law on Cybercrime (substantive and procedural provisions);
  - 2003 Law on Combating Organized Crime.

- ✓ **Creating specialized structures in countering organized crime**
  - **DIICOT**- Directorate for Investigating Organized Crime and Terrorism
  - **DCCO** – Directorate for Combating Organized Crime

- ✓ **DIICOT** was set up in 2004 by Law No. 508/2004 and by EGO no.78/2016 is functioning with a new operational structure
  - is the only structure within the Public Ministry specialized in investigating and countering terrorism and aggravated offences with organized crime
  - has a national wide **structure** and **jurisdiction**
  - has a special legal status, budget that includes special funds for undercover operations
  - has special regulation on organization and functioning

LEGAL COMPETENCES – Art.11 of EGO no.78/2016

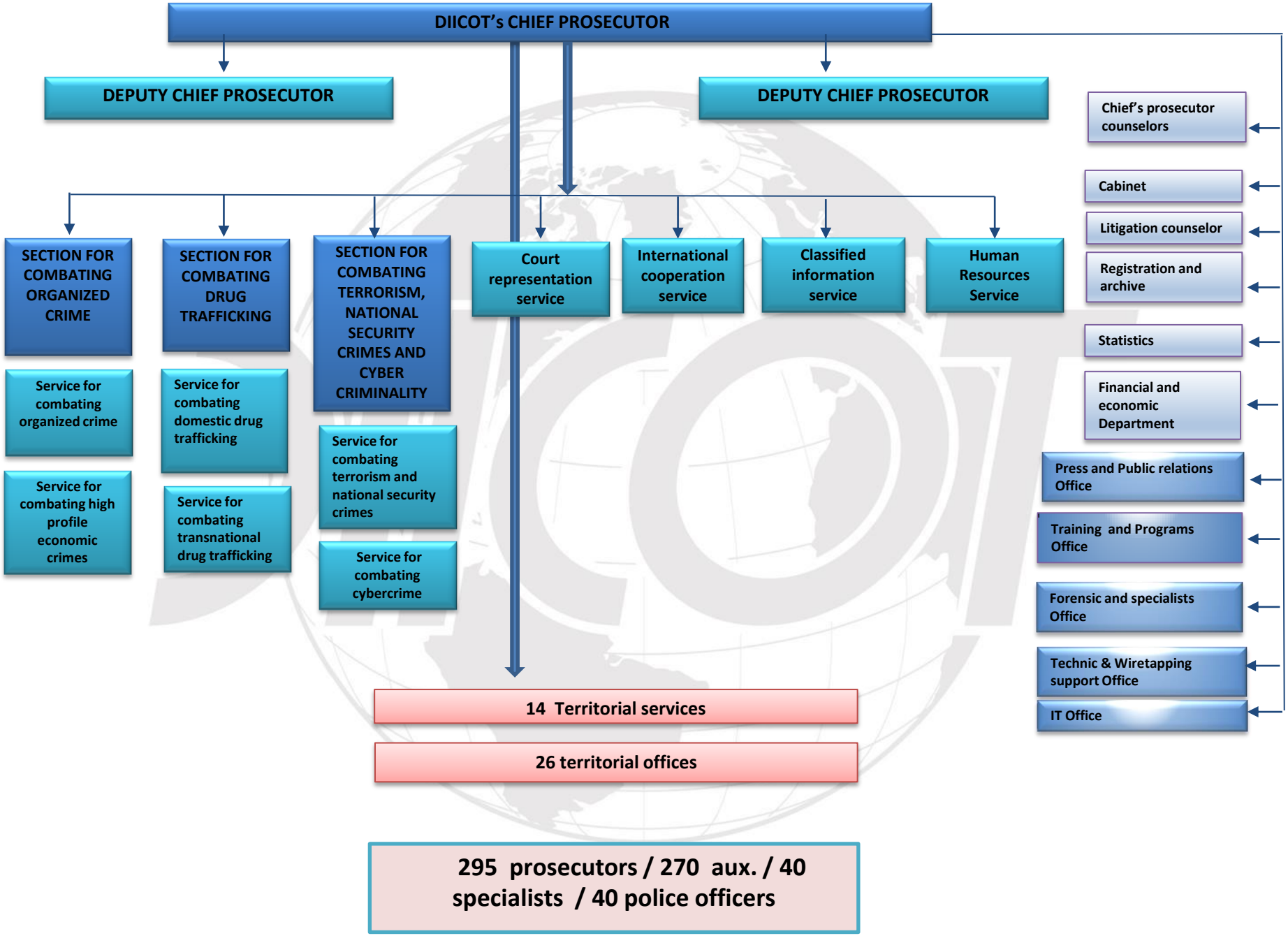
The following offences, either they are committed within an organized criminal group or not:

- Crimes against computer systems and data;
- Child pornography;
- Drugs trafficking;
- Offences against the legal regime of drug precursors;
- Offenses against national security;
- Terrorism and financing of terrorism;
- Trafficking in human beings

The following offences, only if they are committed within an organized criminal group:

- Homicide, aggravated homicide;
- Blackmail;
- Illegal depravation of freedom;
- Theft, aggravated theft, robbery, piracy;
- Bankruptcy fraud;
- Usury
- Fraudulent management;
- Diversion of public tenders;
- Embezzlement;
- Computer fraud;
- Fraudulent financial operations;
- Counterfeiting of currency, electronic payment instruments;
- Trafficking in toxic products or substances
- Tax evasion, contraband

Money laundering if the proceeds are obtained by one of the above mentioned crime


DIICOT's CHIEF PROSECUTOR
DEPUTY CHIEF PROSECUTOR
DEPUTY CHIEF PROSECUTOR
Chief's prosecutor counselors
Cabinet
Litigation counselor
Registration and archive
Statistics
Financial and economic Department
Press and Public relations Office
Training and Programs Office
Forensic and specialists Office
Technic & Wiretapping support Office
IT Office
SECTION FOR COMBATING ORGANIZED CRIME
SECTION FOR COMBATING DRUG TRAFFICKING
SECTION FOR COMBATING TERRORISM, NATIONAL SECURITY CRIMES AND CYBER CRIMINALITY
Court representation service
International cooperation service
Classified information service
Human Resources Service
Service for combating organized crime
Service for combating high profile economic crimes
Service for combating domestic drug trafficking
Service for combating transnational drug trafficking
Service for combating terrorism and national security crimes
Service for combating cybercrime
14 Territorial services
26 territorial offices
295 prosecutors / 270 aux. / 40 specialists / 40 police officers

Specific Material Means of Evidence (computer systems, data storage of any kind, phones, tablets, iPads etc.)

Art.35 para. (1) Law no.161/2003
lett. a – computer system means any device or assembly of interconnected devices or that are in a operational relation, out of which one or more provide the automatic data processing by means of a computer program;

Art.138 para.4 CPC
A computer system is any device or combination of devices interconnected between them or in a functional relationship, one or more of which provide the automatic data processing by means of a computer program.

Art.181 para.1 CC
Computer systems mean any device or group of (functionally) interconnected devices, where one or several of such systems ensure automatic processing of data, using a computer program.

Computer data
is not obviously readable to humans
It is volatile,
easy to altering, tempering, destroying and it is original

Computer systems create/store/ produce evidence in reference to:

Content – documents, images, sounds

Metadata – data related to data (not immediately visible)

Configuration data /settings – shows the way a system is functioning

Logs – data created by applications or by the operating system that can be used to reconstruct an event (history, events, recent files etc.)

Traffic data – computer data related to a communication through a computer system, representing a part of the communication chain, indicating the communication origin, destination, route, time, date, size, volume and duration, as well as the type of service used for communication;

Special means of collecting digital evidence

- Surveillance or special investigation methods, article 138 CPC (Art.20 of CCC)
- Computer search, article 168 CPC (Art.19 of CCC)
- Preservation of computer data, article 154 CPC (Art.16-17 of CCC)
- Production order, art.152 CPC, art.170 CPC (Art.18)
- Undercover operations, article 149 CPC
- Authorized activities, article 150 CPC

Surveillance or special investigation methods, article 138 CPC

(1) The following are surveillance or investigation special methods:

a) wiretapping of communications or of any type of remote communication;

b) accessing a computer system;

c) video, audio or photo surveillance;

d) tracking or tracing with the use of technical devices;

e) obtaining data regarding the financial transactions of individuals;

....

(2) Wiretapping of communications or of any type of messages designates the wiretapping, accessing, monitoring, collection or recording of communications via phone, computer system or any other communication device.

(3) Accessing a computer system designates the penetration of a computer system or of other data storage device either directly or from a distance, through specialized programs or through a network, for the purpose of identifying evidence.

(4) A computer system is any device or combination of devices interconnected between them or in a functional relationship, one or more of which provide the automatic data processing by means of a computer program.

(5) Computer data is any representation of facts, information or concepts in a form appropriated for processing in a computer system, including a program able to determine the performance of a function by a computer system.

Conditions, Article 139 CPC:

- there is a **reasonable suspicion** in relation to the preparation or commission of one of the serious offenses listed;
- such measure is **proportional** to the restriction of fundamental rights and freedoms, considering the particularities of the case, the importance of information or evidence that are to be obtained or the seriousness of the offense;
- **evidence could not be** obtained in any other way or its obtaining implies special difficulties that would jeopardize the investigation, or there is a threat for the safety of persons or of valuable goods;
- list of serious crime.

Issuing authority: court order/mandate (the judge for rights and liberties)

Exception provided by Article 141 CPC: in **urgent** cases and only in cases of the crimes listed in Article 139 paragraph 2 the prosecutor may order for a 48 hours period the interception of any communication or the access to a computer system.

Duration: The mandate is given for 30 days at the most, with the extension possibility under the same conditions, for dully justified reasons, each extension not exceeding 30 days. The maximum duration of these measures is 6 months

Obligation to inform: the prosecutor is obliged to give advice, in writing, to the persons against whom the measures were taken until the end of the criminal investigation

The production order

The production order may differ according to the data sought.

Obtaining traffic and location data processed by providers of public electronic communications networks or providers of electronic communication services intended for the public, other than the content of communications, and stored by these, article 152 CPC - court order

Surrender of objects, documents or computer data, article 170 CPC/Forced seizure of objects and documents, article 171 CPC – prosecutor's order

Conditions:

- reasonable suspicion in relation to the preparation or commission of an offense;
- reasons to believe that an object or document can serve as evidence in a case;
- the criminal investigation bodies or the court may order a person or legal entity holding them to provide and surrender them.

Or

- criminal investigation bodies or the court may order:
  - any person or legal entity to communicate specific computer data in their possession or under their control;
  - any provider of public electronic communication networks or provider of electronic communication services specific data referring to **subscribers, users and to the provided services** that is in its possession or under its control, other than the content of communications and then those specified by Art. 138 para. (1) item j).

Preservation of computer data, article 154 of RCPC

If there is a **reasonable suspicion** in relation to the preparation or commission of an offense, for the purpose of **collecting evidence** or of **identifying a perpetrator**, suspect or defendant, the prosecutor may order **immediate preservation of computer data, including of data referring to traffic data**, that were stored by means of a computer system and that is in the possession or under the control of a provider of public electronic communication networks or of a provider of electronic communication services intended for the public, in the event that there is a **danger that such data may be lost or altered.**

Conditions:

- justified cases; preparation or the performance of an offence;
- purpose of gathering evidence or identifying the perpetrators;
- object : computer data or the data referring to the traffic; data endangered of destruction or alteration

Issuing authority: prosecutor's order

Period: no longer than 60 days and can be exceeded, only once, no more than 30 days.

Partial disclosure: allowed

Disclosure: court order for retrieval of the preserved data.

Obligation to inform: by the end of the investigation

Computer search, article 168 CPC

represents the technical **procedure aiming to investigate, discover, identify and collect evidence** stored in a computer system or in a computer data storage medium, performed by means of adequate technical devices and procedures, of nature to ensure the integrity of the information contained by these.

Conditions:

- the necessity to investigate a computer system or a computer data storage device;
- the purpose of discovering or gathering evidence.

Issuing authority: court order

Retaining copies: mandatory

The search from the starting point: allowed

Usually the computer search is conducted after the house search, which means the identification of the devices to be searched is certain.

General consideration on Cybercrime in Romania

- Criminals rapidly had found and exploited the technological development and freedom of movement, engaging their resources to transfer knowledge and to commit crimes borderless;

- The migration of organized criminal groups to Cybercrime it is considered the most significant fact that created, starting with 2003, the new design of Cybercrime in Romania

- Moving to an organized character had affected the entire way of investigating and prosecuting Cybercrime

- Criminal enterprise, similar to any lucrative activity is based on concepts of efficiency, in order to obtain maximum profits. Computer crimes and credit card fraud offer maximum profits at low costs.

Difficulties in dealing with Cybercrime

The extraneous element present in 80% of the cases

- offences committed home /results abroad (victims)
- offences committed abroad by Romanian nationals
- offences committed entirely abroad/proceeds of crime transferred or collected in Romania

Consequence

- delay in obtaining /assessing evidence/ e-evidence
- difficulties in incorporating evidence, e-evidence into the national proceedings

The Romanian 24/7 Contact Point was established by art.62 Law no.161/2003 (the Service for Combating Cyber Criminality)

- **provides specialized assistance** and offers data on the Romanian legislation in the domain;
- **disposes the expeditious preservation of data** as well as the seizure of the objects containing computer data or the data regarding the data traffic required by a competent foreign authority;
- **executes or facilitates the execution** of letters rogatory in cases of cyber-crime fighting, cooperating with all the competent Romanian authorities.

Service for Combating Cyber Criminality have also national-wide investigative jurisdiction on cyber crime cases and works directly with the **International Judicial Assistance Office,** that was created with the purpose of enabling the mutual legal assistance regarding the investigations of crimes falling under the Directorate' jurisdiction, ensuring as well the data and information exchange.

In fact the 24/7 Contact point is :

An intermediary to the investigative national authorities and similar ones abroad with the purpose of securing evidence, especially e-evidence.

Important role in preservation powers of traffic and computer data (incoming/outgoing internationally).

- **subscriber information (90%);**
- **content (10%).**

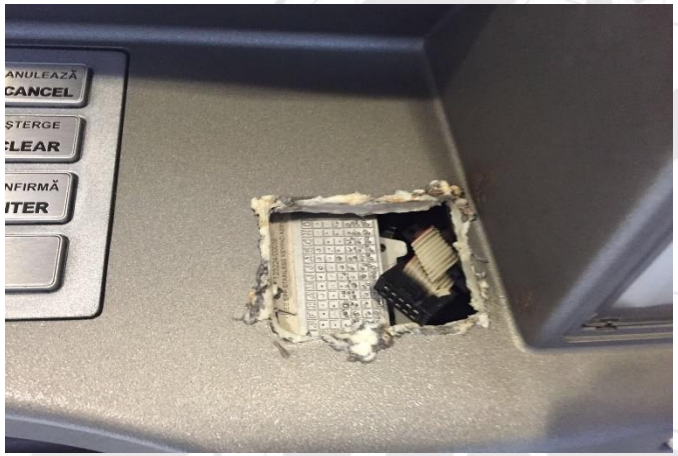
An advisor to the investigative national authorities and similar ones abroad on effective measures for obtaining e-evidence or their effectiveness.

Requested authority for complex cybercrime requests as investigative unit.

contact: cybercrime@mpublic.ro

CASE STUDY I

- **Notification from a bank (04.07.2016)**
  - 2 ATMs (24h) vandalized (02.07)
  - Money withdraw



Thermal cutting of some portions of the mask (front) of the ATMs (keyboard proximity)

Disconnecting of some internal devices/ disrupting functions of the ATMs

Connection with the computer system inside/ data overriding

Set of commands to dispense the money

10.995 RON (2.500 EURO) and **236.800 RON (50.050 EURO)**

I. Investigation:

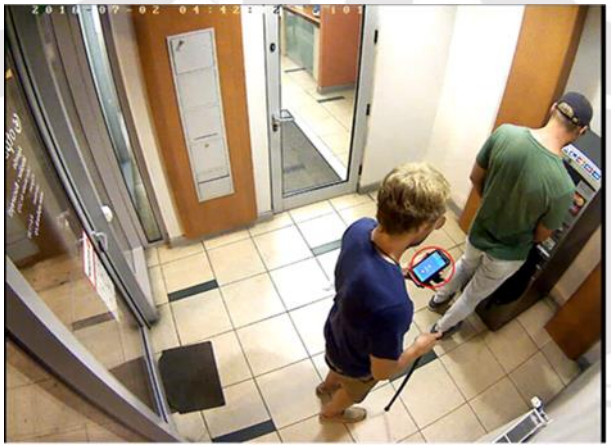
Identification of the mobile terminals used at the time and locations *GPS* of the ATMs attacked:

2 terminals identified (IMEI and SIMs)

iPhone and Lenovo matching with the imagines retrieved from the ATMs (04.07)

Call records analyzed – tracking the suspects from the airport to the location of the ATMs and other places in Bucharest and back to the airport (05.07)

Matching time/imagines/flight records = identity of the attackers



II. Investigation

- Wire tapping on the 2 mobile terminals (RO SIMs & IMEI);
- Airport notification

Positive match after 2 weeks !!!

same suspects – technical tracking showed travel to Ploiesti

Physical surveillance

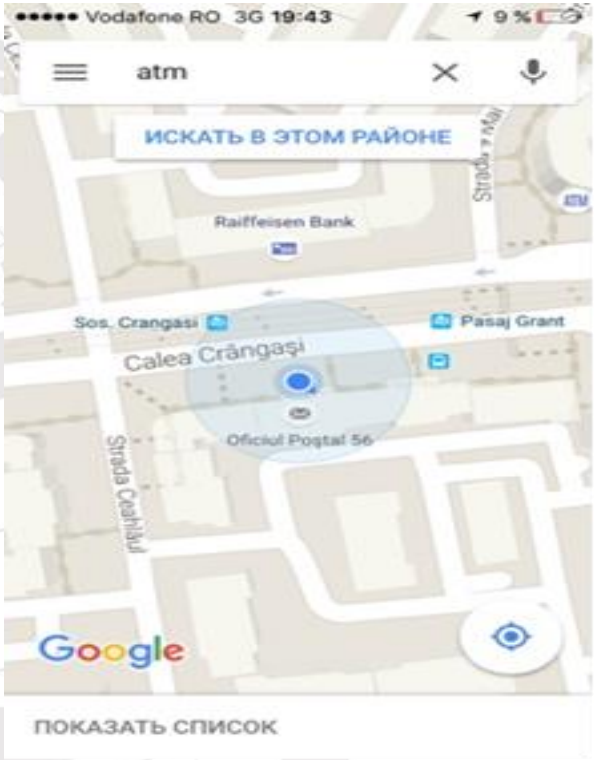
III. Investigation:

House search – hotel room:

- mobile terminals used on 02.07
- Flight tickets
- Tools used
- Clothing

Computer/mobile terminals search:

- Saved location of one of the ATMs attacked
- Pictures
- Call records with Germany and Russia



INDICTMENT (2016)

Article 360 CP – illegal access to computer system
(art.2 of CCC)
Article 363 CP – serious hindering of a computer system
(art.5 of CCC)
Article 249 CP – computer fraud
(art.8 of CCC)
Article 253 CP – destruction

CONVICTION (2017)

2 years and 2 months imprisonment

CASE STUDY II

A bank in Romania receives on 03.09.2016, on one official email, messages apparently coming from an email pertaining to the domain **europa.eu** with the subject **”*Challenges for European banks*”** and the following content:

” Very low interest rates, if sustained over a long period of time, can have cumulative effects on financial intermediation and stability. However, the euro area experience so far has been clearly positive, Executive Board Member Benoit C?ure tells the Yale Financial Crisis Forum.

General public enquiries
For information about the ECB’s activities, please contact us by e-mail or phone
from Monday to Friday between 8:30 and 17:30 CET.

info@ecb.europa.eu&n bsp;
+49 69 1344 1300”

Attachment – rules for European banks.doc

Once the attachment is opened:

- a temporary file is generated **~$e rules for European banks.doc** on the target system;
- **a Trojan** – application Cobalt Strike starts to run on the volatile memory of the target system;
- other temporary files are created in Windows;
- **connection is opening to a C&C server** allowing the perpetrators to run different commands on the target system in order to obtain information about the network and its users;
- **credentials are exfiltrated** followed by a set of commands with the purpose of modifying privileges.

As a consequence:

- within 90 min. **20 computers have been infected** among which 2 systems *C026N11* and *C026ATM3* belonging to the Bank's ATM network;
- **new files downloaded and installed**: crss.exe, d2.exe, d2sleep.exe, sdel.exe, sdelete.exe, wr.exe, xtl.exe with different functions among which: **overriding critical files such as Master Boot Records or legitim predefined commands**;
- **remote connection to ATMs**;
- **run commands to unauthorized dispense of money** from the ATMs infected (31).

CASH-OUT

In the same day between **17:38 – 19:44 si 21:50 – 00:29**
on **31** ATMs in **9** cities
3.818.000 lei (830.000 Euro)

1 perpetrator identified during the cash-out operation
(around **17.300 EURO** delivered)

Evidence used:

Computer search
(bank's computers; perpetrator's mobile terminals)
Call records
Images
Malware analysis and expert opinion

INDICTMENT

Art.367 CP – organized crime group

Art.249 CP - computer fraud (art.8 of CCC)

CONVICTION (2017)

4 years and 10 months imprisonment

The investigation continues against other aprox.60 persons who haven't been identified yet

Article 360 CP – illegal access to computer system (art.2 of CCC)

Article 362 CP – computer data interference, alteration of computer data (art.4 of CCC)

Article 363 CP – serious hindering of a computer system (art.5 of CCC)

Article 249 CP – computer fraud (art.8 of CCC)

QUESTIONS ?

THANK YOU !

Ioana Albani

Deputy chief prosecutor of DIICOT

albani_ioana@mpublic.ro

www.diicot.ro