



BANCHE E SICUREZZA 2016 - Milan, ITALY - 27/06/2016

**ENHANCING  
CYBER  
SECURITY**

**ENCYSEC**



**Besnik LIMAJ**  
Team Leader

A large red circle with a black outline, containing the text "PROJECT SYNOPSIS" in white, bold, uppercase letters.

**PROJECT  
SYNOPSIS**

A large black circle with a white outline, containing the number "1" in white, bold, uppercase letters, centered within the circle.

**1**



**PROJECT FUNDED BY:  
EUROPEAN UNION'S INSTRUMENT CONTRIBUTING TO  
STABILITY AND PEACE**

**Total Budget:  
1.48 Million Euros**

**LAUNCHED:  
JANUARY 2014 - DURATION 24 MONTHS (Extension + 6 Month)**

**PARTNER COUNTRIES:  
FYR of Macedonia,  
Kosovo,  
and Moldova**

**REGIONS:  
East Europe and Western Balkans**

A large red circle with a black outline, containing the text "PROJECTS ACTIVITY AREAS" in white, bold, uppercase letters.

**PROJECTS  
ACTIVITY  
AREAS**

A large black circle with a white outline, containing the number "2" in white, bold, uppercase letters. The circle is set against a teal background.

**2**

# PROJECT COMPONENTS

## COMPONENT 1:

NATIONAL CYBER SECURITY STRATEGY (NCSS):  
AWARENESS RAISING:



## COMPONENT 2:

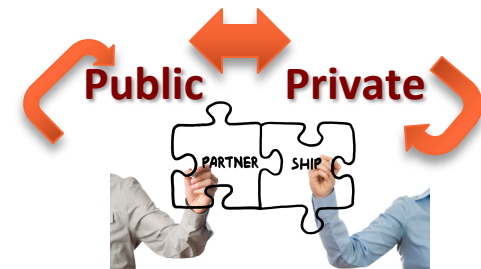
CERT CAPACITY BUILDING:  
FACILITATION OF CYBER EXERCISES:



## COMPONENT 3:


PPP/CIIP:

INTERNATIONAL COOPERATION:





**COUNTRY  
FOCAL  
POINTS**



**3**

# COUNTRY FOCAL POINTS: MACEDONIA

Contacted representatives:

The Cyber Crime Unit

Ministry of Information Society and Administration

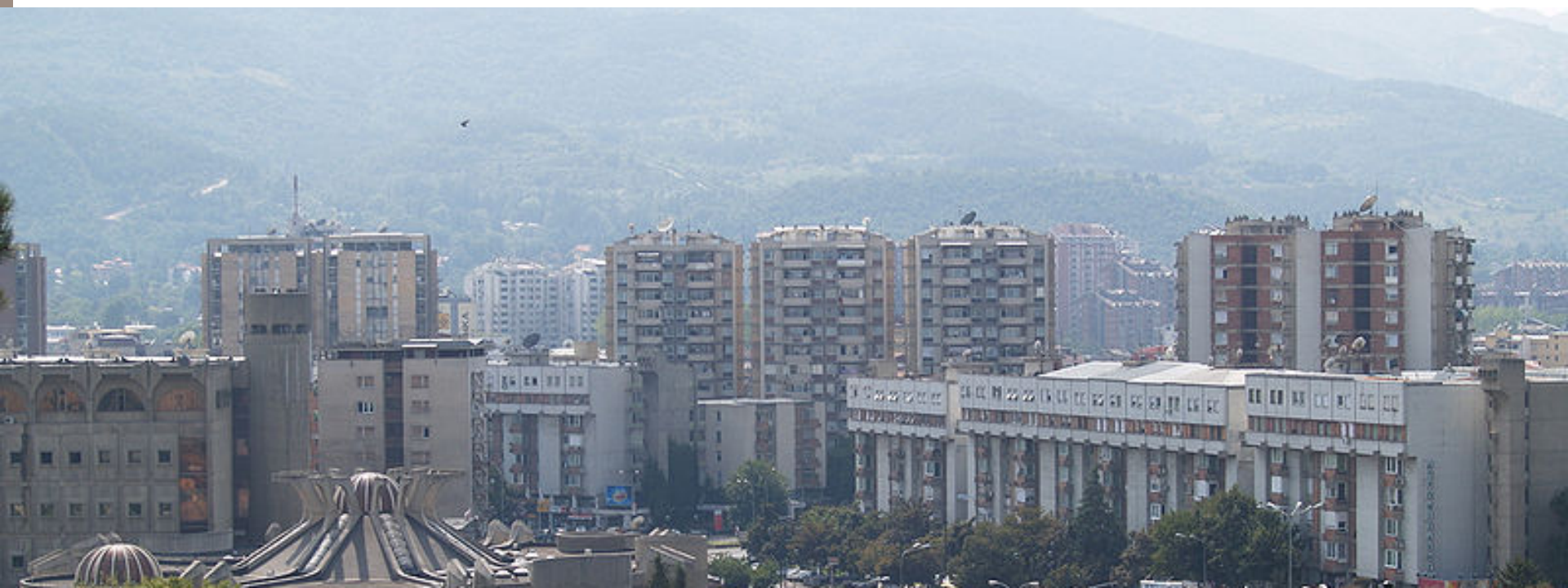
Agency for Electronic Communications - (CERT)

Ministry of Interior

DSCI, MFA, MOD,

University,

MASIT, EUD, Banking Sector, Telecomm Providers, Critical Infrastructure ...



# COUNTRY FOCAL POINTS: KOSOVO

## Contacted representatives:

Ministry of Interior,

Kosovo Police, Cyber Crime Unit

Regulatory Authority of Electronic and Postal Communications - C.E.R.T.

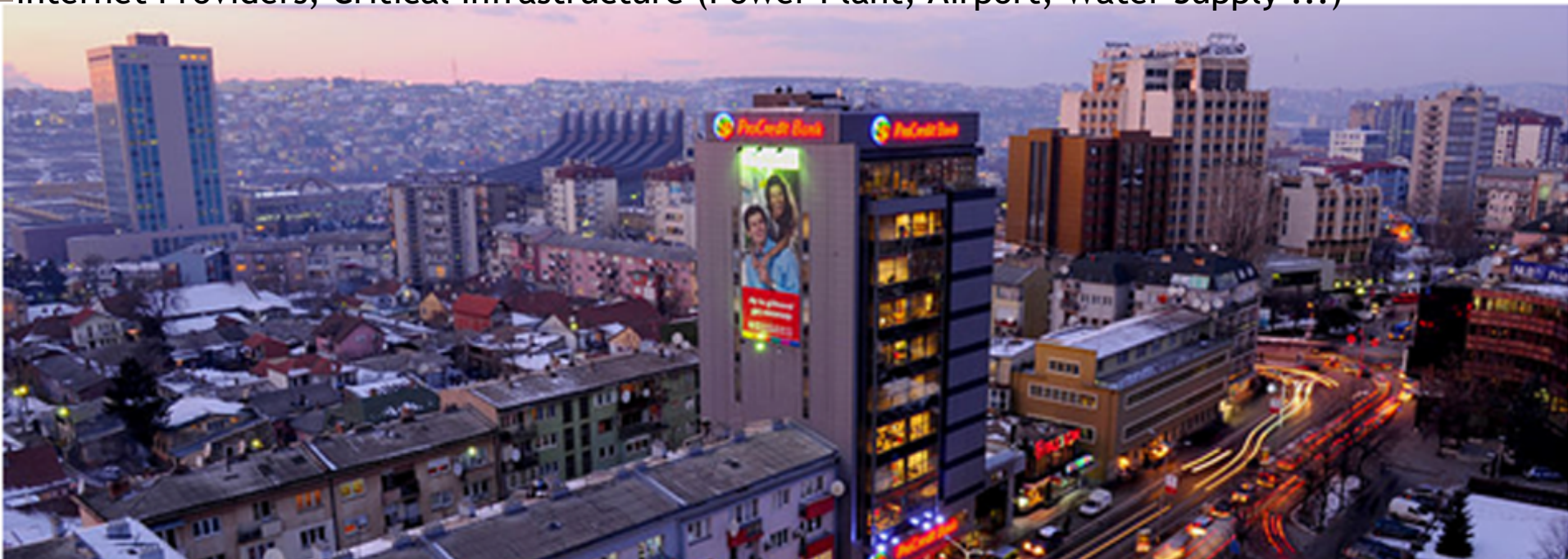
Agency of Information Society

Office of the Prime Minister, Office of the President

National Agency for Protection of Personal Data

University, EUD, MFA, MKSF, MED, MJ,

Internet Providers, Critical Infrastructure (Power Plant, Airport, Water Supply ...)





# COUNTRY FOCAL POINTS: MOLDOVA

Contacted representatives:

CERT - GOV - MD

Ministry of Internal Affairs, Cyber CRIME Unit

E-Government Centre/ Government CIO Office

National Center for Protection of Personal Data

Parliament of Moldova,

National Agency for Energy Regulation

Ministry of Regional Development. Ministry of Environment,

University, EUD, MOD, MFA, MOJ, National Institute of Justice, Banking Sector, Mobile providers ...



# OUR TEAM

---

✓ BESNIK LIMAJ, Team Leader

## POOL OF SHORT TERM EXPERTS:

RAOUL CHIESA

SELENE GIUPPONI

DAN TOFAN (Now works for ENISA)

RADIM OSTADAL

RAUL RIKK

MONIKA JOSI

PETER BURNETT

JEAN-CHRISTOPHE LE TOQUIN

MICHEL RIGUIDEL

GERGERLY DZSINICH

MORE S.T.E. TO BE IDENTIFIED PER SPECIFIC TASKS OF THE PROJECT

**National  
Cyber Security  
Strategy  
in  
PARTNER  
COUNTRIES**

**4**

# NATIONAL CYBER SECURITY STRATEGY - MACEDONIA

WORKING GROUP FOR NCSS:  
**ESTABLISHED BEFORE THE PROJECT START**

**LEADER: MINISTRY OF INTERIOR**

MEMBERS OF THE WORKING GROUP:

3 from Ministry of Interior (1 for Administration)

1 from Ministry of Information Society

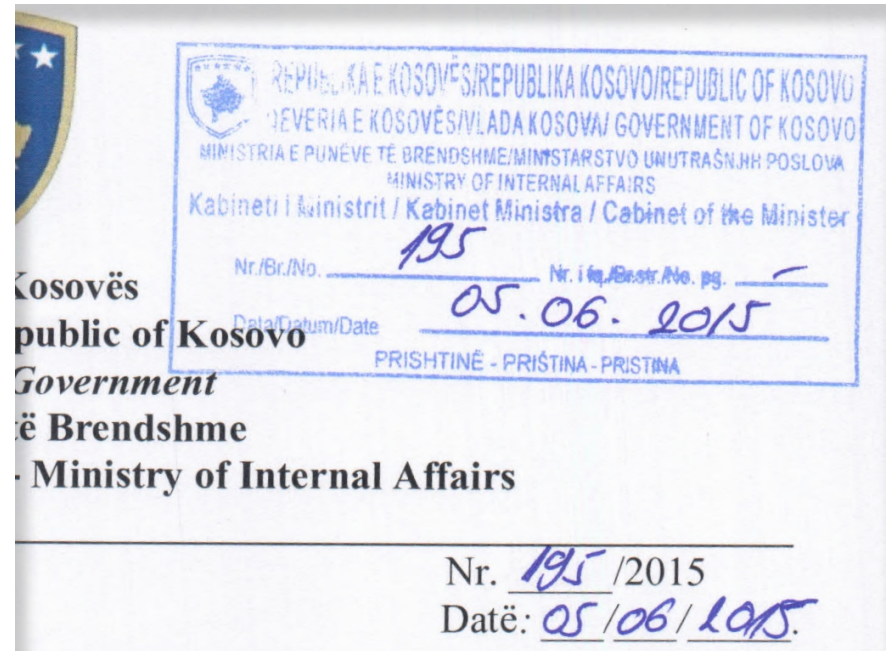
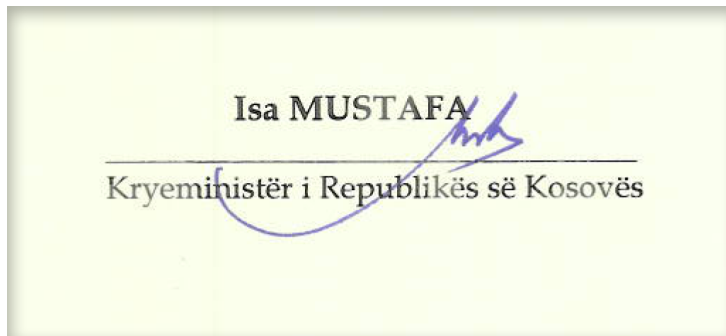
1 from Ministry of Health

1 from Ministry of Defense

1 from Ministry of Education

# NATIONAL CYBER SECURITY STRATEGY - KOSOVO

## WORKING GROUP FOR NCSS: ESTABLISHED IN JUNE 2015 PRIME MINISTER AND MINISTER OF INTERIOR SIGNED DECISION FOR CREATION OF THE NATIONAL CYBER SECURITY STRATEGY AND WORKING GROUP



**LEADER: MINISTRY OF INTERNAL AFFAIRS**

# NATIONAL CYBER SECURITY STRATEGY - KOSOVO

## WORKING GROUP FOR NCSS: ESTABLISHED LEADER: MINISTRY OF INTERNAL AFFAIRS



Republika e Kosovës  
Republika Kosovo - Republic of Kosovo  
Qeveria - Vlada - Government  
Ministria e Punëve të Brendshme  
Ministarstvo Unutrašnjih Poslova - Ministry of Internal Affairs

Nr. 195 / 2015  
Datë: 05.06.2015

Ministri i Ministrisë së Punëve të Brendshme,  
Duke marrë parasysh nenet 4, 21, 22 të Ligjit nr. 03/L-189 Për Administratën Shtetërore të Republikës së Kosovës, (Gazeta Zyrtare, nr. 82, 21 tetor 2010), si dhe duke u bazuar në Nenin 8 (paragrafi 1.4) dhe Shtojcën 3 të Rregullores nr. 02/2011 për lëshat e përgjegjësisë administrative të Zyrës së Kryeministrit dhe Ministrive (22.03.2011), nxjerr:

### V E N D I M

1. Themelohet Grupi Punues për hartimin e Strategjisë për Sigurinë Kibernetike dhe Planin e Veprimit 2015-2018.

2. Grupin Punues nga pika 1 e këtij vendimi e përbëjnë:

2.1. Këshilltari Politik i Ministrisë të MPB-së	Kryesues
2.2. Drejtori i Departamentit të Hetimeve/PK/MPB	Zëvendës Kryesues
2.3. Përfaqësuesi MZHE	Zëvendës Kryesues
2.4. Përfaqësuesi Sekretariatit i Këshillit të Sigurisë të Kosovës	Anëtar
2.5. Përfaqësuesi Zyrtar për Planifikim Strategjik/ZKM	Anëtar
2.6. Përfaqësuesi Zyrtar Lajçore/ZKM	Anëtar
2.7. Përfaqësuesi MP	Anëtar
2.8. Përfaqësuesi Agjencia për Shoqërimë e Informacionit	Anëtar
2.9. Përfaqësuesi MF-SK	Anëtar
2.10. Përfaqësuesi MPJ	Anëtar
2.11. Përfaqësuesi Autoriteti Rregullativ i Komunikimeve Elektronike dhe Postare	Anëtar
2.12. Përfaqësuesi Agjencia Shtetërore për Mbrojtje e të Dhënave Personale	Anëtar
2.13. Përfaqësuesi MD	Anëtar
2.14. Përfaqësuesi MI	Anëtar
2.15. Përfaqësuesi MIE	Anëtar
2.16. Përfaqësuesi AKI	Anëtar
2.17. Përfaqësuesi Dogana K	Anëtar
2.18. Përfaqësuesi Sekretariatit i Strategjive/MPB	Anëtar
2.19. Përfaqësuesi DIEKP/MPB	Anëtar
2.20. Përfaqësuesi DL/MPB	Anëtar
2.21. Përfaqësuesi DTIK/PK/MPB	Anëtar
2.22. Përfaqësuesi Sektori për Hetimin e Krimeve Kibernetike/PK/MPB	Anëtar
2.23. Përfaqësuesi DTIK/MPB	Anëtar

3. Në cilësinë e ekspertëve ftohen përfaqësuesit si në vijim:

- 3.1. Përfaqësuesi Shoqata e Bankave të Kosovës
- 3.2. Përfaqësuesi Universiteti i Prishtinës
- 3.3. Përfaqësuesi Qendra Kosovare për Studime të Sigurisë
- 3.4. Përfaqësuesi Shoqata e Teknologjisë së Informacionit dhe të Komunikimit të Kosovës
- 3.5. Përfaqësuesi Zyra e BE-së
- 3.6. Përfaqësuesi Projekti i BE-së "ENCYSEC"
- 3.7. Përfaqësuesi ICITAP
- 3.8. Përfaqësuesi EULEX
- 3.9. Përfaqësuesi OSBE
- 3.10. Përfaqësuesi UNDP.

4. Sipas nevojës dhe në bazë të vlerësimit të Kryesuesit të Grupit Punues gjatë hartimit të Strategjisë dhe Planit të Veprimit sipas pikës 1 të këtij vendimi, mund të ftohen edhe anëtarë apo ekspert të tjerë nga institucionet shtetërore dhe shoqëria civile.

5. Grupi Punues ka për detyrë të hartojë Strategjinë për Sigurinë Kibernetike dhe Planin e Veprimit 2015-2018, sipas Udhëzimit Administrativ Nr. 02/2012 Për procedurat, kriteret dhe metodologjinë e përgatitjes dhe miratimit të dokumenteve strategjike dhe planeve për zbatimin e tyre.

6. Ftohen të gjitha ministratë dhe institucionet tjera të administratës shtetërore t'i kryejnë obligimet e parapara me këtë vendim, si dhe të bashkëpunojnë me Grupin Punues.

7. Vendimi hyn fuqi diten e nënshkrimit.

  
Shkender Hyseni  
Ministër i Ministrisë së Punëve të Brendshme

Vendimi i dërgohet:

3.5. Përfaqësuesi Zyra e BE-së  
3.6. Përfaqësuesi Projekti i BE-së "ENCYSEC"

# NATIONAL CYBER SECURITY STRATEGY - KOSOVO



## U miratua Strategjia shtetërore për sigurinë kibernetike 2016-2019 dhe plani i veprimit



22.01.2016

Republika e Kosovës për herë të parë bëhet me strategji shtetërore për sigurinë kibernetike 2016-2019 dhe planin e veprimit. Ky dokument strategjik është hartuar dhe finalizuar nën udhëheqjen e Ministrisë së Punëve të Brendshme.

# MOLDOVA

## Government Decision signed on 29 October, 2015 FOR CYBER SECURITY PROGRAMME!



Government of Moldova  
Ministry of Information Technology and Communications

AAA

[Home](#) [About the Ministry](#) [Legislation](#) [Foreign relations](#) [Transparency](#) [Library](#) [Useful information](#)

**Transparency**

Public consultations

- Projects under discussion
- Projects archive 2014
- Projects archive 2013

**Proiectul hotărîrii Guvernului cu privire la Programul privind asigurarea securităţii cibernetice a Republicii Moldova**


Name	Download
Hotărîrea Guvernului	

Data publicării: 29 aprilie 2015  
Datele de contact:  
Stratan Veronica, (+373 22) 251-162, [stratan.veronica@mtic.gov.md](mailto:stratan.veronica@mtic.gov.md)



A large red circle with a black outline, containing white text. The text is centered and reads "CERT's in PARTNER COUNTRIES".

**CERT's in  
PARTNER  
COUNTRIES**

A large black circle with a white outline, containing a white number "5". The circle is set against a teal background.

**5**

# MACEDONIA

LOCATION: Agency for Electronic Communications

LEGAL FRAMEWORK: Law on Electronic Communications (January 2015)

STAFF: AEC - 140 Employees - CERT - up to 5 persons



✓ Equipment purchased

Employee requirement in Process

In the mean time ENCYSEC Project has trained 4 employees at the AEC (Agency for Electronic Communications) that could be later on engaged in working with CERT.



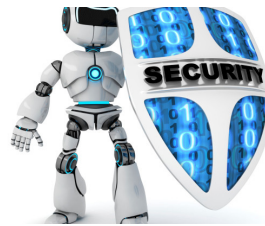
# KOSOVO

**LOCATION:** Regulatory Authority for Electronic and Postal Communications (**RAEPC**)

**LEGAL FRAMEWORK:** Regulated with the

- Law on Electronic Communications **No. 04/L-109** – November 2012 and
- Electronic Comm. Sectoral Policy- **Digital Agenda for Kosovo 2013-2020**

**STAFF:** RAEPC – 39 Employees - CERT – up to 5 persons and by the end of 2016 – in KOS-  
CERT are planning to work 8-10 people



**Current situation:**

**2 Staff Recruited**

**1<sup>st</sup> Employee selected and already started working (November 2014).**

**2<sup>nd</sup> Employee started working on 6 October 2015.**



# KOSOVO

## CERT CAPACITY BUILDING

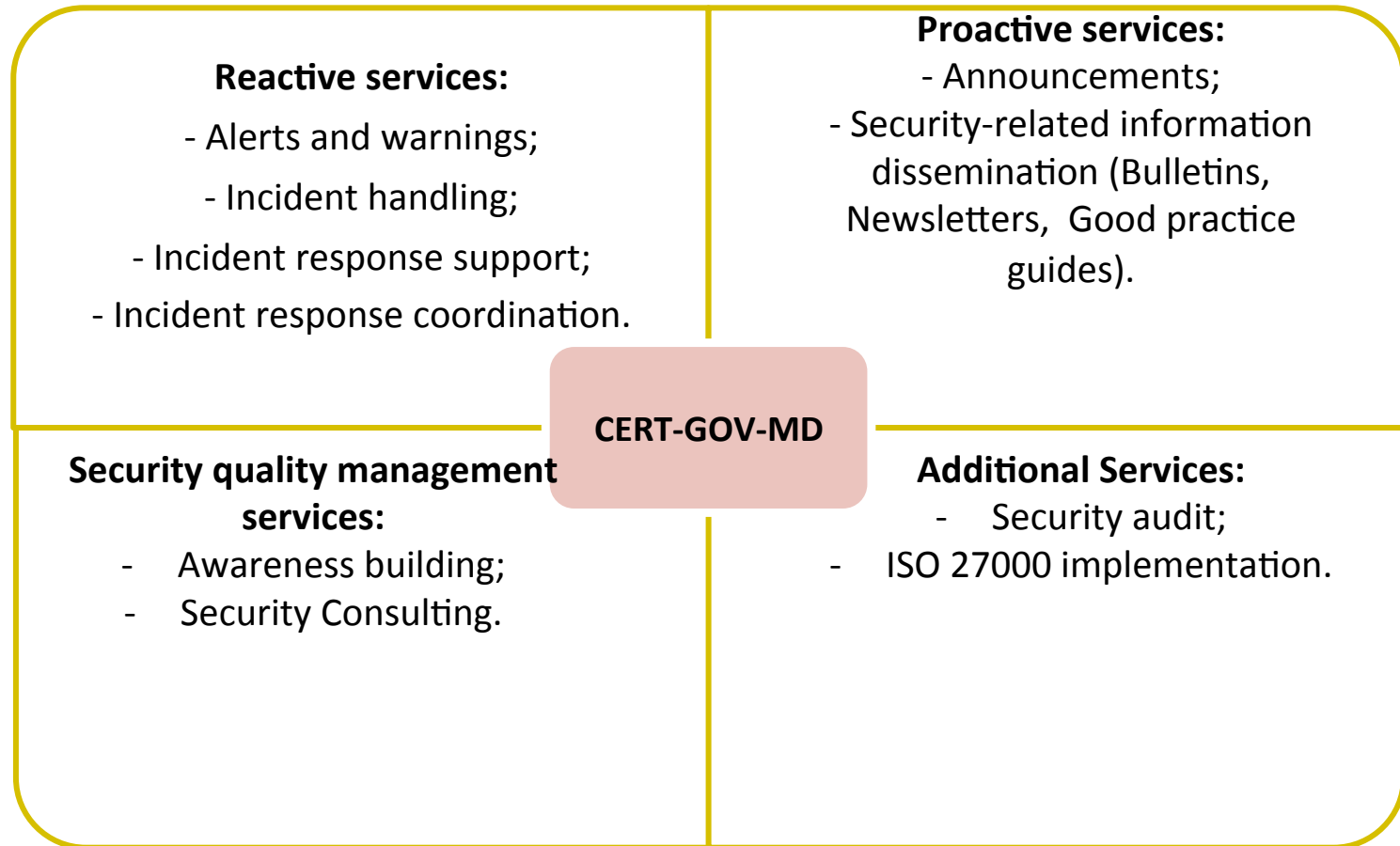
Since National CERT in Kosovo is not functional for 4 years, has limited resources and could employ only two persons and have no equipment yet other institutions have initiated a process of building other CERT's as:

1. **GOV - CERT** within Agency for Information Society as they have State of the Art Data Centre and capable staff (**58 employees**) that we've trained
2. **Police CERT** - We've trained their personnel and they also have capable staff (**51 employees in IT Department**) and they have State of the Art Data Centre
3. **MOI CERT** - We've trained them as well and they also have capable staff (**53 employees in IT Department**) and State of the Art Data Centre for personal records



# MOLDOVA

## CERT-GOV-MD SERVICES



# MOLDOVA

## INTERNATIONAL COOPERATION



A large red circle with a black outline, containing the word "METHODOLOGY" in white, bold, uppercase letters.

**METHODOLOGY**

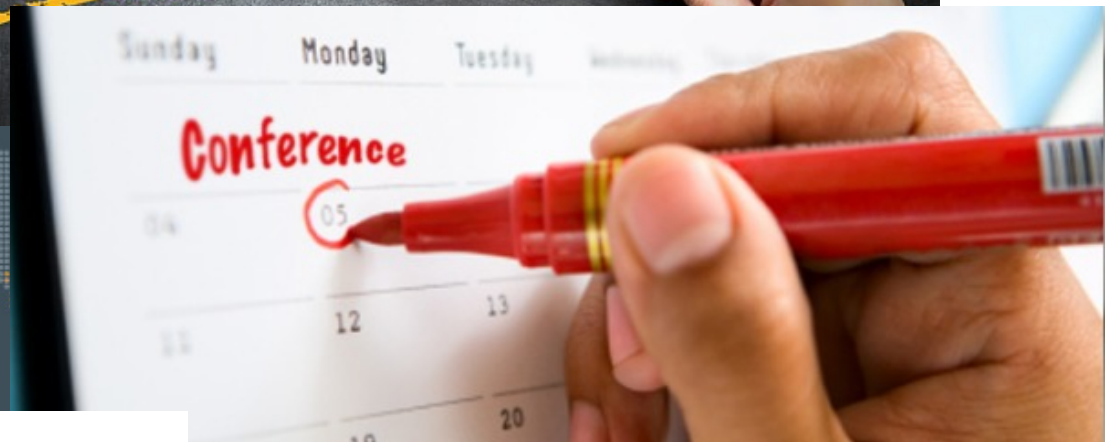
A large black circle with a white outline, containing the number "6" in white, bold, sans-serif font.

**6**

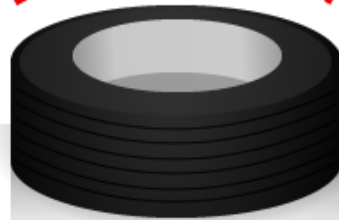
# METHODOLOGY



**STUDY**  
TOURS



**Don't Reinvent it!**




**Perfect it!**




INTERNATIONAL  
**CYBER  
EXERCISE**



# DILEMMA



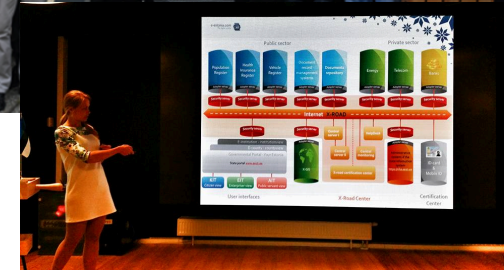
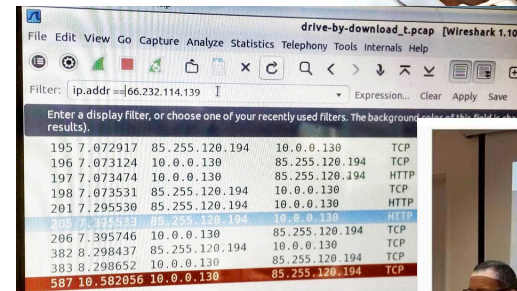
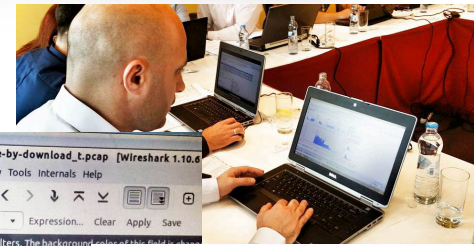
What if we train them and they leave?



What if you don't train them and they stay?

# WORKSHOPS AND CONFERENCES ORGANISED/PARTICIPATED

- EU ISS Conference in Paris, France February 2014
- Workshop with ANSSI in Paris, France April 2014
- 43rd TF-CSIRT Meeting, 18th & 19th September, ROME
- Workshop – Conference, October - Sibiu, Romania
- Workshop ON NCSS/CERT – October 2014, Paris, France
- Workshop – December 2014, Prague, Czech Republic
- FIC 2015 Conference – January – Lille, France
- Cyber Needs Conference, Brussels February 2015
  - TARGET GROUP:
  - **CENTRAL AND SOUTH AMERICA**
  - AFRICA
  - ASIA
- STUDY TOUR – CERT-RO BUCHAREST, ROMANIA MARCH, 2015
- TRANSITS I TRAINING – PRAGUE, CZECH REPUBLIC APRIL, 2015
- MENTORING WORKSHOPS IN THREE PARTNER COUNTRIES
- CIIP/PPP Workshop – May, 2015 – Paris, France
- Study Visit – June, 2015 – Estonia
- Cyber Exercise – June, 2015 – Prague, Czech Republic
- Cyber Security Conference – September, 2015 – Sibiu, Romania
- Cyber Drill Exercise – September - October, 2015 – Budva, Montenegro
- ENCYSEC - FIRST – UNDP Conference in Istanbul
- Study Visit – Enisa – Athens, Greece
- Study Visit – Vannes, Brittany - France



# EU ISS Conference in Paris, France February 2014

**Cyber Capacity Building  
as a Development Issue:  
What Role for Regional Organisations?**

International conference hosted by  
the EU Institute for Security Studies  
Paris, 13-14 March 2014



# Workshop with ANSSI in Paris, France April 2014



# 43<sup>rd</sup> TF-CSIRT Meeting, 18th & 19th September, ROME



TRUSTED INTRODUCER IS ASSOCIATION OF ALL CERTS FROM EUROPE.  
WE WERE INVITED IN THEIR MEETING IN ROME EVEN WITHOUT BEING  
CREATED AS CERTS

## ACTIVITIES

- Presentation of the Project
- Introduction of the Partner Country Representatives
- Networking with various CERT representatives
- Presentations

## FOLLOW UP:

- Listing request form sent for TI registration (Klaus-Peter Kossakowski)
- Approval by next TF-CSIRT meetings

# WORKSHOP - CONFERENCE, OCTOBER - SIBIU, ROMANIA



## **CYBERSECURITY IN ROMANIA - CONFERENCE -**

Second Edition, Sibiu, 2 - 3 October 2014

### ACTIVITIES

- **\_PRESENTATION OF THE PROJECT**
- **NETWORKING WITH VARIOUS CYBER SECURITY ACTORS**
- **PRESENTATIONS ON AWARENESS RAISING**
- **IDENTIFICATION OF POTENTIAL SHORT TERM EXPERTS**

### FOLLOW UP:

- **INVITATION TO PARTICIPATE AS OBSERVERS IN 2015 ITU CYBER-DRILLS (ISTANBUL OR MONTENEGRO) - (Mrs. Rosheen Awotar-Mauree)**
- **INVITATION FOR A POSSIBLE STUDY TOUR ON CRITICAL INFRASTRUCTURE INFORMATION PROTECTION IN SWITZERLAND (Representative of the Swiss Government)**

# WORKSHOP - CONFERENCE, OCTOBER - SIBIU, ROMANIA



**IN ROMANIA**  
- CONFERENCE -

Second Edition, Sibiu, 2 - 3 October 2014

## WORKSHOP ON C.E.R.T.

- C.E.R.T. CASE STUDY OF ROMANIA
- C.E.R.T. CASE STUDY OF CZECH REPUBLIC

## TOPICS COVERED:

- HOW THEY STARTED
- LEGAL FRAMEWORK
- ORGANISATIONAL CHART
- SERVICES OFFERED
- HOW THEY HANDLE INCIDENTS
- WHAT TOOLS THEY USE



# WORKSHOP - OCTOBER 2014, PARIS, FRANCE

**THALES**



**LEXSI**

## ACTIVITIES

- **PRESENTATION OF THE CURRENT SITUATION OF THE PROJECT**
- **THALES (MR. PAUL THERON) PRESENTATION ON:**
  - **Review of EPCIP (European Programme for Critical Infrastructure Protection) and CIIP (Critical information Infrastructure Protection)**
- **LEXSI PRESENTATION ON:**
  - **CSIRT ROLE IN NCSS**
- **ANSSI (MR. JEAN BAPTISTE DEMAISON) PRESENTATION ON:**
  - **DEVELOPING AND IMPLEMENTING A NCSS**
- **CASE STUDY OF NCSS - CZECH REPUBLIC (STE RADIM OSTADAL)**
- **CASE STUDY OF NCSS - ROMANIA (STE DAN TOFAN)**

## FOLLOW UP:

- **MENTORING MISSIONS AND WORKSHOP IN PARTNER COUNTRIES**
- **POSSIBLE STUDY VISIT TO THALES (2015)**
- **POSSIBLE STUDY VISIT TO LEXSI (2015)**



# WORKSHOP - OCTOBER 2014, PARIS, FRANCE

THALES



LEXSI



# WORKSHOP - DECEMBER 2014, PRAGUE, CZECH REPUBLIC

**Block I - CSIRT Organisation -**

**Block II - CSIRT Operations**

**Block III - Basic attacks techniques -**

**Block IV - Basic Training on Certified Ethical Hacker -**



# FIC 2015 CONFERENCE - JANUARY - LILLE, FRANCE



## CONFERENCE HOSTED BY :

1. Mr Bernard Cazeneuve, Minister of the Interior,  
Republic of France
2. Mr Thomas de Maizière, Minister of the Interior,  
Federal Republic of Germany

# CYBER NEEDS CONFERENCE, BRUSSELS FEBRUARY 2015



## TARGET GROUP:

- CENTRAL AND SOUTH AMERICA
- AFRICA
- ASIA

## THREE THEMATIC AREAS

- CYBER CRIME AND JUSTICE
- CRITICAL INFORMATION INFRASTRUCTURE PROTECTION
- RESILIENT E-DEVELOPMENT

# CYBER NEEDS CONFERENCE, BRUSSELS FEBRUARY 2015



## - NETWORKING -



# MARCH - APRIL, 2015

## STUDY TOUR - CERT-RO BUCHAREST, ROMANIA

9-10 MARCH, 2015



## TRANSITS I TRAINING - PRAGUE, CZECH REPUBLIC

23-24 APRIL, 2015





« *networking the networkers* »

[NEWS](#) · [EVENTS](#) · [ACTIVITIES](#) · [PUBLICATIONS](#)

[ABOUT](#) · [CONTACT](#) · [SOCIAL](#) · [LOGIN](#) ·

[HOME](#) > [ACTIVITIES](#) > [TRANSITS](#) > [TRANSITS-I](#) > [PRAGUE](#) > [APR15](#)

## 25th TRANSITS I Training Workshop



# CERT TRAINING WORKSHOPS - SKOPJE, PRISHTINA, CHISINAU



**Metasploit**

- Platform for writing, testing, and using exploit code
- Allows launching exploits on real-world applications
- It is build-in tool in Kali operating system
- Free vs PRO version
- Big database of known vulnerabilities and corresponding exploits
- Metasploit offers many types of payloads, including:
  - Command shell - enables to run collection scripts
  - Metasppreter - enables control of the screen of a device using VNC and to browse, upload and download files
  - Dynamic payloads - enables to evade anti-virus detection by generating unique payloads

May, 2015



# CERT TRAINING WORKSHOPS - SKOPJE, PRISHTINA, CHISINAU



May, 2015

# CERT WORKSHOPS - SKOPJE, PRISHTINA, CHISINAU



# MENTORING MISSIONS - MARCH-OCTOBER, 2015

## *Mentoring Session*



**NCSS WORKSHOP -  
Chisinau  
17 - 18 MARCH, 2015**

# CIIP/PPP - MAY, 2015 - PARIS, FRANCE



- ❖ ENISA Guidelines on PPPs
- ❖ Trusted Information Sharing - Essence of PPP
- ❖ GIP RENATER
- ✓ Security as strategic priority for research and education networks



- ❖ Identification of CII
- ❖ SCADA vulnerabilities
  
- ❖ Security Framework for
  - Network Providers
  - Data Protection providers
  - Financial Banking Sector

# CIIP/PPP - MAY, 2015 - PARIS, FRANCE



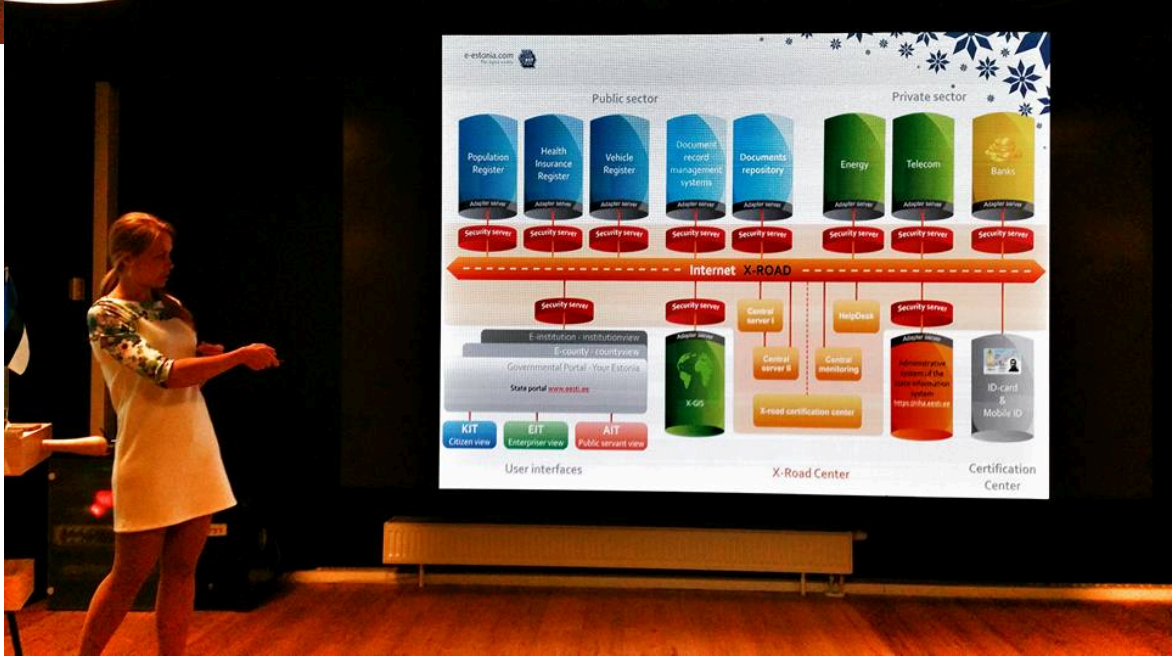
# CIIP/PPP - MAY, 2015 - PARIS, FRANCE



# CIIP/PPP - MAY, 2015 - PARIS, FRANCE

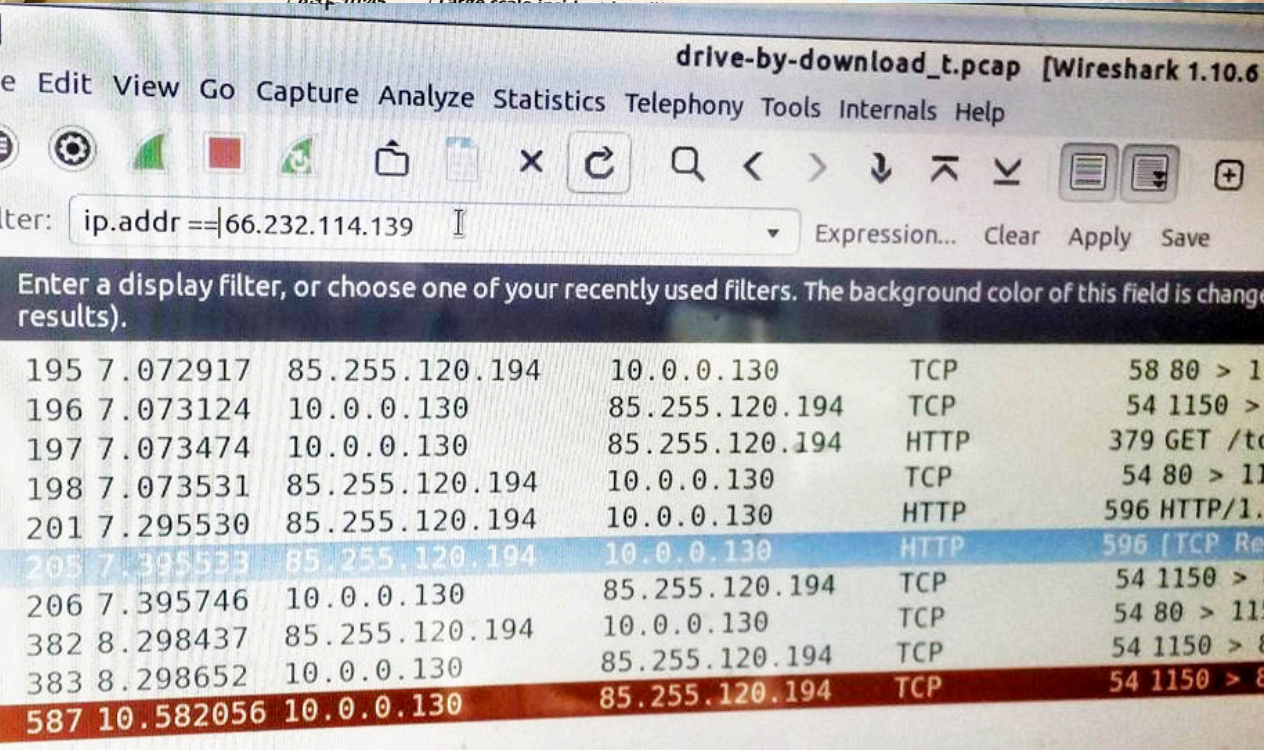
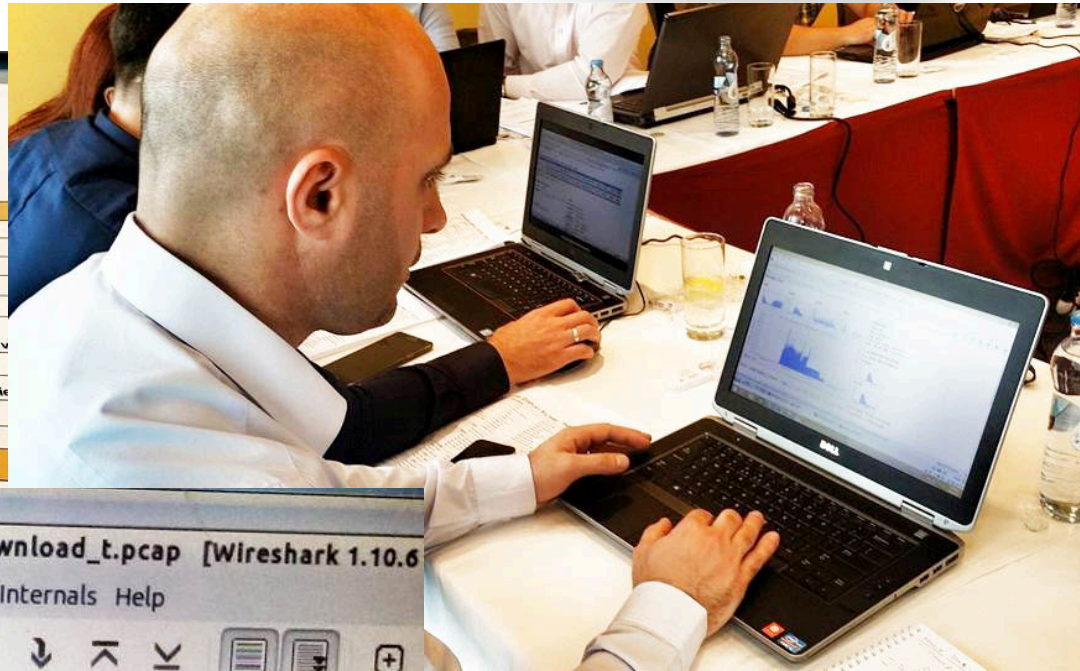


# STUDY VISIT - JUNE, 2015 - ESTONIA





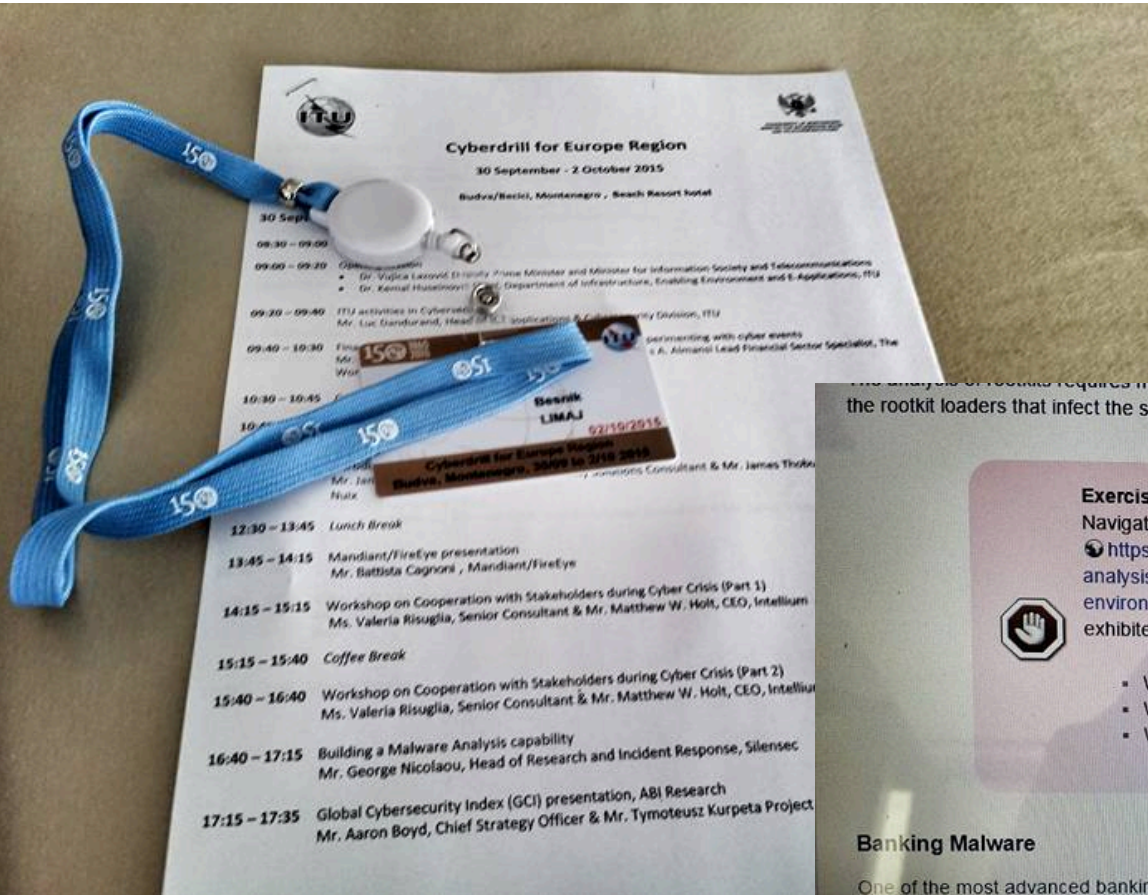
# CYBER EXERCISE - JUNE, 2015 - PRAGUE, CZECH REPUBLIC



# CYBER SECURITY CONFERENCE - SEPTEMBER, 2015 - SIBIU, ROMANIA



# CYBER DRILL EXERCISE - SEPTEMBER - OCTOBER, 2015 - BUDVA, MONTENEGRO



...analysis of results requires manual reverse engineering and cannot be done using a sandbox technology. However, the rootkit loaders that infect the system.

## Exercises:

Navigate to the following URL containing a report produced by the VxStream sandbox technology:

🌐 <https://www.hybrid-analysis.com/sample/1a7dc86d9fb6b27f7f7b3156ddf3369474b83784cbd12e8d8b8137bd50f2?environmentId=2> This sandbox technology provides high level descriptions of the behavior exhibited by the malware. Discuss and answer the following questions in your group:



- What malicious behaviour indicates the presence of a rootkit?
- Which runnable executable files does this sample access or execute? (drivers and executables)
- Would you consider the Anti-Reverse Engineering and Stealth techniques advanced?

## Banking Malware

One of the most advanced banking malwares that stirred a panic within the financial industry is the well known Zeus malware variant SpyEye. The following reports include a sandbox analysis of an advanced SpyEye sample:

🌐 <https://malwr.com/analysis/NGIzNzdjYTIkNzVINGI5NmEyODkzZWY0NmU4ZmZhNGI/>

🌐 <https://www.hybrid-analysis.com/sample/591be7d2050cd4f7946b22b42575f108ea8b3299519774118fe4abb8051c5cf52>

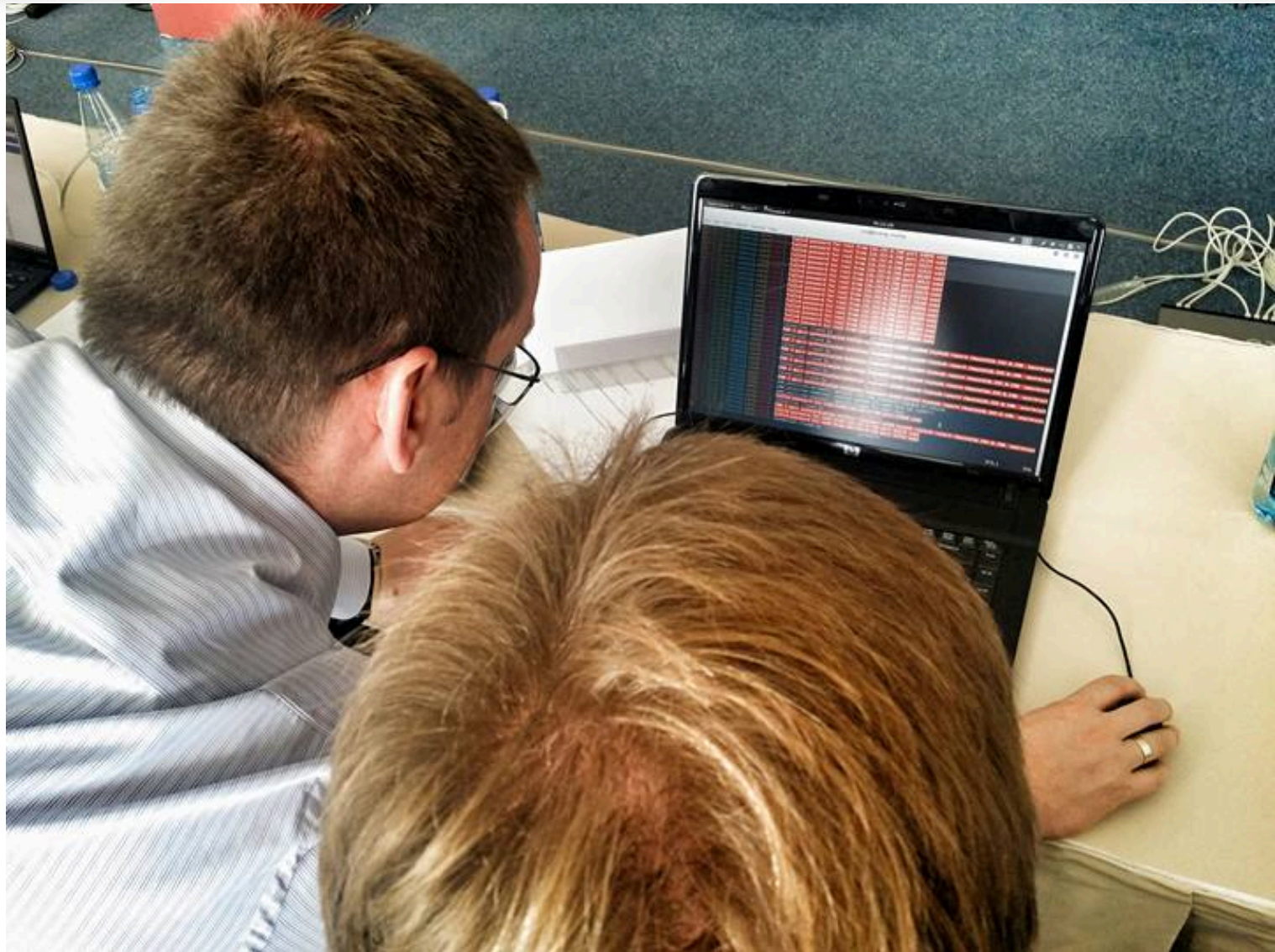
**Exercises:** Familiarize yourself with the reports given above. Discuss and answer the following questions:

- Do you see any indications that the malware sample uses the Tor privacy network?
- The VxStream report indicates that the sample has the ability to "Query Process Information". What API is used (you can expand the signature and see the API) what does it do?

# CYBER DRILL EXERCISE - SEPTEMBER - OCTOBER, 2015 - BUDVA, MONTENEGRO



# CYBER DRILL EXERCISE - SEPTEMBER - OCTOBER, 2015 - BUDVA, MONTENEGRO



# SYNERGY WITH OTHER DONORS



26-27 OCTOBER, 2015  
ISTANBUL CONFERENCE  
CROWN PLAZA

TWO TRACK:  
• MANAGERIAL  
• TECHNICAL



2015  
**FIRST**  
TC and TRANSITS  
Training

Istanbul, TR  
October 26-27, 2015

# ENCYSEC - FIRST - UNDP CONFERENCE IN ISTANBUL



# FACILITATION OF CYBER SECURITY TRAINING EXERCISES IN PARTNER COUNTRIES



December  
2015



# STUDY VISIT - ENISA - DECEMBER 2015



# STUDY VISIT VANNES, FRANCE - FEBRUARY 2016



# MOBILE FORENSICS - CYBER ESPIONAGE, CIIP - FEBRUARY-MAY 2016



# PARTICIPATION IN VARIOUS WORKSHOPS AND CONFERENCES



**CYBERSECURITY  
IN ROMANIA  
- CONFERENCE -**

Second Edition, Sibiu, 2 - 3 October 2014




**Cybersécurité  
et Transformation Numérique**



**CYBER NEEDS  
AND DEVELOPMENT**

A large red circle with a black outline, containing the text "NEXT STEPS" in white, bold, uppercase letters.

**NEXT STEPS**

A large black circle with a white outline, containing the number "7" in white, bold, sans-serif font.

**7**

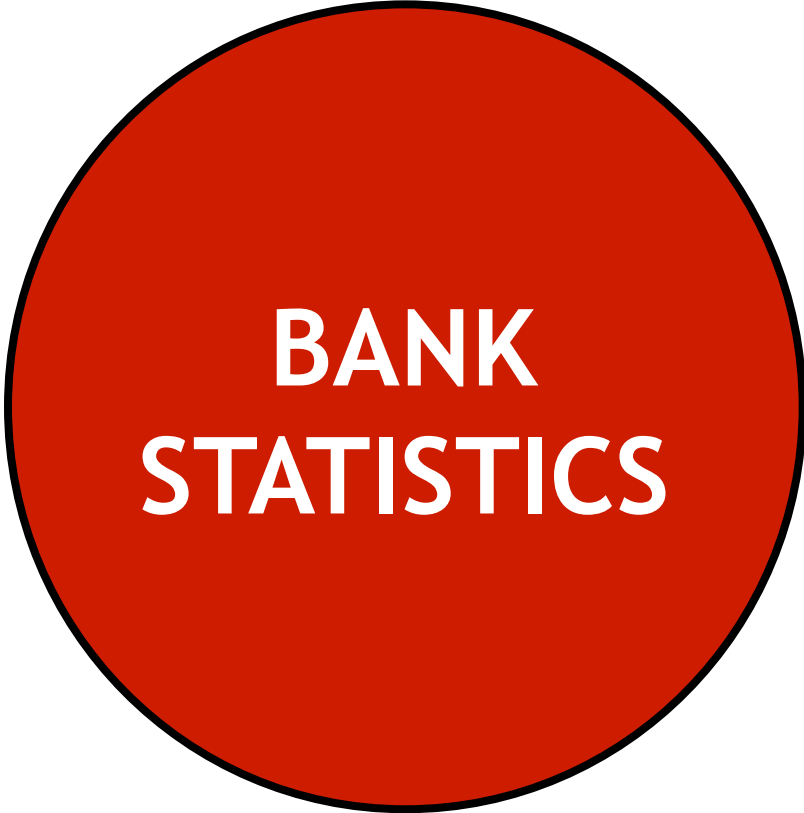
# PROJECT EXTENSION - JUNE 2016

## TAILOR MADE ACTIVITIES




# INTERNATIONAL COOPERATION



A large red circle with a black outline, centered on a white background. Inside the circle, the words "BANK" and "STATISTICS" are written in white, bold, uppercase letters, stacked vertically.

**BANK  
STATISTICS**

A large black circle with a white outline, centered on a teal background. Inside the circle, the number "8" is written in white, bold, uppercase letters.

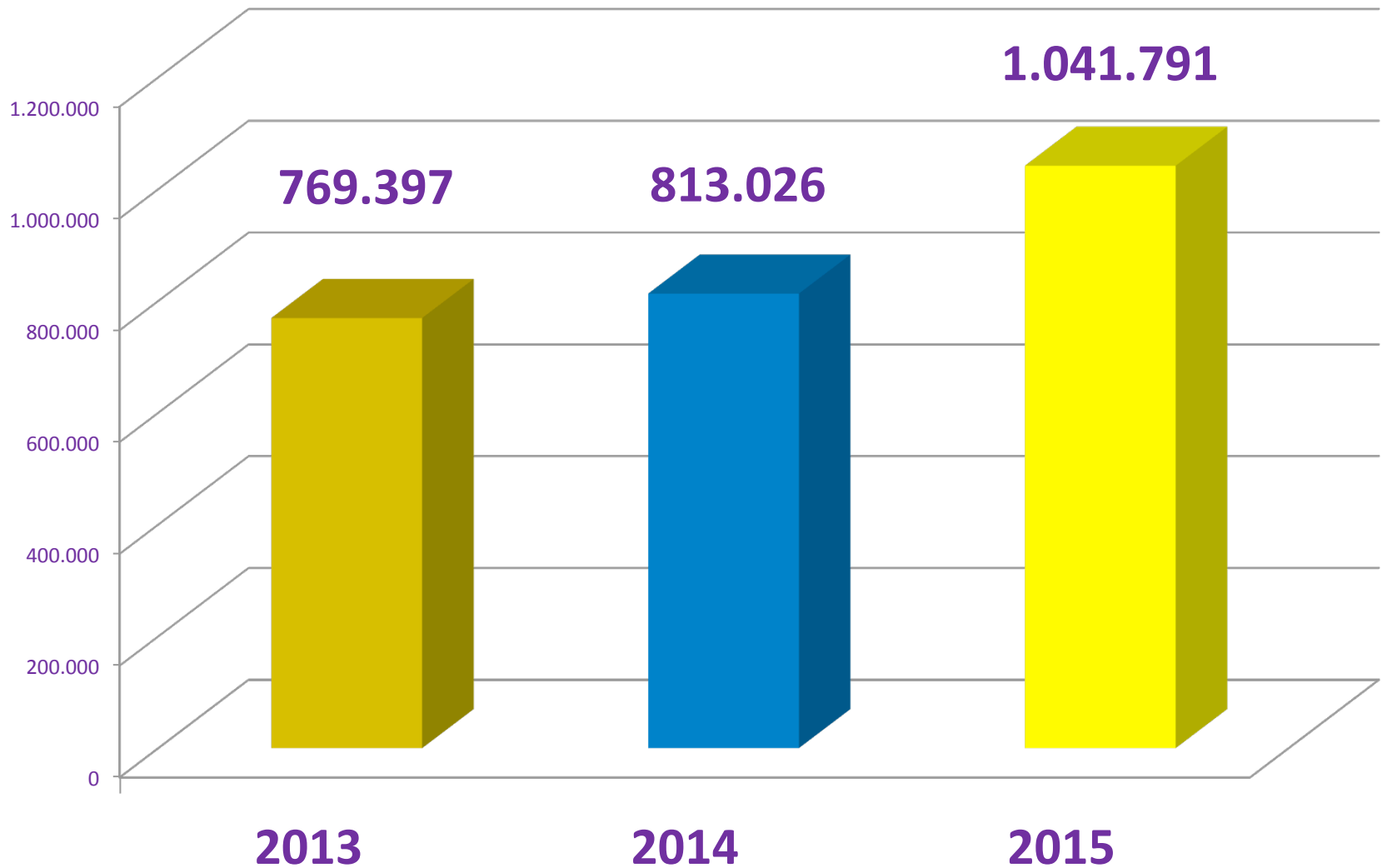
**8**



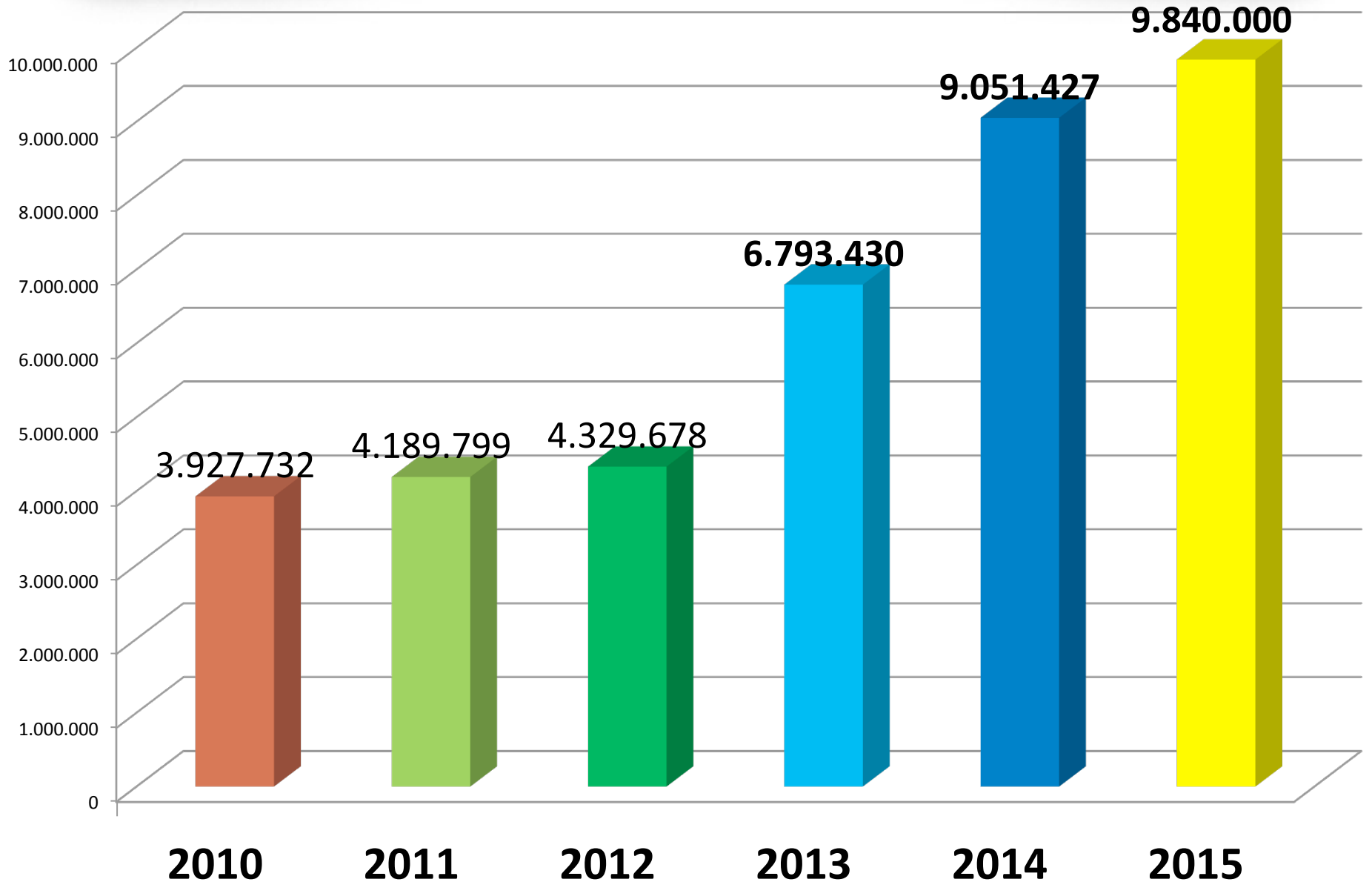
# SPEAR PHISHING - CEO FRAUD



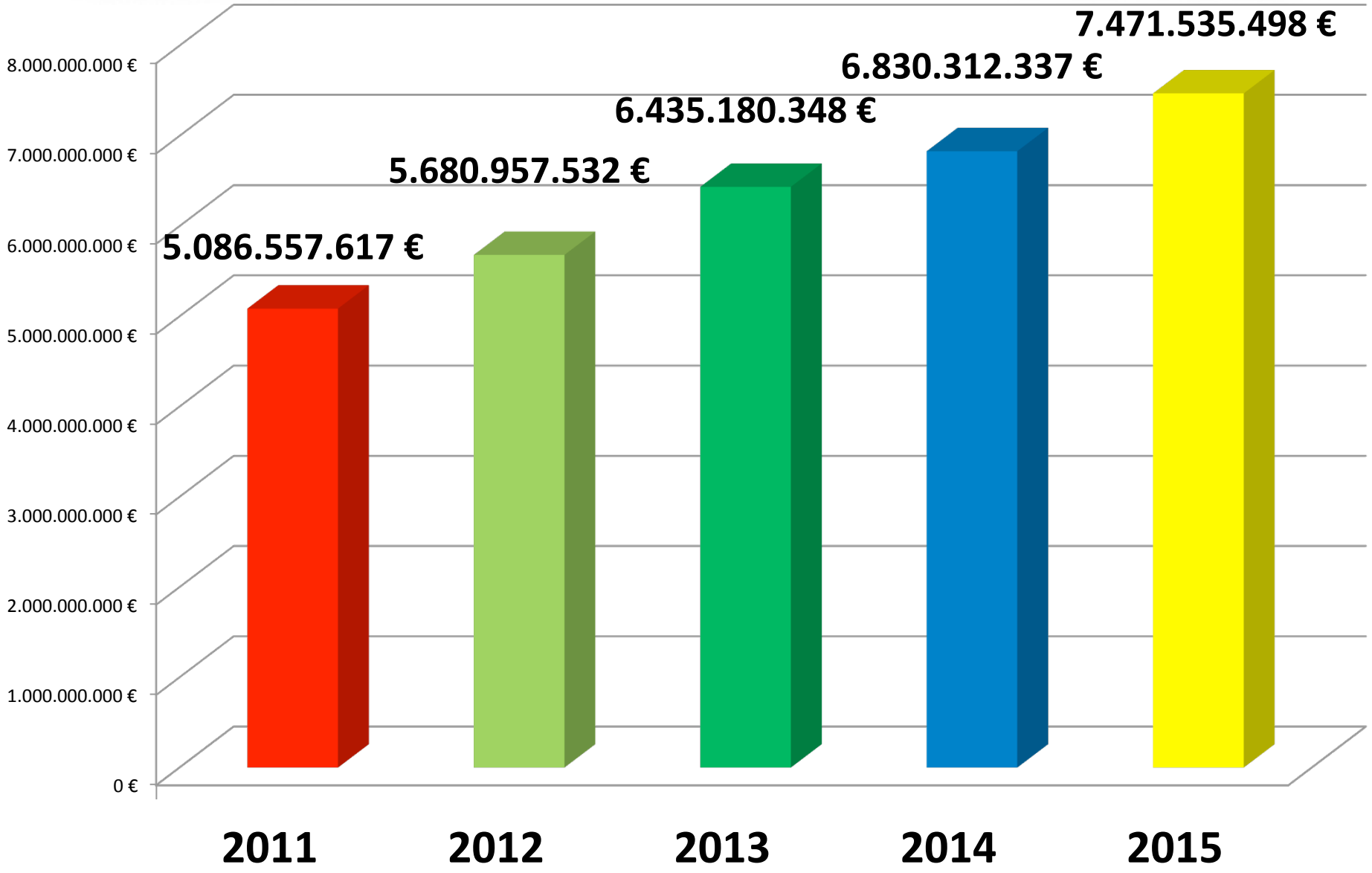
# Number of issued Bank cards per Year in one of ENCYSEC Partner Countries



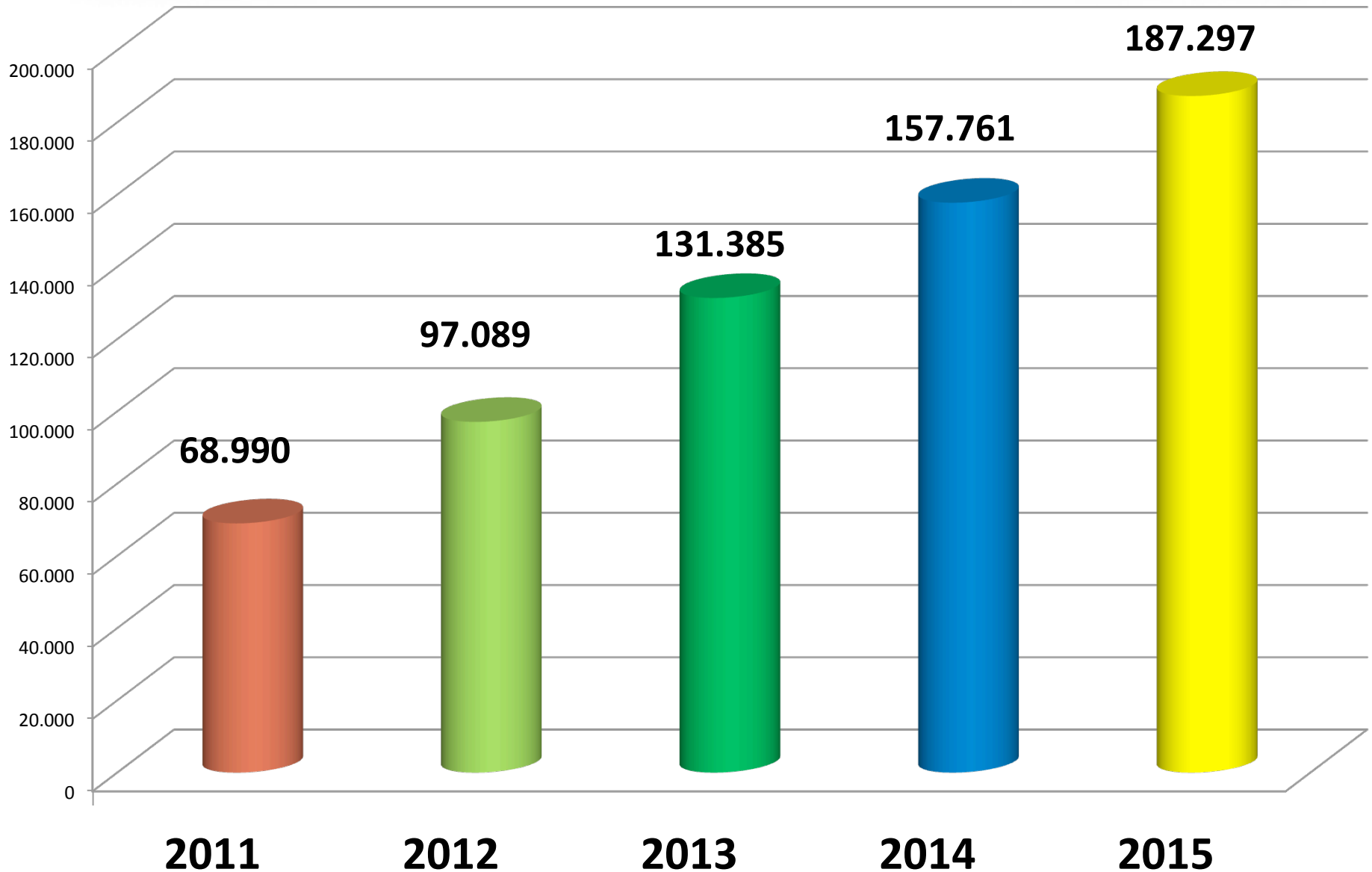
# Number of interbank transactions per year in one of ENCYSEC Partner Countries



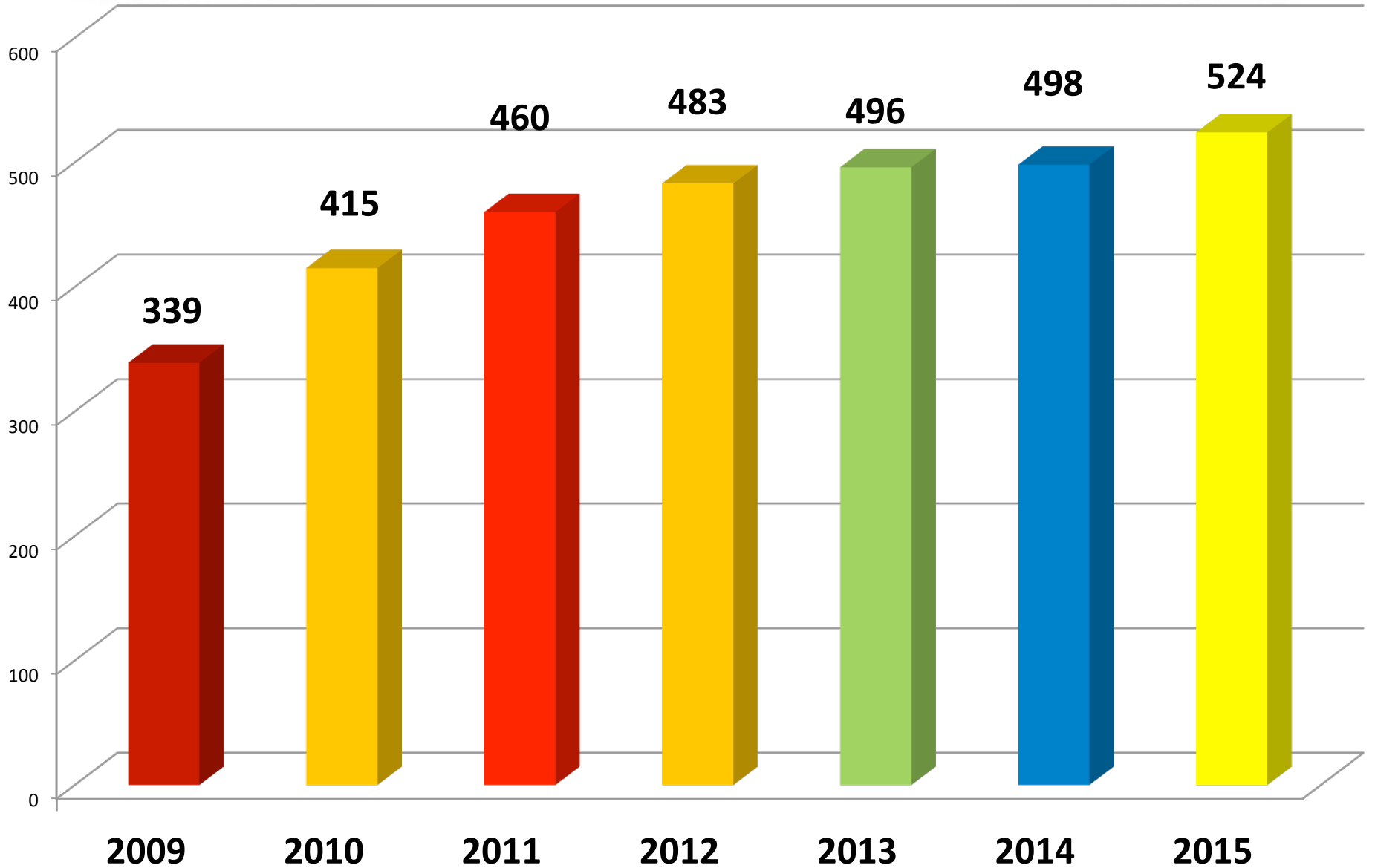
# The value of interbank transactions in one of ENCYSEC Partner Countries



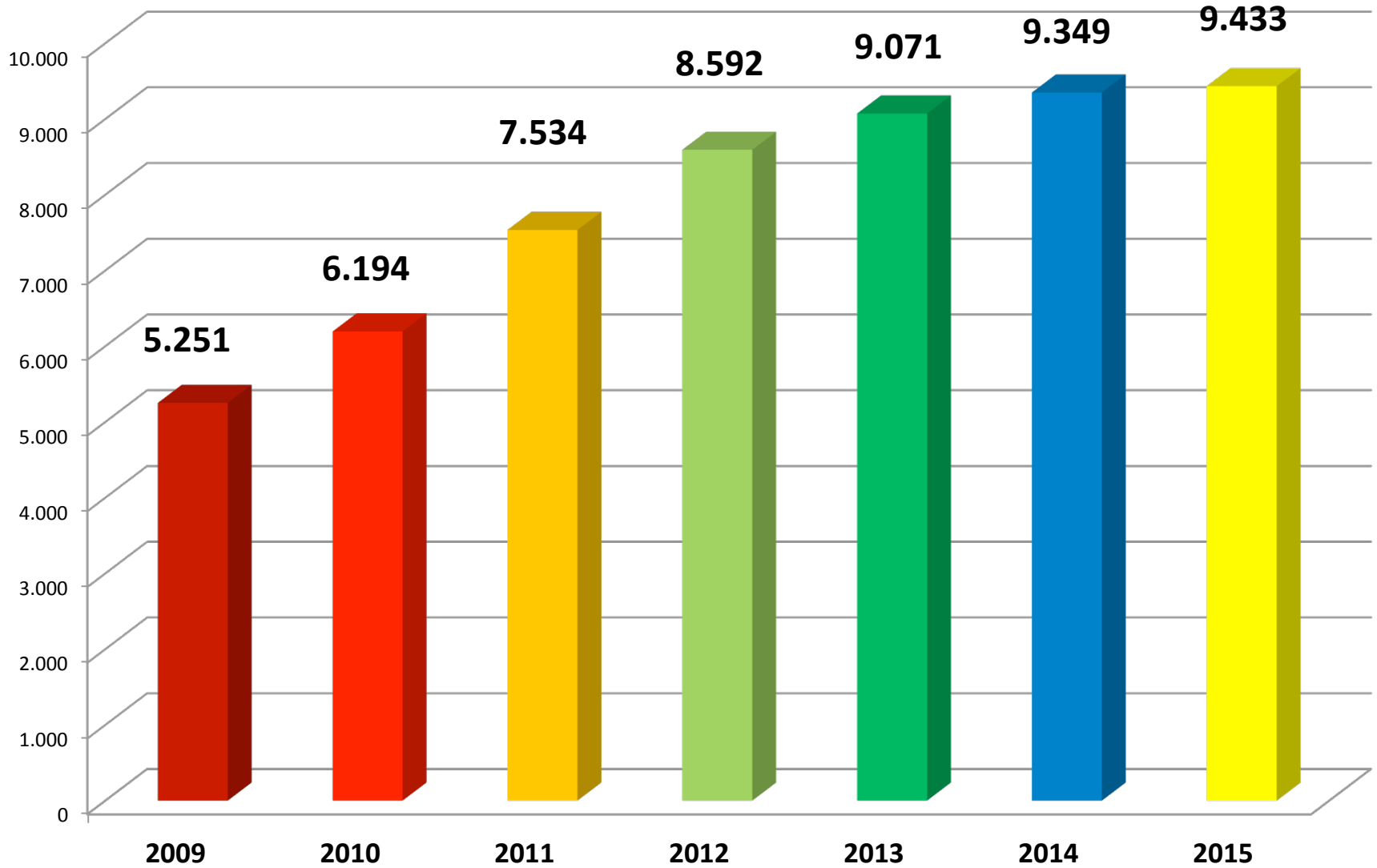
# Number of e-banking accounts per Year in one of ENCYSEC Partner Countries



# Number of ATM's per Year in one of ENCYSEC Partner Countries

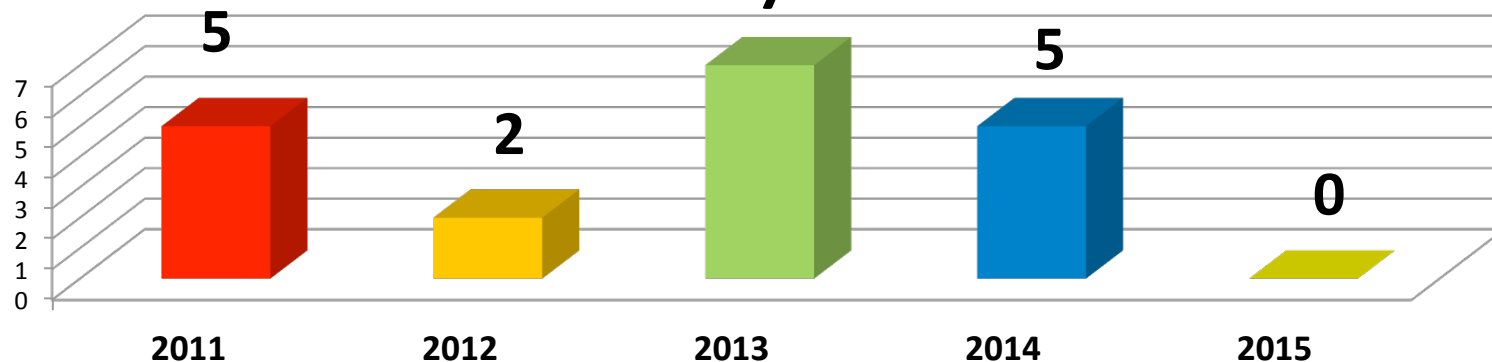


# Number of POS terminals per Year in one of ENCYSEC Partner Countries

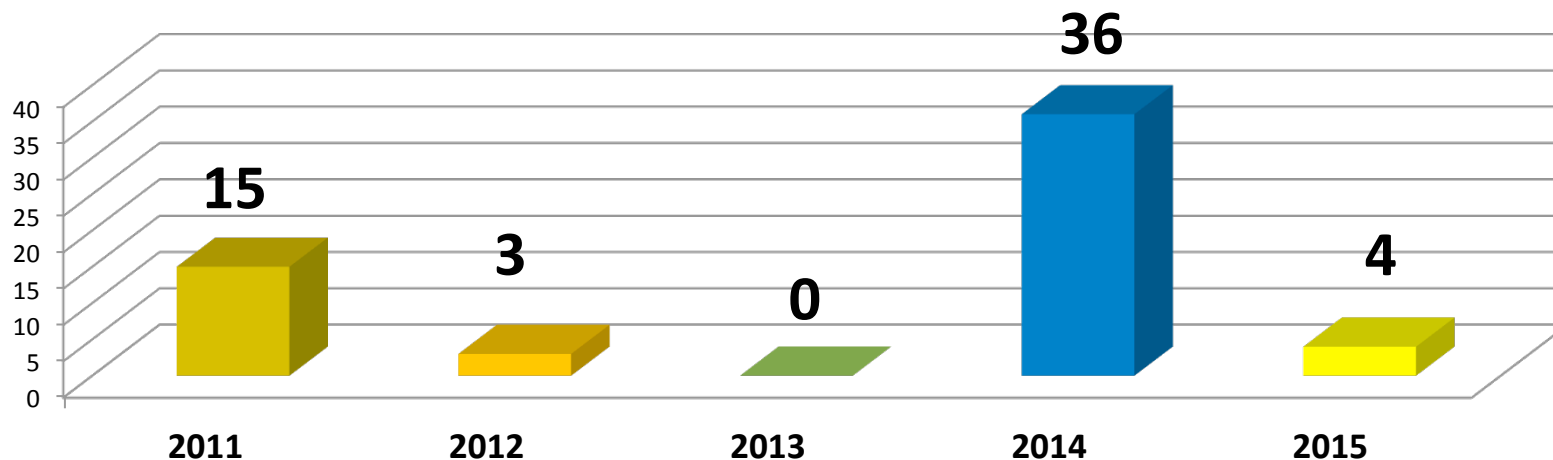


# PHYSICAL THEFTS VS ATM ATTACKS

Number of physical thefts in Banks per Year in one of ENCYSEC Partner Countries



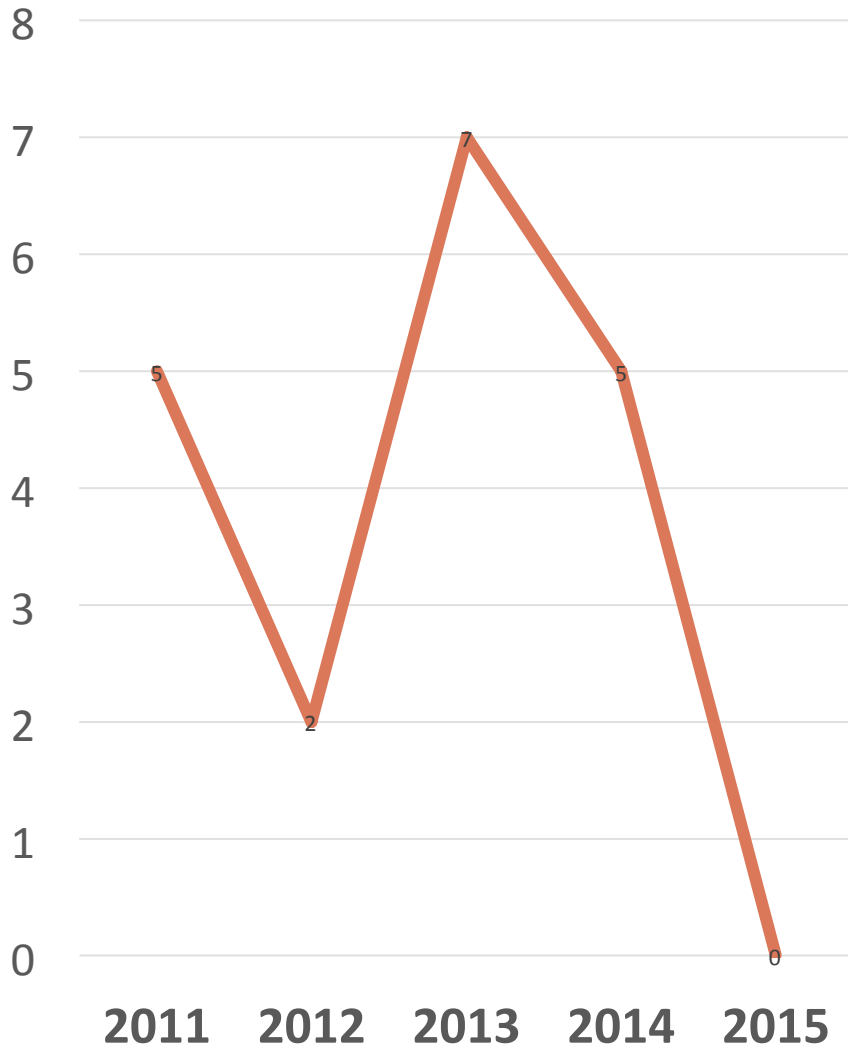
Number of ATM attacks per Year in one of ENCYSEC Partner Countries  
Skimmer and other smart attacks



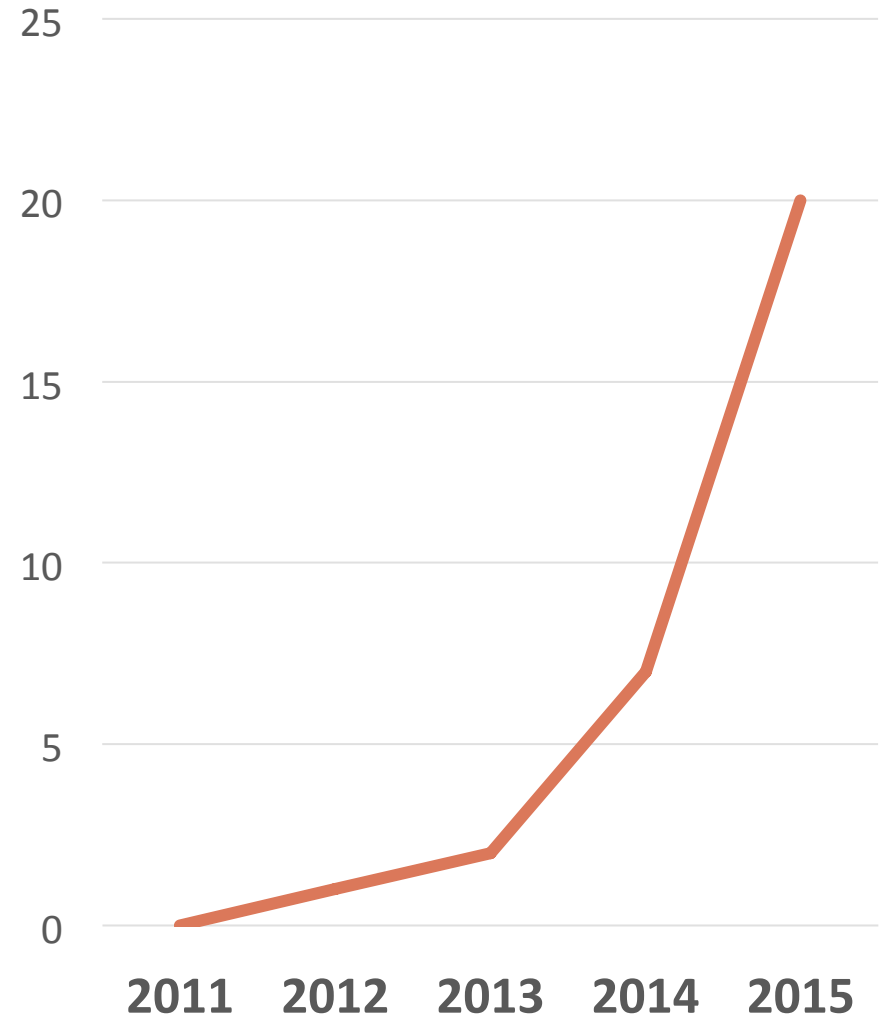


# PHYSICAL VS. CYBER THEFTS

## Physical Thefts



## Cyber Thefts



# SPEAR PHISHING - CEO FRAUD



# CHANGE OF BANK ACCOUNT

← << >> 🗑️ Delete 📁 Move ▾ 🛡️ Spam ▾ ⋮ More ▾

The payment should now be made by another bank account

Dear Sir

Please note that our Company accountant just informed

us that our bank account that was send to you in our

previous invoice has just been overdraft

and currently undergoing auditing, for this reason we

cannot receive any payment for the time being in the

account. please kindly make the payment to our

second trade bank account below.

Beneficiary name: HB BODY

Bank Name: HALIFAX BANK PLC

A/C Number: 00664536

Sort Code: 11-05-20

IBAN: GB64HLFX11052000664536

BIC: HLFXGB21E26

please cancel the payment and remake it with this bank

Your prompt reply will be highly appreciated.

◀ ▶ 🗑️ Delete 📁 Move ▼ 🛡️ Spam ▼ ⋮ More ▼

The payment should now be made by ano

Dear Sir

Please note that our Company accountant just informe

us that our bank account that was send to you in our

previous invoice has just been overdraft

and currently undergoing auditing, for this reason we

cannot receive any payment for the time being in the

account. please kindly make the payment to our

second trade bank account below.

Beneficiary name: HB BODY

Bank Name: HALIFAX BANK PLC

A/C Number: 00664536

Sort Code: 11-05-20

IBAN: GB64HLFX11052000664536

BIC: HLFXGB21E26

please cancel the payment and remake it with this bank

Mark as Unread K

Star L

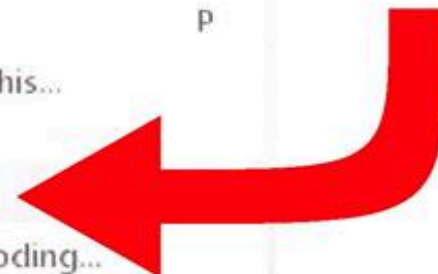
Block

Print P

Filter Emails Like This...

View Full Header

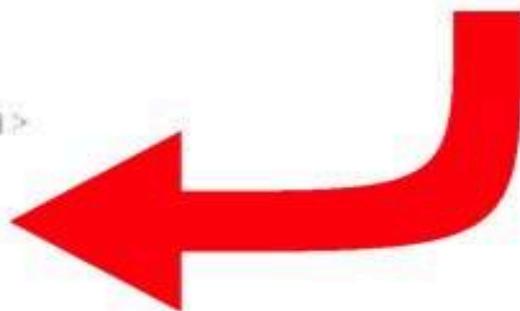
Set Language Encoding...



# Full Header



X-Originating-IP: [46.167.245.118]  
Authentication-Results: mta1036.mail.bf1.yahoo.com from=hbody.com;  
domainkeys=neutral (no sig); from=hbody.com; dkim=neutral (no sig)  
Received: from 127.0.0.1 (EHLO emkei.cz) (46.167.245.118)  
by mta1036.mail.bf1.yahoo.com with SMTP; Wed, 09 Dec 2015 12:50:04 +0000  
Received: by emkei.cz (Postfix, from userid 33)  
id AE454D581F; Wed, 9 Dec 2015 13:51:41 +0100 (CET)  
To: portacolors@yahoo.com  
Subject: The payment should now be made by another bank account  
From: "HBBODY S.A EXPORT DPT" <export@hbody.com>  
X-Priority: 3 (Normal)  
Importance: Normal  
Errors-To: export@hbody.com  
Reply-To: HBBODY S.A EXPORT DPT <expert@hbody.com>  
Content-Type: text/html; charset=utf-8  
Message-Id: <20151209125141.AE454D581F@emkei.cz>  
Date: Wed, 9 Dec 2015 13:51:41 +0100 (CET)  
Content-Length: 781



OK

# FAKE MAILER

Select Language ▼



2k

Like

Share

Tweet

247

G+

## EMKEE'S MAILER

Free online fake mailer with attachments, encryption, HTML editor and advanced settings...

From Name:

From E-mail:

To:

Subject:

Attachment:  No file chosen

Attach another file

Content-Type:  text/plain  text/html  Editor

Text:

**IMPORTANT!**



A close-up photograph of a person's hand holding a white rectangular sign. The person is wearing a dark suit jacket, a light-colored shirt, and a striped tie. The background is a blurred office setting with a light blue wall. The sign contains the text 'Grazie' and 'Thank you' in a bold, black, sans-serif font.

**Grazie  
Thank you**

**Contact:**

Email: [besnik.limaj@encysec.eu](mailto:besnik.limaj@encysec.eu)

Web: [www.encysec.eu](http://www.encysec.eu)