Polizia di Stato

Prevenzione e contrasto alle aggressioni ai servizi di home banking e monetica: OF2CEN, una *best practice* italiana

BANCHE E SICUREZZA 2016

Direttore Tecnico Principale
Dott. Francesco TAVERNA
Servizio Polizia Postale e delle Comunicazioni

Milano, 26 maggio 2016

CHI SIAMO

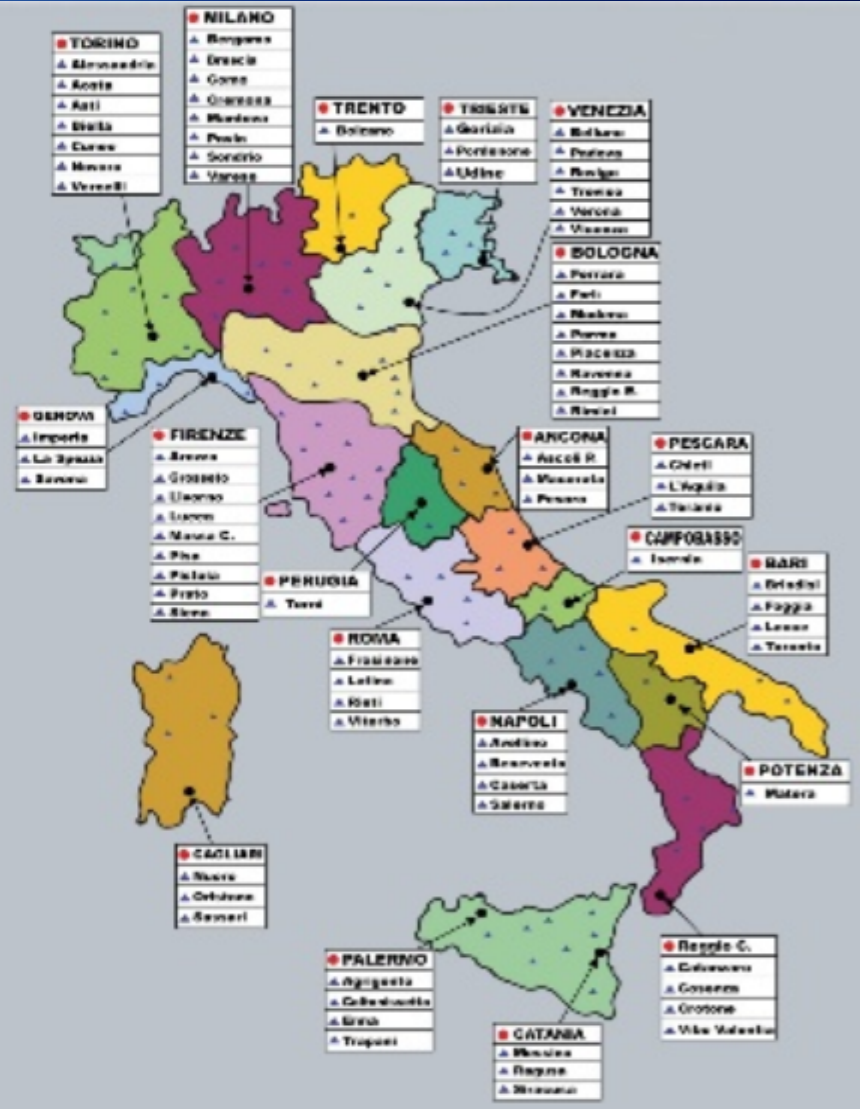
La Polizia Postale e delle Comunicazioni è un **settore specialistico** della Polizia di Stato nato per **prevenire e contrastare la criminalità informatica**, a garanzia dei valori costituzionali della segretezza della corrispondenza e della libertà di ogni forma di comunicazione.

LA STRUTTURA

Servizio Centrale

20 *Compartimenti regionali*

80 *Sezioni provinciali*



Compartimenti Polizia Postale

Sezioni della Polizia Postale

AMBITI

- **Pedopornografia**
- **Cyberterrorismo**
- **Hacking e Protezione Infrastrutture Critiche**
- **Financial cyber-crime**
- Copyright e E-commerce
- Giochi e scommesse on-line
- Tutela dei servizi postali e di telecomunicazione
- Analisi criminologica dei fenomeni emergenti

FCU

All’interno del Servizio di Polizia Postale e delle Comunicazioni è attiva l’**unità per il contrasto al crimine informatico di tipo finanziario** (FCU, Financial Cyber-crime Unit).

L’unità coordina a livello nazionale le indagini in materia di **home banking e monetica**, interfacciandosi con il Servizio di Cooperazione Internazionale di Polizia (SCIP) per le questioni transnazionali.

OPERAZIONE TRIANGLE

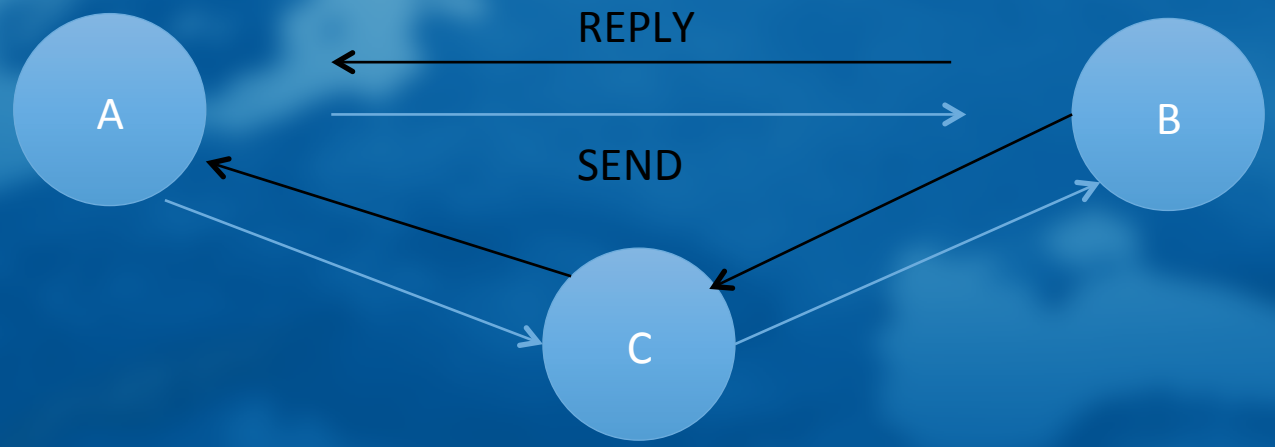
Nel giugno 2015 la Polizia Postale ha sgominato un'associazione per delinquere, a carattere transnazionale, i cui sodali utilizzavano la tecnica MITM per girare fraudolentemente ingenti somme di denaro da conti correnti bancari di soggetti vittime a conti correnti di destinazione, intestati a membri dell'organizzazione (in gergo chiamati «muli»).

TRIANGLE: Richiama il modus operandi, ma anche la cooperazione Italia-LEAs (Spagna tra tutte) per il tramite di Europol

SOCIAL ENGINEERING

Man In The Middle

L'*hacker* apprende che è in essere una corrispondenza elettronica di carattere commerciale tra due utenze, e si intromette nella comunicazione osservando, intercettando o replicando verso un'altra destinazione prestabilita, i messaggi inviati dai due interlocutori.



SOCIAL ENGINEERING

Man In The Middle (fase 1)

info@dittaA.com

info@dittaB.com

Alice
Buyer

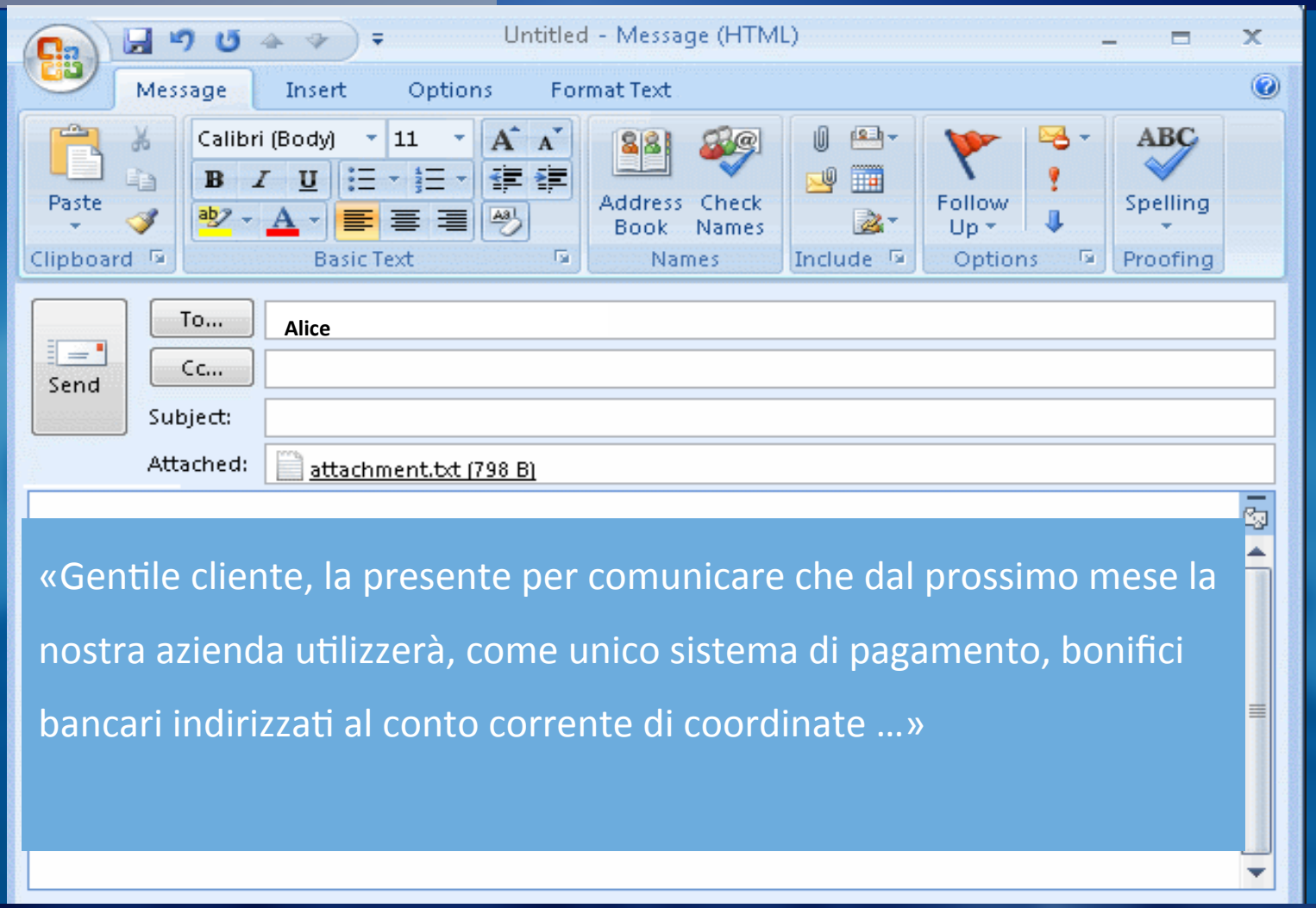
Bob
Seller

Hi! I'm Bob! My email has changed: dittaB@email.com

Hi! I'm Alice! My email has changed: dittaA@email.com

SOCIAL ENGINEERING

Man In The Middle (fase 2)



FCU
Attività investigative

Investigazioni tradizionali

1. Identificazione degli intestatari dei conti beneficiari e sequestro degli stessi, eventualmente avvalendosi del J-CAT (Joint-Cybercrime Action Taskforce) presso EC3 (Europol).
2. Intercettazioni telefoniche
3. Perquisizioni locali e personali
4. Ricostruzione del flusso del denaro (anche per le monete virtuali)

FCU
Attività investigative

Investigazioni informatiche

1. Analisi forense dei dispositivi che hanno subito l'attacco o da cui è partito l'attacco (estrazione ed analisi del *sample* del *malware* utilizzato, analisi degli *header* dei messaggi, …)
2. Intercettazioni telematiche passive (es. tramite duplicazione delle caselle di posta) o attive (tramite inoculazione di malware)
3. Convenzione con soggetti finanziari (banche, issuer, acquirer…) per lo scambio dei dati
4. Alimentazione del **DB OF2CEN**

OF2CEN

«On-line Frauds Cyber Centre and Expert Network» è un progetto nato per il contrasto al fenomeno del *phishing*

- **Piattaforma di condivisione di informazioni tra la Polizia e le Banche**
- **Interventi tempestivi per blocco conti-correnti e carte in frode**
- **Recupero somme frodate**
- **Inserimento in black-list degli indirizzi IP e degli account dei phisher**
- **Analisi statistica del fenomeno**

OF2CEN
Privacy

- Le banche hanno accesso a una vista del DB generale, dove sono mascherate le origini delle transazioni fraudolente.
- I dati vengono utilizzati per implementare i sistemi antifrode.
- E’ in corso di sviluppo il sistema che consente la comunicazione diretta tra sistemi antifrode e OF2CEN (tramite web service)

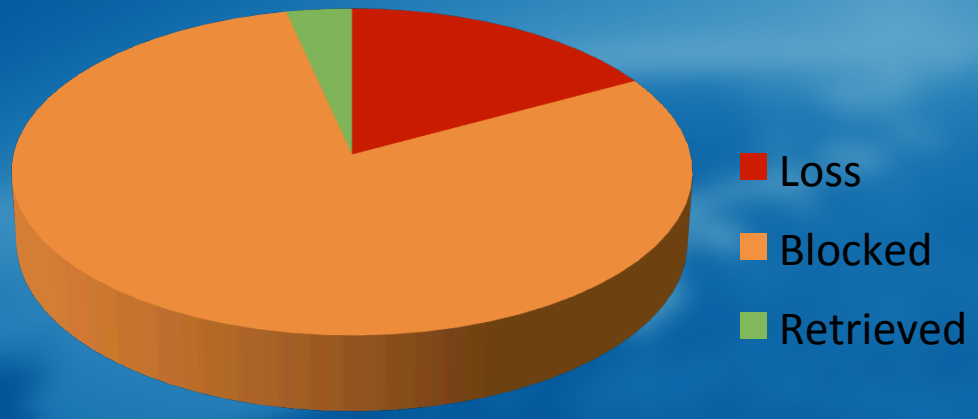
OF2CEN
Volumi

ANNO	VOLUME IMPORTI	TRANSAZIONI TOTALI	GRUPPI BANCARI SEGNALANTI
2014	35.683.821,76	3300	9
2015	51.517.740,37	6214	10

OF2CEN

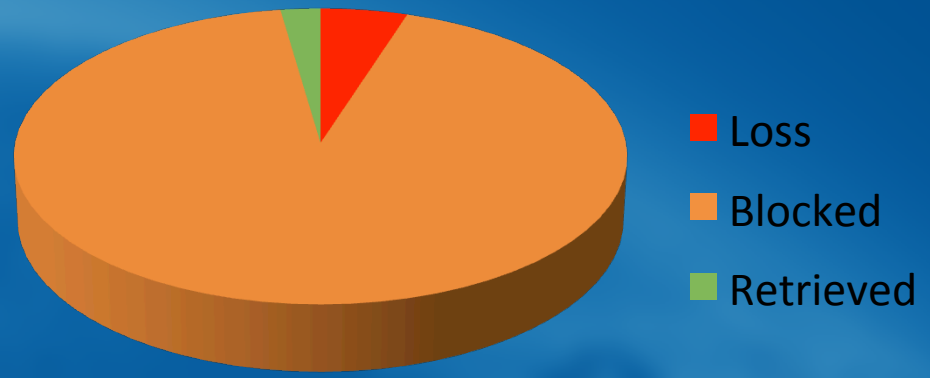
Risultati

2014



LOSS ≈ 15 %

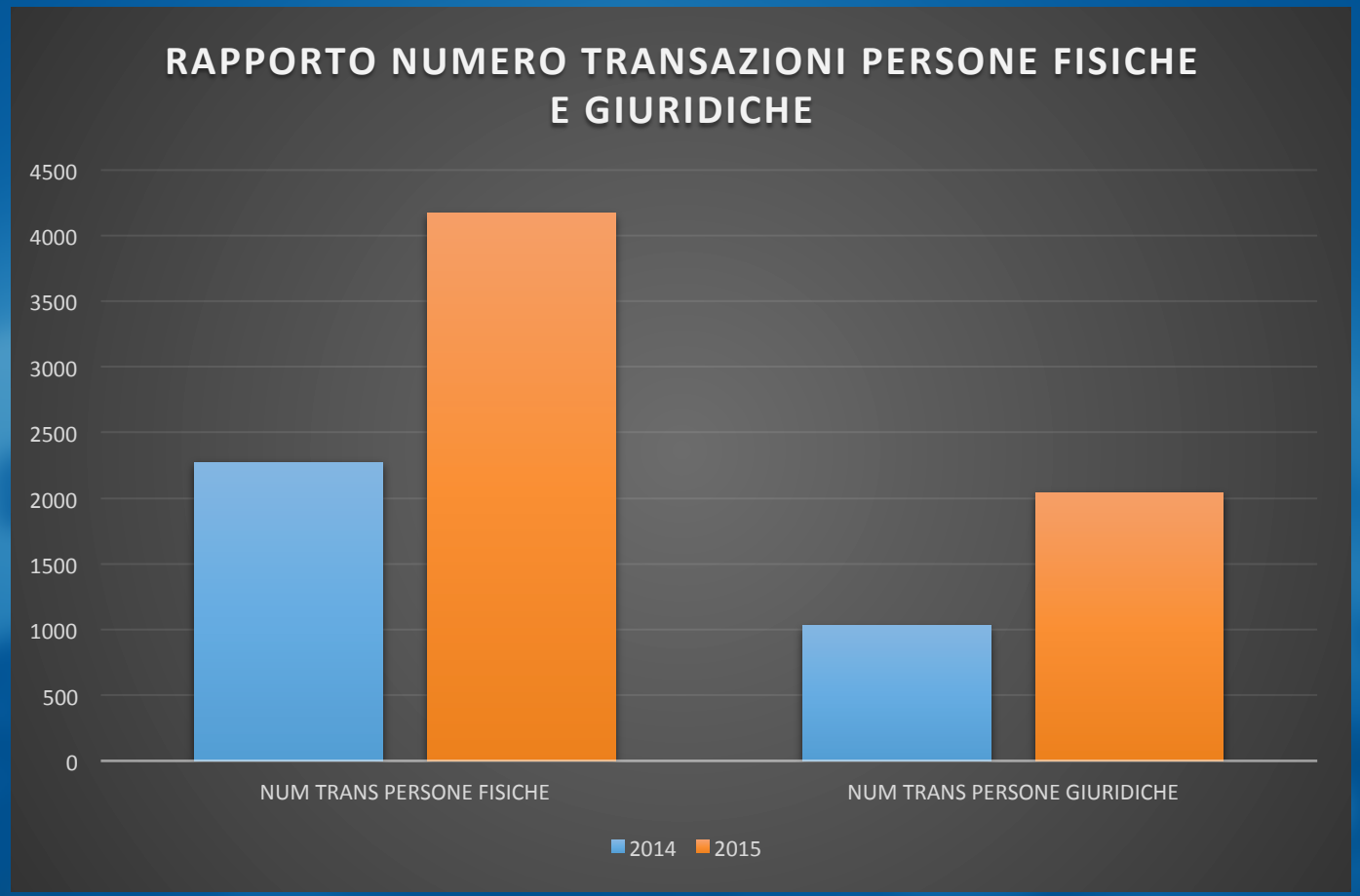
2015



LOSS ≈ 5 %

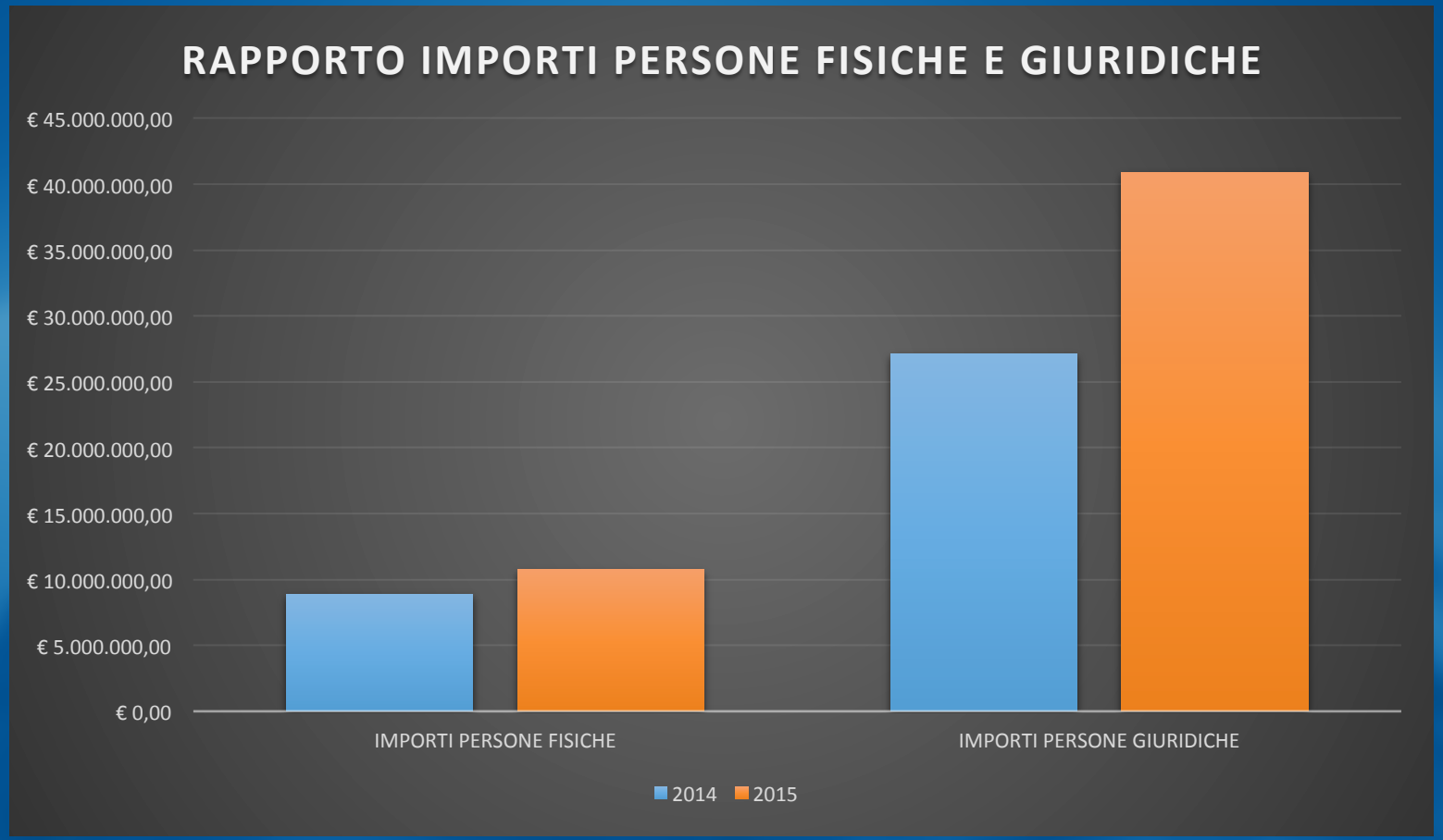
OF2CEN

Risultati



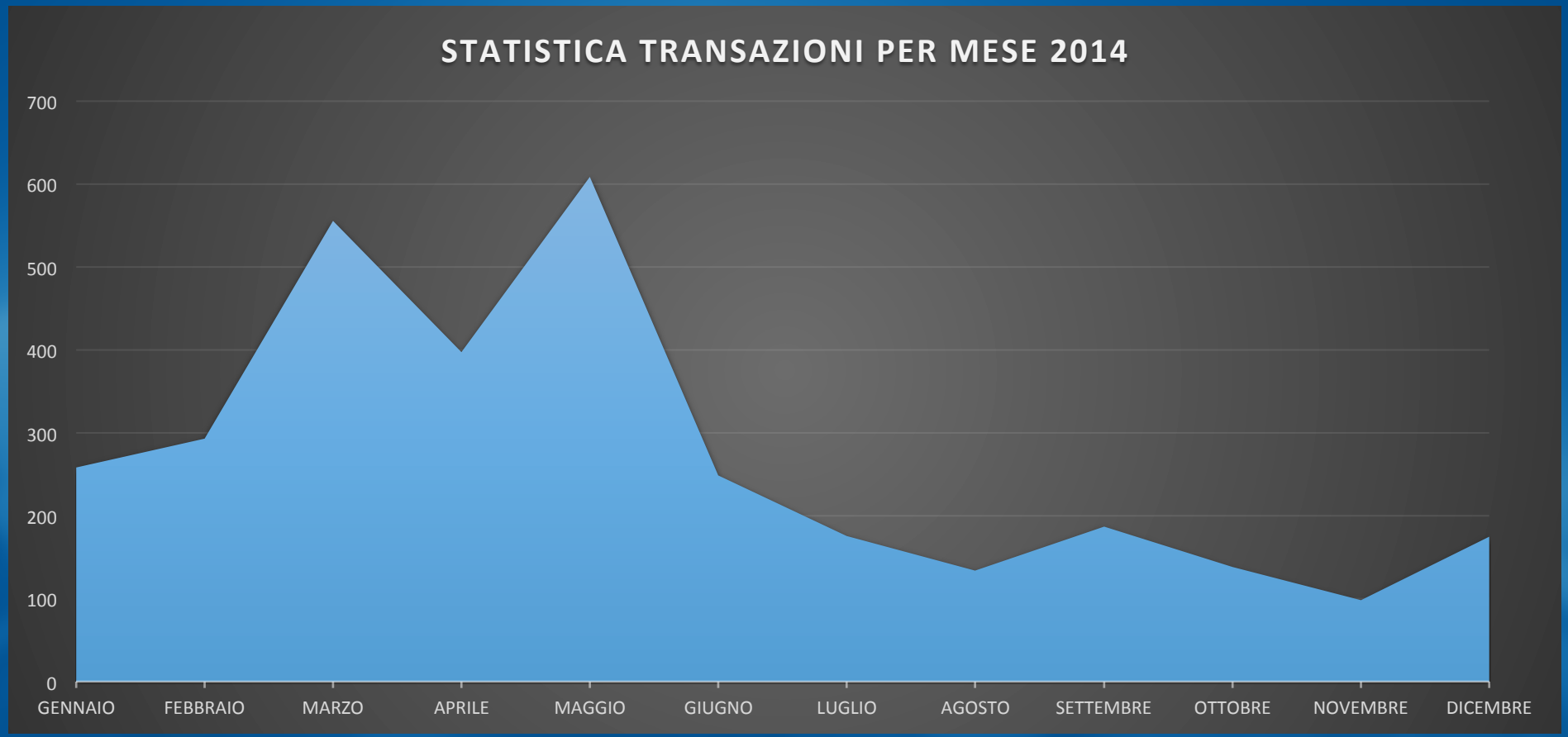
OF2CEN

Risultati



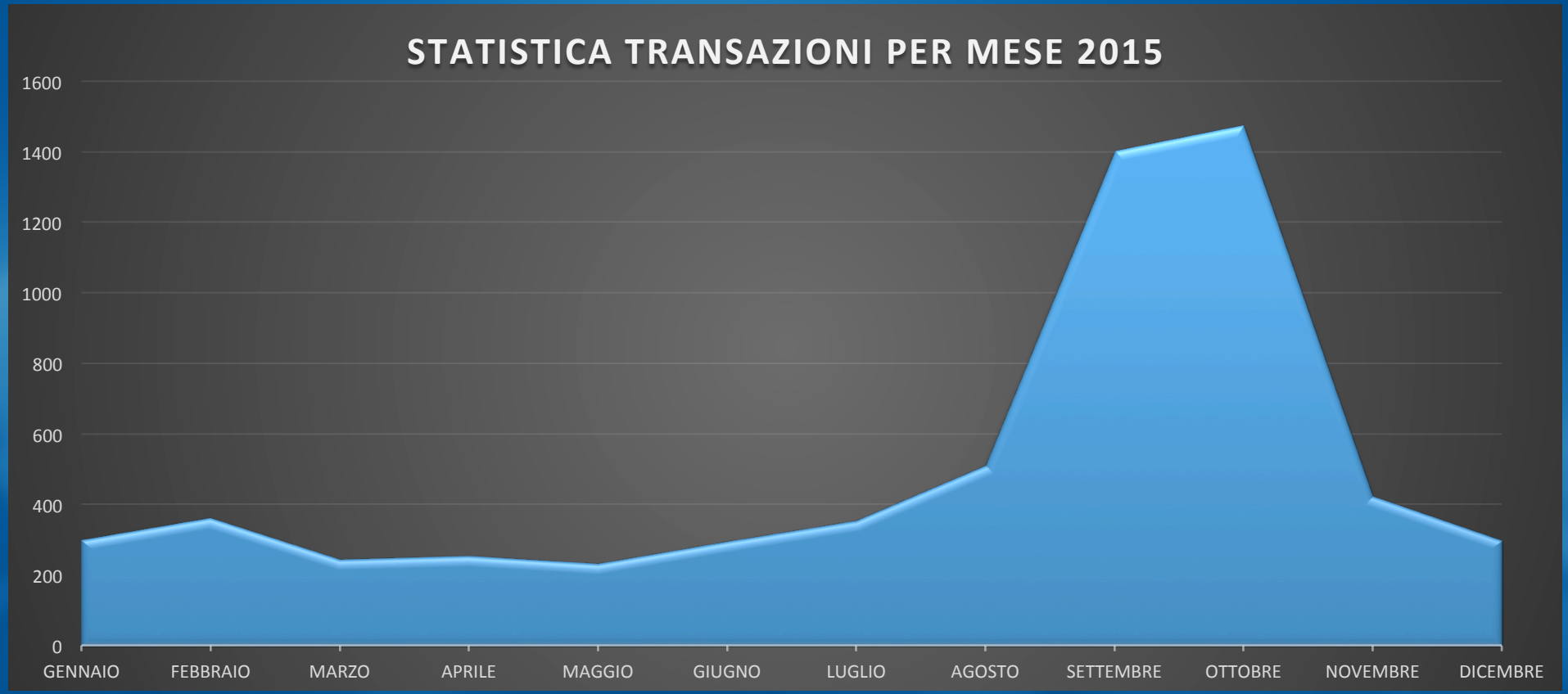
OF2CEN

Risultati



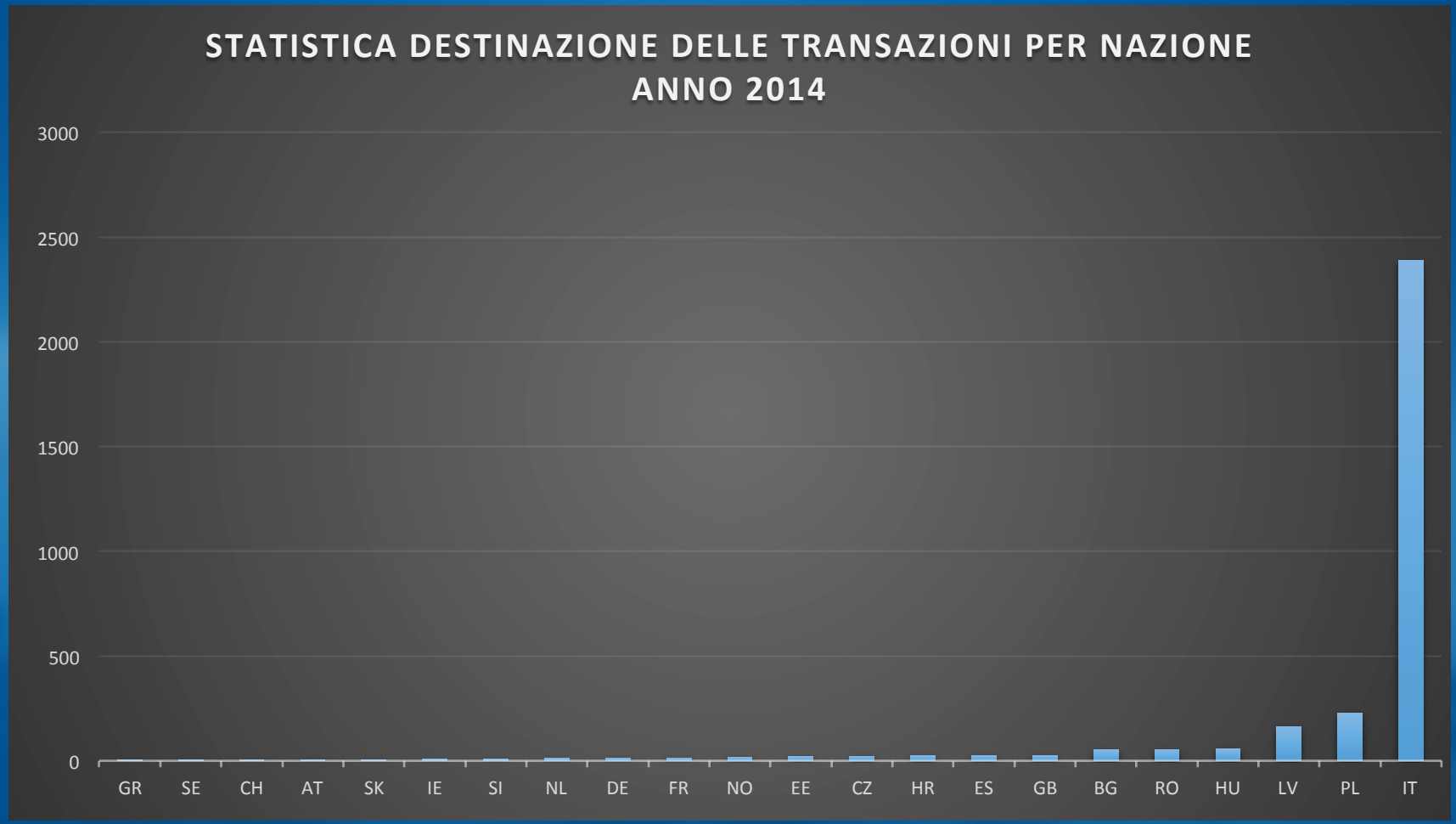
OF2CEN

Risultati



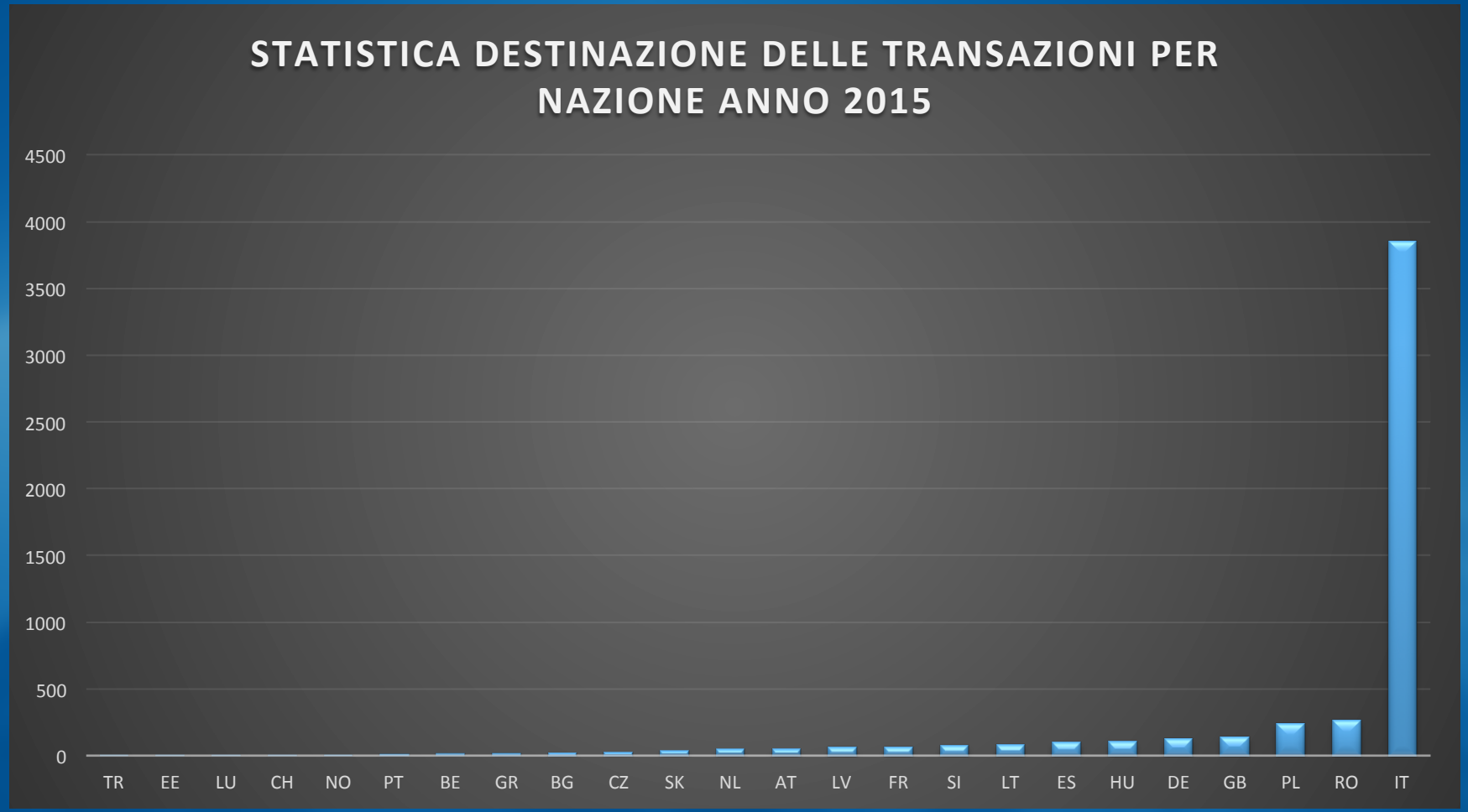
OF2CEN

Risultati



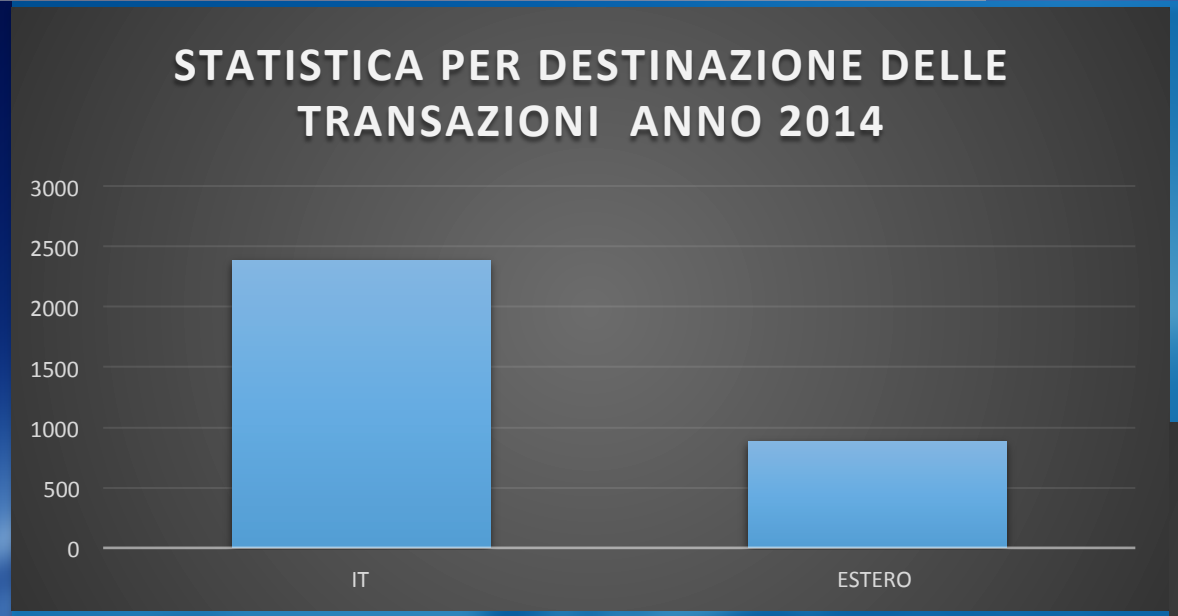
OF2CEN

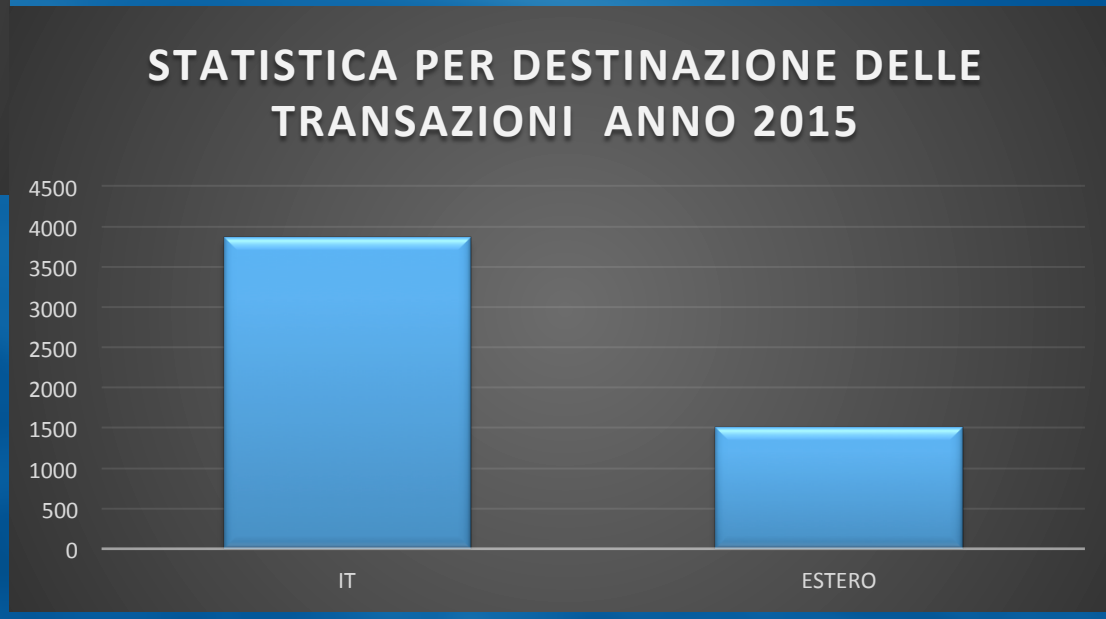
Risultati



OF2CEN

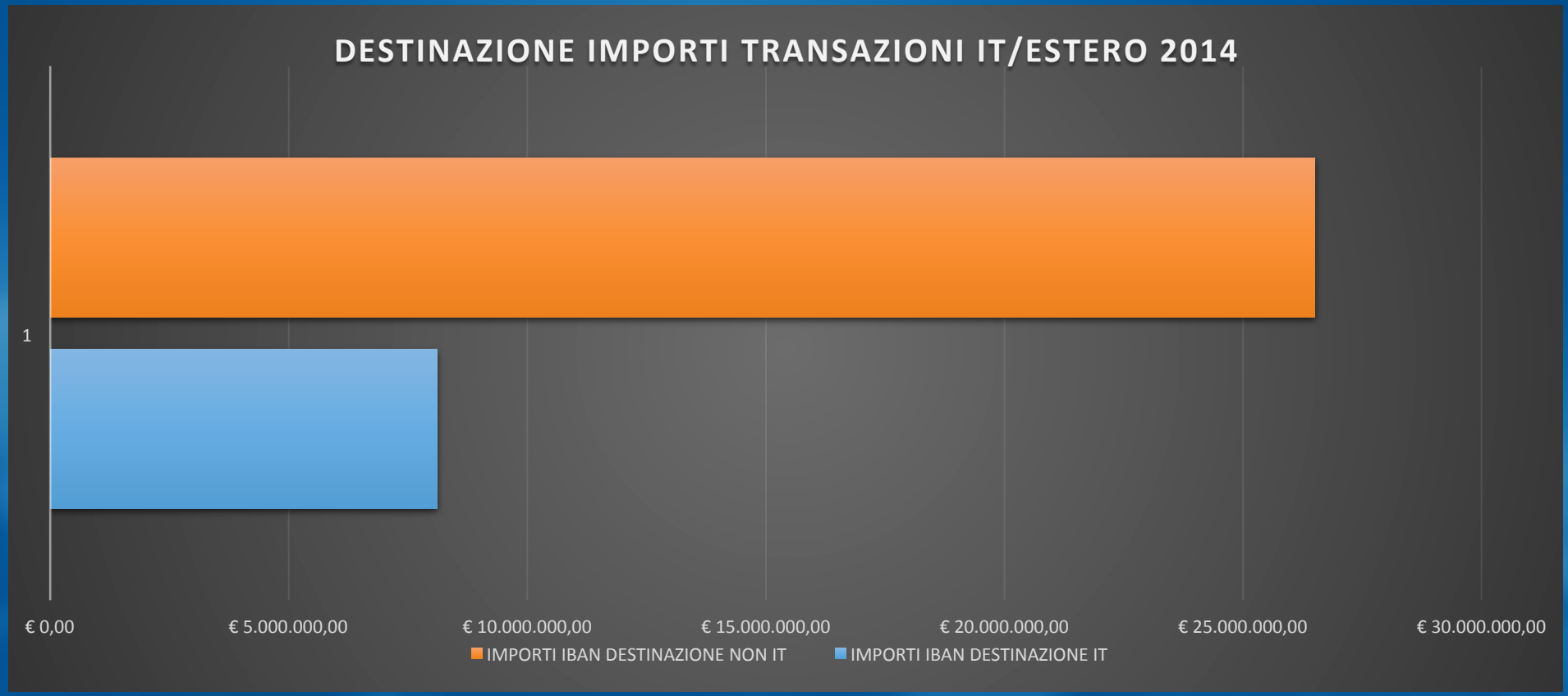
Risultati





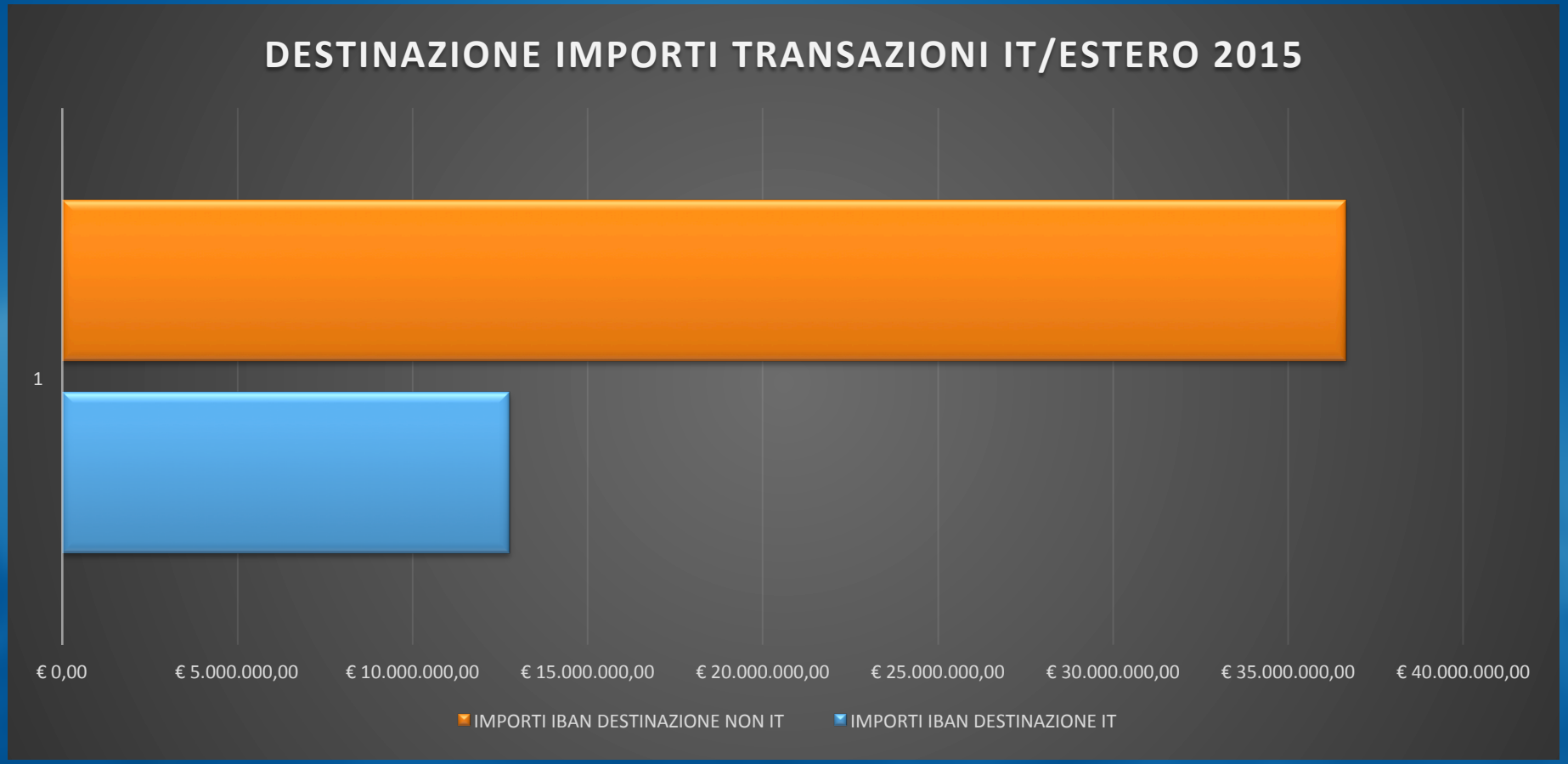
OF2CEN

Risultati



OF2CEN

Risultati



EU OF2CEN
Obiettivi

Operational aims are to:

- Detect and block in real time fraudulent transactions affecting banks throughout Europe.
- Identify criminal groups operating at a European level.

Strategic aims are to:

- Provide LEAs with up-to-date analysis about new modus operandi and trends on financial cyber-crime attacks.
- Facilitate the adoption of common strategies against financial cyber-crime.

EU OF2CEN

Il consorzio

CO - BENEFICIARIES	CO - PARTNERS
Italian Police	EC3-EUROPOL
ABI Lab	EBF
Intellium	Intesa Sanpaolo
Uni-Modena	UniCredit
Uni-Trento	
Poste Italiane Spa	
Hungarian Police	
French Police	
Spanish Police	
SIA Spa	

EU OF2CEN
Il consorzio

- ***LEAs*** ***(Italy, Hungary, France and Spain)*** shall share information with national banks, other EU LEAs and Europol/EC3.
- ***Banks*** ***(Intesa Sanpaolo, UniCredit and Poste Italiane)*** shall contribute with fraud expertise, market knowledge and banking experience and provide feedback on the deployment of the Information Sharing Platform.
- ***Banking Associations*** ***(ABI Lab, EBF)*** shall support the gathering/ analysis of info-sharing needs and expectations and support the dissemination.

EU OF2CEN
Il consorzio

- ***Private expert companies*** ***(Intellium, Poste Italiane Security Practice and SIA)*** shall help in research, analysis and event organization; support the design of the IT System.

- ***Universities*** ***(University of Modena-Reggio Emilia and University of Trento)*** shall develop the Information Sharing Platform.

EU OF2CEN
Il supporto di EBF

EBF will support the project Consortium:

- in the **dissemination and campaign phase**, by spreading and illustrating the main outcomes of the project
  - via the Cybersecurity Working Group
  - via other suitable meetings within EBF/ at EU level
- for **the promotion of the project**, given its central role in banking industry, in order to
  - involve the Banking Associations of the Member States already part of the project
  - engage other EU Member States
- to represent the **state-of-the-art** of the information sharing initiatives and PPPs already set in EU Member States, in order to create the appropriate framework for information sharing

EU OF2CEN

Il supporto di Europol

European Cybercrime Center of Europol, as a focal point in the EU's fight against cybercrime, will:

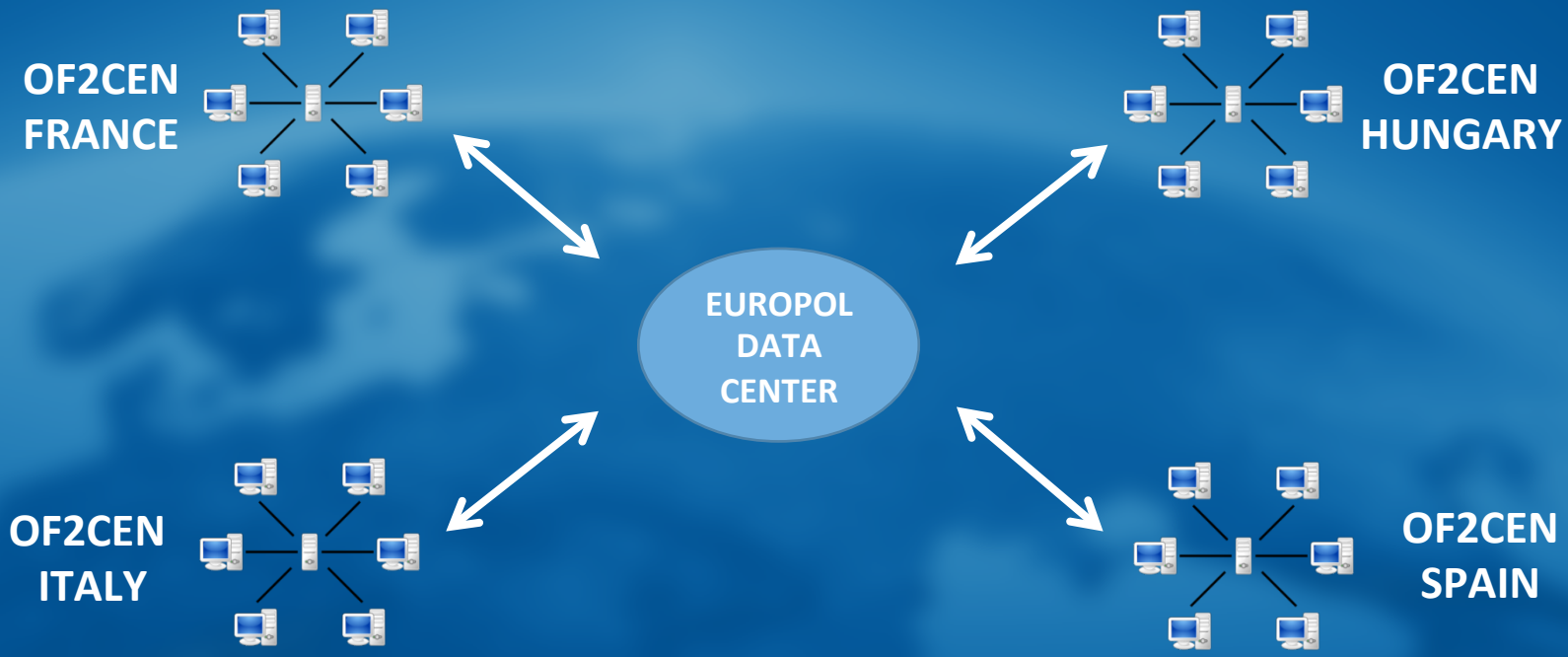
- **Help the engagement in the project** of Member States all around the Europe
- **Represent the pivot with EU LEAs** joining the project

Moreover, **Europol will benefit by an enhanced ability to identify new crime trends**

EU OF2CEN

La nuova topologia

Design a data center working as a hub, to be installed at Europol



Grazie per l’attenzione

Polizia di Stato

polizia delle comunicazioni