



Polizia di Stato

IL PROGETTO OF2CEN PER IL CONTRASTO ALLE FRODI ON-LINE

Direttore Tecnico Principale Ing. Francesco Taverna
(Servizio Polizia Postale e delle Comunicazioni - Roma)





CHI SIAMO

Polizia di Stato

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 POLIZIA POSTALE E DELLE COMUNICAZIONI

Servizio Centrale

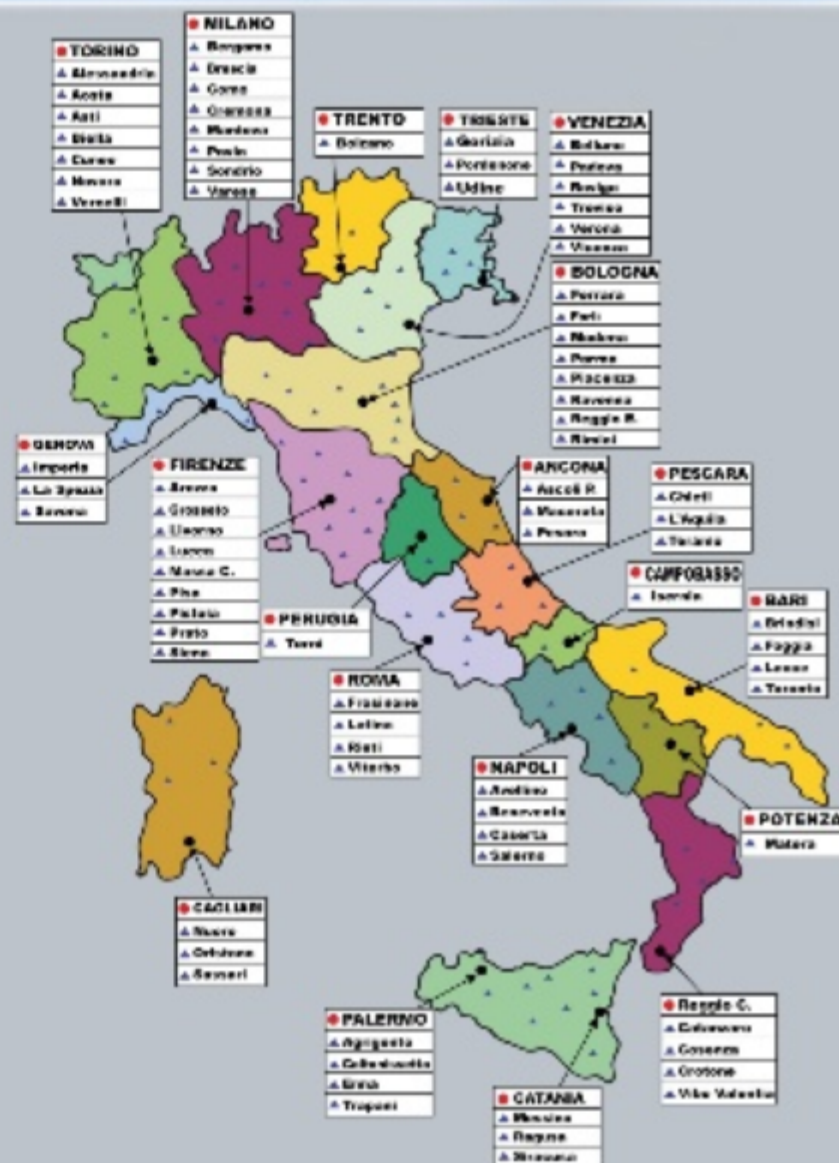
20 Compartimenti regionali

80 Sezioni provinciali



 Compartimenti Polizia Postale

 Sezioni della Polizia Postale





DI COSA CI OCCUPIAMO

Polizia di Stato

- Pedopornografia
- *Cyberterrorismo*
- *Copyright*
- *Hacking* e Protezione Infrastrutture Critiche
- *Frodi on-line (e-Banking/e-Commerce)*
- Giochi e scommesse *on-line*
- Tutela dei servizi postali e di telecomunicazione
- Analisi criminologica dei fenomeni emergenti





IL SERVIZIO CENTRALE

Polizia di Stato

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)**.





AMBITI DI INTERVENTO

Polizia di Stato

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





ATTIVITA' INVESTIGATIVE

Polizia di Stato

- **Investigazioni tradizionali**

1. Identificazione degli intestatari dei conti beneficiari e sequestro degli stessi, eventualmente avvalendosi del **J-CAT** (EC3 Europol).
2. Intercettazioni telefoniche
3. Perquisizioni locali e personali



ATTIVITA' INVESTIGATIVE

Polizia di Stato

- **Investigazioni informatiche**

1. Analisi forense dei dispositivi attaccati (rilevamento dell'eventuale *malware* utilizzato, analisi degli *header* dei messaggi, ...)
2. Intercettazioni telematiche (duplicazione o sequestro delle caselle di posta, inoculazione da remoto di *trojan horse*...)
3. Interrogazione del DB **OF2CEN**





IL PROGETTO OF2CEN PER IL CONTRASTO AL PHISHING

Polizia di Stato

OF2CEN

ONLINE FRAUDS CYBER CENTRE AND EXPERT NETWORK





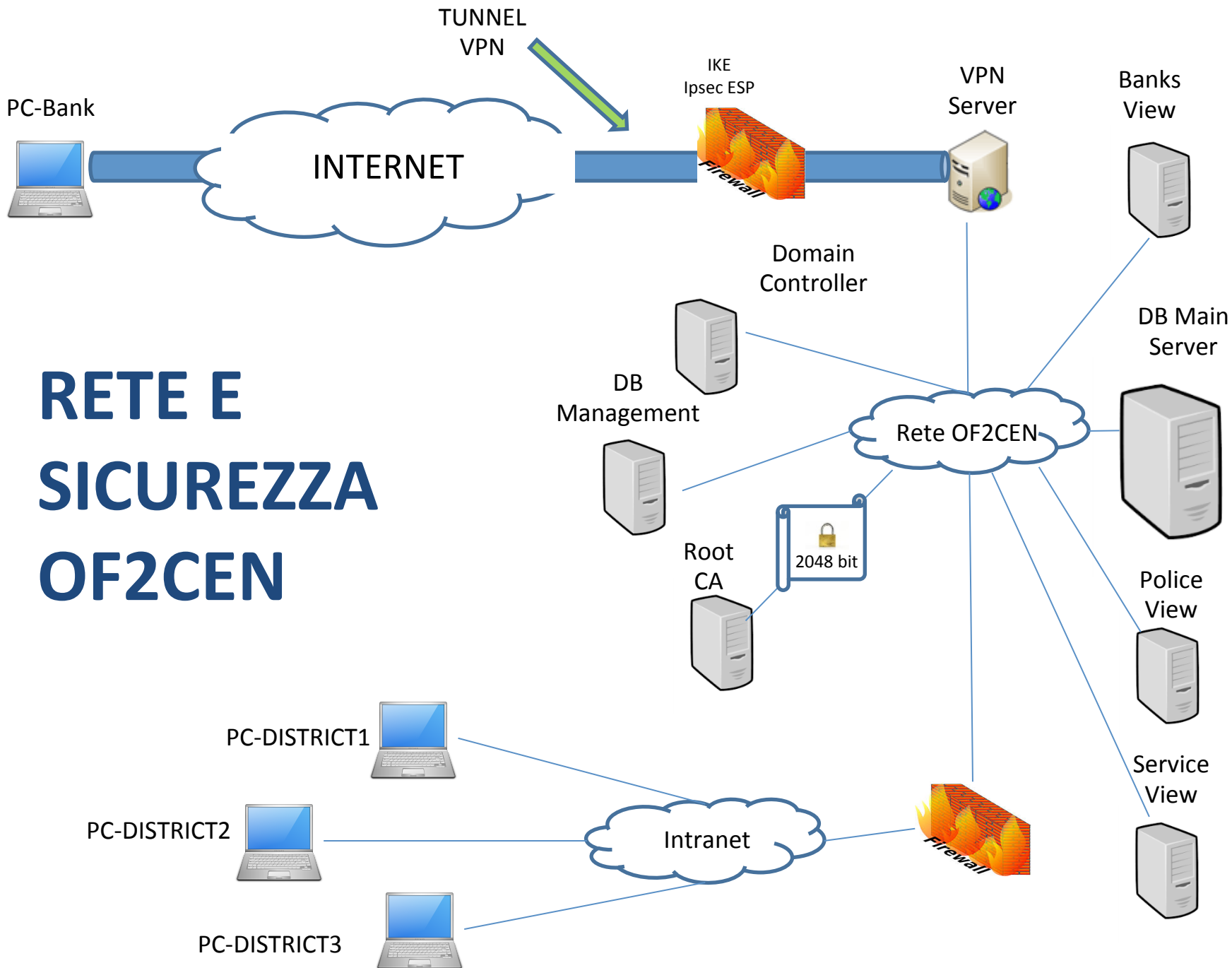
OF2CEN

Polizia di Stato

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

- *Piattaforma di condivisione di informazioni tra la Polizia Postale 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 IBAN dei phisher*
- *Analisi statistica del fenomeno*







PROBLEMI DI PRIVACY

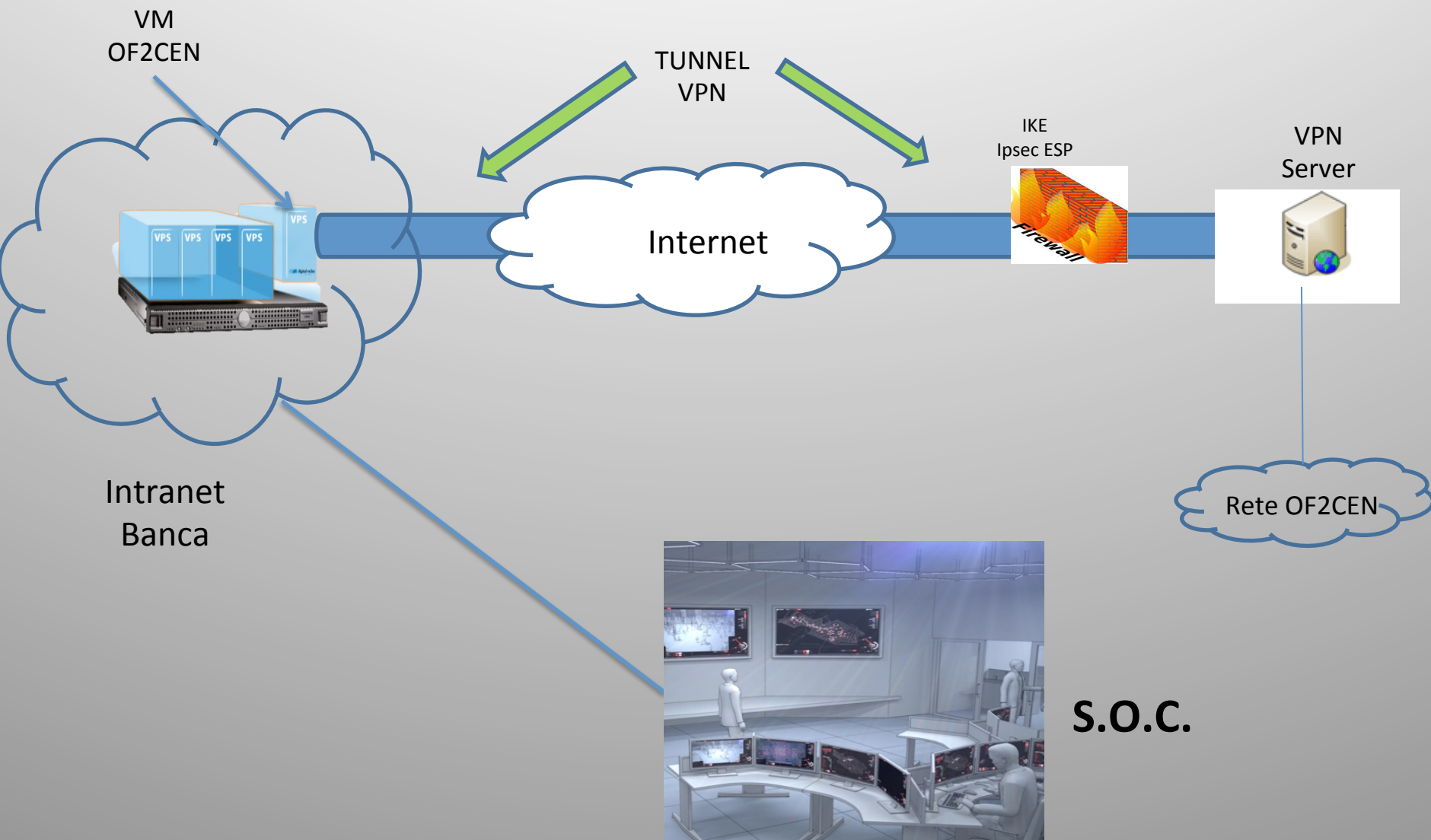
Polizia di Stato

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.



NUOVO COLLEGAMENTO BANCHE



OF2CEN POLIZIA

OF2CEN

Rapporti

Transazioni

IP Sospetti

Siti Clone

News

Numeri Utili

File Utili

Accedi

Q Campi di ricerca impostati :

Numero totale di Righe : **10500**

Righe per pagina

10

Cerca Tra :

Tutte le transazioni

Pagine

1 2 3 4 5 6 7 8 9 10 ...



Origine



Destinazione



Dati Transazione



Dati Polizia

Q Cerca

Esporta

	Codice	Nominativo Origine	Rapporto Origine	Nominativo Destinazione	Rapporto Destinazione	Importo	IP	Esito	Data Disposizione	Data Inserimento
▼	12752	marco	IT74Q0306984561015280	Stefano	IT74Q0306984561015280	€ 5.346,55	45.54	Avvenuto	18/03/2015 00:00:00	26/03/2015 11:05:37
▼	12751	Stefano	IT98Z0306967684510321	Marco	IT98Z0306967684510321	€ 7.676,65	54.54	Avvenuto	03/03/2015 01:30:00	26/03/2015 11:00:23
▼	12750	Stefano	IT42M0306903353018050	Veronica Claudia	IT98Z0306967684510321	€ 456,54	54.53	Avvenuto	02/03/2015 01:30:00	26/03/2015 10:56:22
▼	12748	Stefano	IT74Q0306984561015280	Marco	IT29A01030402300000006	€ 120,00	12.12	Avvenuto	13/02/2015 12:33:00	13/02/2015 16:37:45
▼	12749	Stefano	IT74Q0306984561015280	Marco	IT41E030695613468	€ 123,00	12.12	Avvenuto	13/02/2015 12:22:00	13/02/2015 16:41:32
▼	12744	VERONICA MATTEO	IT29A01030402300000006	AILTON	PT5000380000395414957	€ 123,00	151.66	Avvenuto	18/02/2014 23:33:00	18/02/2014 11:05:37
▼	12746	VERONICA MATTEO	IT29A01030402300000006	AILTON	IT24W0306967684510321	€ 20.000,00	151.66	Avvenuto	18/02/2014 11:11:00	18/02/2014 11:14:14



OF2CEN POLIZIA

Polizia di Stato

DETTAGLI RAPPORTO

OF2CEN Rapporti Transazioni IP Sospetti Siti Clone News Numeri Utili File Utili [Accedi](#)

Banca: Tutte le Banche Nazione: Tutte le Nazioni

Rapporto: IT74Q03069845610152804 Origine ☒ Destinazione ☒ [Cerca](#)

Inizio Precedente Prossima Ultima

IT74Q03069845610152804

Destinatario 2 **Origine 5**

🏦 Banca: INTESA SANPAOLO SPA
🏠 Filiale: COMIT - MILANO-METANOPOLI
📄 ABI: 03069
📄 CAB: 84561

[Info](#) [Transazioni](#)

Info

IT74Q03069845610152804

2 Transazioni in cui è destinazione

€ 10.693,10 Importo tot. Ricevuto

5 Transazioni in cui è Origine

€ 13.924,10 Importo tot. Inviato

[Close](#)



OF2CEN

Queries possibili: per origine, destinazione, transazione o MIPG (collegamento con il DB dei fascicoli di PG della Polizia di Stato)

OF2CEN Rapporti Transazioni IP Sospetti Siti Clone News Numeri Utili File Utili Accedi

Campi di ricerca impostati: marco

Numero totale di Righe : 1 Righe per pagina: 10 Cerca Tra : Tutte le transazioni

Origine

Nominativo di Origine: marco

Rapporto di Origine:

Codice Fiscale di Origine:

Partita Iva di Origine:

Destinazione

Nominativo di Destinazione:

Rapporto di Destinazione:

Dati Transazione

Codice:

Importo:

Data Dal:

Data Al:

IP Disposizione:

Dati Polizia

MIPG:

Anno:

Provincia:

Numero:

Cerca Esporta

Codice	Nominativo Origine	Rapporto Origine	Nominativo Destinazione	Rapporto Destinazione	Importo	IP	Esito	Data Disposizione	Data Inserimento
12752	marco	015280440178	Stefano	IT74Q0306984	€ 5.346,55	45.5	Avvenuto	18/03/2015 00:00:00	26/03/2015 11:05:37

Ricerca in Origine
Ricerca in Destinazione
Entra nel dettaglio
Informazioni Veloci



OF2CEN E MIPG



OF2CEN

Inserimento Manuale (tipico dei Compartimenti)

OF2CEN Rapporti Transazioni IP Sospetti Siti Clone News Numeri Utili File Utili Accedi

Transazioni fraudolente

Segnalazione Banca Selezione una banca
BANCA COMMERCIALE ROMANA

Origine
Persona Fisica Prova Cliente *
Codice Fiscale
IBAN IT72B6410157725612948013920 *

Destinazione
Persona Fisica Phisher *
Codice Fiscale
IBAN IT87Z7065329705095699292610 *

Transazione
RIF Transazione
IP
Importo € 0
Importo Bloccato € 0
Importo Sornato € 0
Data disposizione dd/mm/yyyy hh:mm:ss
Esito AVVENUTO

Prova Cliente Nominativo nuovo
IT72B6410157725612948013920 IBAN Corretto
Nazione : Italia
Banca : ND
Filiale : ND

Phisher Nominativo nuovo
IT87Z7065329705095699292610 IBAN Corretto
Nazione : Italia
Banca : ND
Filiale : ND

Salva

OF2CEN

Interrogazione del DB dei BIN delle carte di credito

OF2CEN Rapporti Transazioni P Sospetti Siti Clone News Numeri Utili File Utili

Transazioni fraudolente

Denuncia Utente

Origine

Persona Fisica Roberto Marchesi

Codice Fiscale RBRMCH75E02H501T

CC 4556570627016407

Destinazione

Persona Fisica Kuzma Istomin

Codice Fiscale

IBAN SI18292725993489076

Transazione

RIF Transazione RT48613121

IP 58 48 47 11

Importo 1500 25

Importo Bloccato € 0

Importo Stornato € 0

Data disposizione 05/05/2015 11:00:00

Esito AVVENUTO

Salva

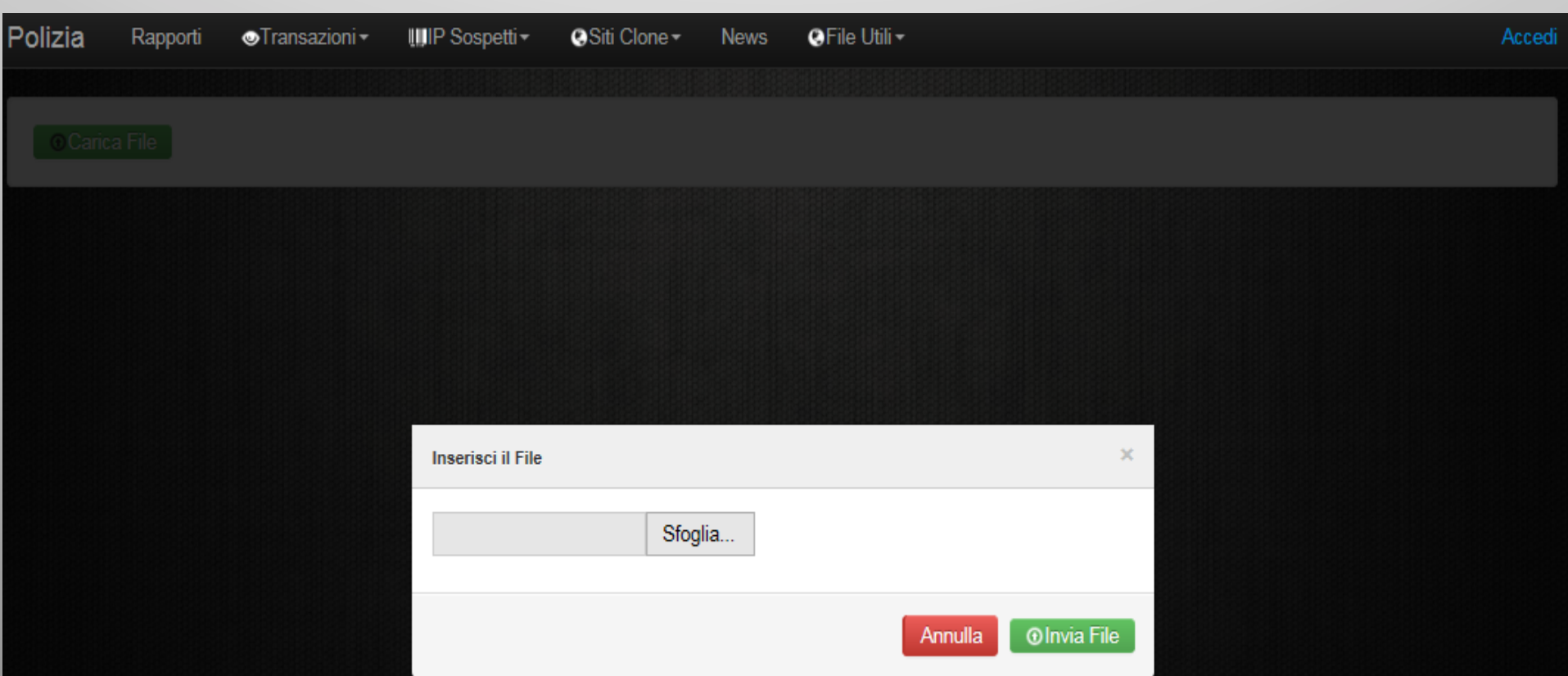
Roberto Marchesi Nominativo nuovo
RBRMCH75E02H501T Codice fiscale errato
4556570627016407 Numero di CC corretto
ICBA Bancard (USA)

Kuzma Istomin Nominativo nuovo
SI18292725993489076 IBAN Corretto
Nazione : Slovenia
Banca : ND
Filiale : NDFiliale : ND

OF2CEN

Inserimento Massivo tramite file (tipico delle banche):

- **.csv**
- **.json**



FORMATO CSV

NOME	TIPO	AMMETTE NULLI	DESCRIZIONE
source_type	int	NO	1 per valore persone Fisiche 0 per persone giuridiche
source_name	string	NO	nome e cognome dell'origine del bonifico, ragione sociale, se il tipo è 'persona giuridica'
source_type_account	int	NO	Tipologia di account del cliente formato. Indicare 1 per IBAN, 2 per Numero carte di Credito, 3 per conto Gioco, 4 per Altro
source_account	string	NO	Account del cliente frodato (es. l'IBAN se la frode riguarda l'home banking)
source_fiscale_code	string	SI	codice fiscale del cliente frodato, lasciare vuoto se non conosciuto
source_vat_number	string	SI	partita iva del cliente frodati, lasciare vuoto se non conosciuto
destination_type	int	NO	1 per valore persone Fisiche 0 per persone giuridiche
destination_name	string	NO	nome e cognome del destinatario della transazione, ragione sociale, se il tipo è 'persona giuridica'
destination_type_account	int		Tipologia di account del destinatario. Indicare 1 per IBAN, 2 per Carte di Credito, 3 per Ricarica Telefonica, 4 per Altro
destination_account	string	NO	Account del destinatario (es. l'IBAN se la frode riguarda l'home banking)
destination_fiscal_code	string	SI	codice fiscale del destinatario, lasciare vuoto se non conosciuto
destination_vat_number	string	SI	partita iva del destinatario, lasciare vuoto se non conosciuto
amount	money	NO	Importo in Euro, oggetto della transazione
amount_blocked	money	NO	Importo in Euro eventualmente bloccato (0,00 altrimenti)
amount_divert	money	NO	Importo in Euro eventualmente stornato (0,00 altrimenti)
date	string	NO	Data di disposizione nel formato dd/mm/yyyy
hour	string	SI	Ora della disposizione nel formato hh:mm:ss lasciare vuoto questo campo se questo valore non è conosciuto
outcome	int	NO	Esito della transazione, specificare 1 se la transazione è avvenuta, 2 per esito Incerto, 3 nel caso in cui la transazione sia stata bloccata.
ip	string	SI	Indirizzo IP da cui è stato disposto il pagamento, lasciare vuoto se non conosciuto
rif	string	NO	Transaction ID (vecchio CRO) della transazione.
not_completable	int	NO	Più assumere i valori 0 o 1. Con il valore 1 si indica che la transazione non è completabile, per cui non verrà proposta in seguito la modifica. Il valore 0 indica che tale comunicazione in futuro potrà essere integrata nei campi 'ip' e 'hour'. Nel caso in cui la transazione risulti già completa è possibile non specificare il

ESEMPIO DI JSON

```
[
{
  "source_type" : 1,
    "source_name" : "Mario Rossi",
    "source_type_account" : 1,
    "source_account" :
      "IT60X0542811101000000123456",
    "destination_type" : 1,
      "destination_name" : "Alen Becic",
      "destination_type_account" : 1,
      "destination_account" :
        "HR1210010051863000160",
        "amount" : "1542,50",
        "date" : "15/02/2015",
        "hour" : "15:10:50",
        "outcome" : 1,
        "ip" : "5.95.78.215",
        "rif" : "12345678901"
  }
]
```




OF2CEN

Inserimento degli IP statici sospetti in *black-list*

OF2CEN Rapporti Transazioni IP Sospetti Siti Clone News Numeri Utili File Utili [Accedi](#)

IP: Nazione: Provenienza della segnalazione: ☒ Transazione Fraudolenta ☒ Sito Clone ☒ IP Sospetto [Cerca](#)

Ultimo evento	IP Sospetto	Nazione		Azioni
10/03/2012 12:00	80.117.44.8		1 1	Azioni ▾
04/07/2013 07:46	79.6.138.14		2 2	Azioni ▾
12/04/2012 12:00	93.64.248.3		1 1	Azioni ▾
01/09/2012 04:17	164.132.109.76		1 1	Azioni ▾
23/04/2012 06:28	81.75.81.173		3 3	Azioni ▾
01/08/2013 10:43	82.186.31.210		1 1	Azioni ▾
19/09/2012 12:34	217.141.238.122		5 5	Azioni ▾
05/04/2012 12:00	95.237.134.209		1 1	Azioni ▾
31/07/2013 06:26	95.254.246.162		1 1	Azioni ▾
16/11/2012 06:53	2.226.116.144		1 1	Azioni ▾

1 2 3 4 5 6 7 8 9 10 ...



OF2CEN

Risoluzione e geo-localizzazione degli IP sospetti

82.186.31.210

Geolocalize

Resolve IP

View map

Country code	State code	State	City	ZIP	Latitude	Longitude
Rev 1: IT	09	Lombardia	Cernusco Sul Naviglio	20063	45.526600	9.332400
Latitude 45.526600		Longitude 9.332400				

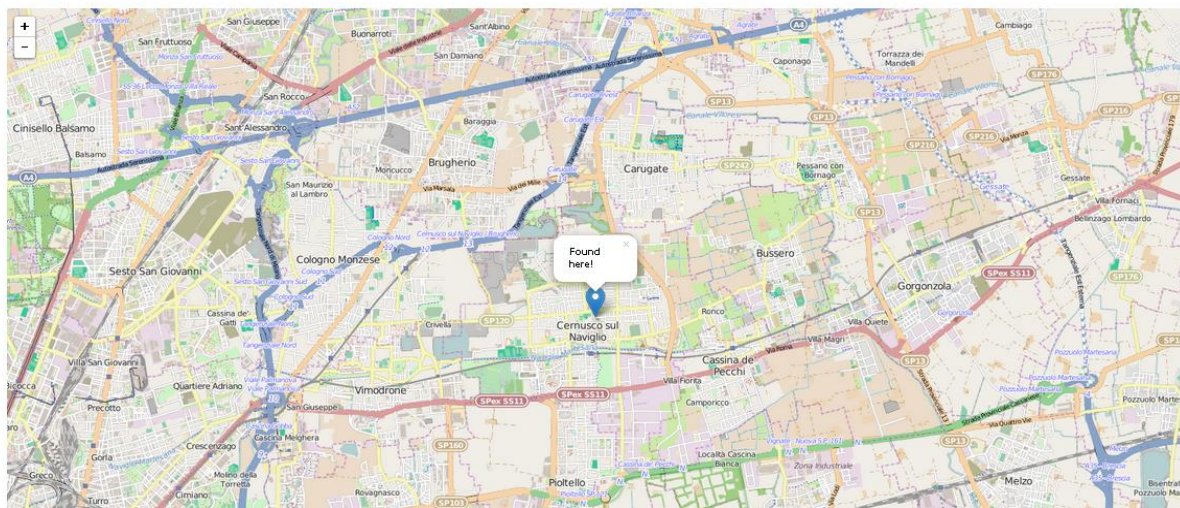
```
* This is the RIPE Database query service.
* The objects are in RPSL format.
*
* The RIPE Database is subject to Terms and Conditions.
* See http://www.ripe.net/db/support/db-terms-conditions.pdf
*
* Note: this output has been filtered.
* To receive output for a database update, use the "-B" flag.
*
* Information related to '82.186.31.208 - 82.186.31.223'
*
* Abuse contact for '82.186.31.208 - 82.186.31.223' is
* 'abuse@business.telecomitalia.it'
*
inetnum:      82.186.31.208 - 82.186.31.223
netname:      COMIT MOTO SRL
descr:        COMIT MOTO SRL
country:      IT
admin-c:      UF2089-RIPE
tech-c:       UF2090-RIPE
status:       ASSIGNED PA
mnt-by:       INTER-MNT
source:       RIPE # Filtered

person:       VALERIA FERRARESE
address:      COMIT MOTO SRL
address:      VIA NAPOLEONA 10
address:      20100
address:      Italy
phone:        +390267505
```

Geo lookup

Intestatario

[Refresh](#)





OF2CEN

ONLINE FRAUD CYBER CENTRE AND EXPERT NETWORK

Gruppi bancari segnalanti	Transazioni segnalate	Somme BLOCCATE	Somme RECUPERATE
10	14986	58.267.838,63 €	2.234.269,31 €





SVILUPPI FUTURI

A livello europeo:

- costruire un quadro generale del trend sul cyber-crime a partire dalle analisi delle LEAs dei MSs
- ridurre il tempo necessario per rilevare e bloccare le transazioni fraudolente tra banche estere
- identificare gruppi criminali a carattere transnazionale
- anticipare l'azione di tali gruppi mettendo in campo una strategia comune di contromisure





ATTIVITA'

Polizia di Stato

- 1) Definizione di una PPP per la condivisione delle informazioni tra Banche e Polizie europee
- 2) Definizione di un modello di business che assicuri la self-sustainability del PPP nel medio e lungo periodo e la sua scalabilità ad altri settori o aree geografiche
- 3) Definizione di un quadro di governance per la protezione dei dati, i requisiti di sicurezza, le competenze e responsabilità, relative allo scambio di informazioni tra banche e EU LEAs





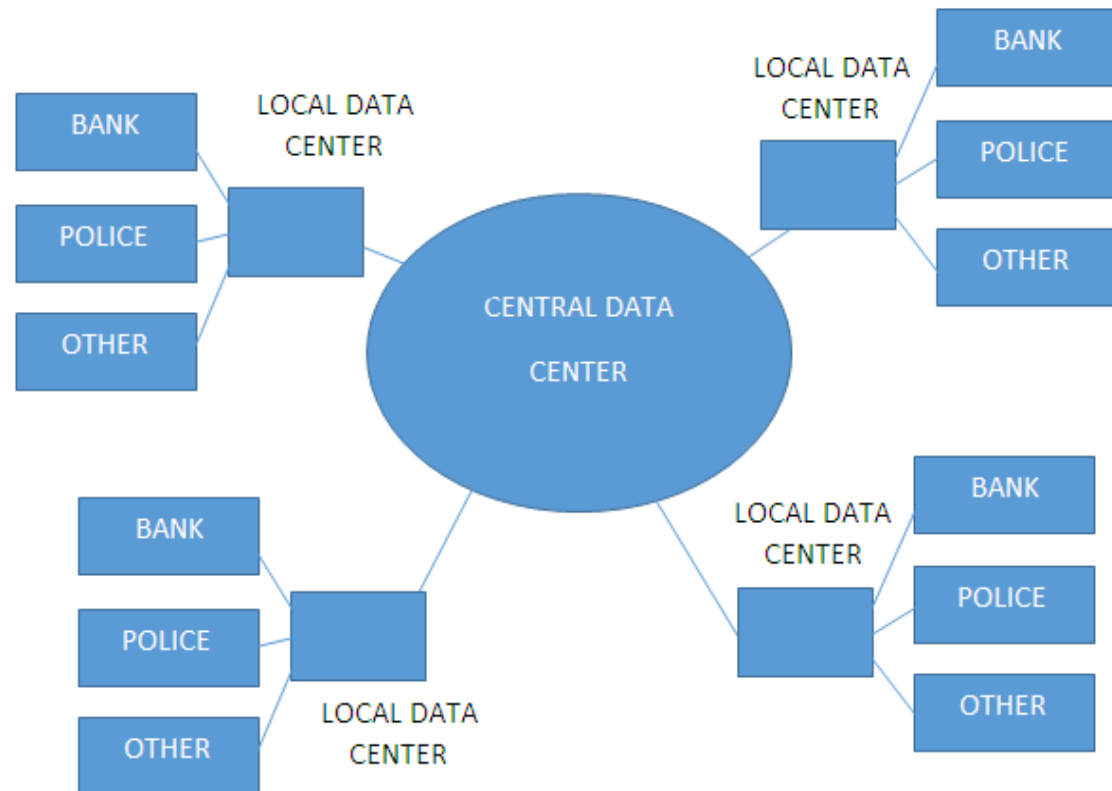
ATTIVITA'

- 4) Distribuzione dell'attuale piattaforma tra i Paesi aderenti, che la adegueranno per utilizzarla a livello Nazionale
- 5) Progettazione, sviluppo e diffusione della nuova piattaforma con le nuove caratteristiche
- 6) Integrazione tra la nuova piattaforma e le altre per lo scambio e l'analisi correlazionale dei dati
- 7) Realizzazione di un archivio centralizzato (*data center*) da installare preferibilmente presso sede Europol



EU OF2CEN

Tale archivio centralizzato verrà connesso a punti di distribuzione locali situati presso gli organi di Polizia degli stati membri, i quali si occuperanno di interfacciarsi con le banche nazionali aderenti, per la fruizione/erogazione dei servizi.





EU OF2CEN - BENEFICIARI

- A **breve termine**: LEAs e Banche aderenti per ciascun MS che potranno sfruttare la piattaforma esistente
- A **medio termine**: LEAs che si scambieranno i dati sulla base di un protocollo comune in attesa della messa in produzione dell'archivio centralizzato
- A **lungo termine**: tutte le LEAs e le Banche europee che beneficeranno della piattaforma integrata





EU OF2CEN - ATTORI

Polizia di Stato

CO - BENEFICIARIES	CO-PARTNERS
Polizia Postale	EC3-EUROPOL
Abi-Lab	EBF
Intellium	Banca Intesa San Paolo
Uni-Modena	Banca Unicredit
Uni-Trento	
Poste Italiane Spa	
Polizia Ungherese	
Polizia Francese	
Polizia Spagnola	
SIA Spa	





RISULTATI ATTESI

Polizia di Stato

1. EU OF2CEN sarà concepito e progettato **da e per** tutti i Paesi EU che si uniranno alla Partnership.
2. Auspicabilmente il successo dell'iniziativa sarà determinato dall'impegno reciproco in questa impresa comune.
3. Ogni Stato Membro aderente riceverà e condividerà informazioni strategiche sulle evoluzioni del *cyber-crime* finanziario in Europa e potrà adottare le contromisure che ritiene più opportune





RISULTATI ATTESI

Polizia di Stato

4. A livello operativo le informazioni verranno condivise solo tra gli MS aderenti, che decideranno poi se coinvolgere EUROPOL per le attività investigative susseguenti
5. Aumenterà il livello di sicurezza dei cittadini europei nelle transazioni on-line
6. Aumenterà l'efficienza dei sistemi antifrode bancari
7. Si ridurranno gli introiti delle organizzazioni criminali che usano il *phishing* per finanziare il terrorismo internazionale o altri tipi di reati





CONSIDERAZIONI FINALI

Polizia di Stato

- EU OF2CEN non è concepito come un modello rigido, ma come uno spazio decisionale in cui ogni attore stabilisce quali informazioni condividere e con quali modalità (unicast, multicast or broadcast)
- Europol sarà facilitata nell'identificazione e analisi dei nuovi fenomeni emergenti, lasciando al tempo stesso ampio spazio di manovra alle Forze di Polizia e alle Banche di adottare la strategia più idonea per contrastare il cyber-crime finanziario





Polizia di Stato

**GRAZIE
PER L'ATTENZIONE**

E-mail: francesco.taverna@poliziadistato.it

