Rapporto statistico sulle frodi con le carte di pagamento

No. 5/2015

MINISTERO DELLECONOMIA E DELLE FINANZE

MEF

Dipartimento del Tesoro

Sommario

Sommario

© Ministero dell'Economia e delle Finanze, 2015

Dipartimento del tesoro
Direzione V, Ufficio VI (UCAMP)
Ufficio Centrale Antifrode dei Mezzi di Pagamento
Area Carte di Pagamento

Indirizzo
via XX Settembre, 97
00187 Roma
Telefono
+39 06.47610538
E-mail
ucamp.carte@tesoro.it

Sito internet
http://www.mef.gov.it
http://www.dt.tesoro.it

Tutti i diritti riservati. È consentita la riproduzione
a fini didattici e non commerciali,
a condizione che venga citata la fonte.

ISSN 2239-0189

Aggiornato con i dati relativi ai casi di frode relativi all'annualità 2014

Executive summary

Il Rapporto annuale analizza sotto diversi aspetti i fenomeni delle frodi su carte di pagamento, le manomissioni agli ATM e le revoche delle convenzioni dei POS. In particolare rispetto alle frodi su carte di pagamento (transazioni non riconosciute) si fa riferimento alle frodi perpetrate da carte emesse in Italia e spese ovunque.

Transazioni non riconosciute

Nel 2014, con riferimento alle carte emesse in Italia, è diminuito il valore delle transazioni non riconosciute (frodi) rispetto al totale dei pagamenti genuini mediante carta (dallo 0,0195% allo 0,0189%), mentre è aumentato il numero (da 0,0118% a 0,0131%). Nel 2014 il totale dei pagamenti genuini, sia in valore sia in numero, è aumentato rispettivamente del 4% e del 6%[1]

Il valore delle frodi è aumentato del 5%, mentre il numero è salito del 20%, con una riduzione del valore medio delle singole transazioni (da 177€ a 151€). Trattandosi di una tendenza già riscontrata nel corso del 2013, è possibile ipotizzare un nuovo modus operandi criminale che predilige la parcellizzazione e la moltiplicazione delle transazioni per aggirare le soglie di attenzione sia degli istituti emittenti sia degli stessi utenti.

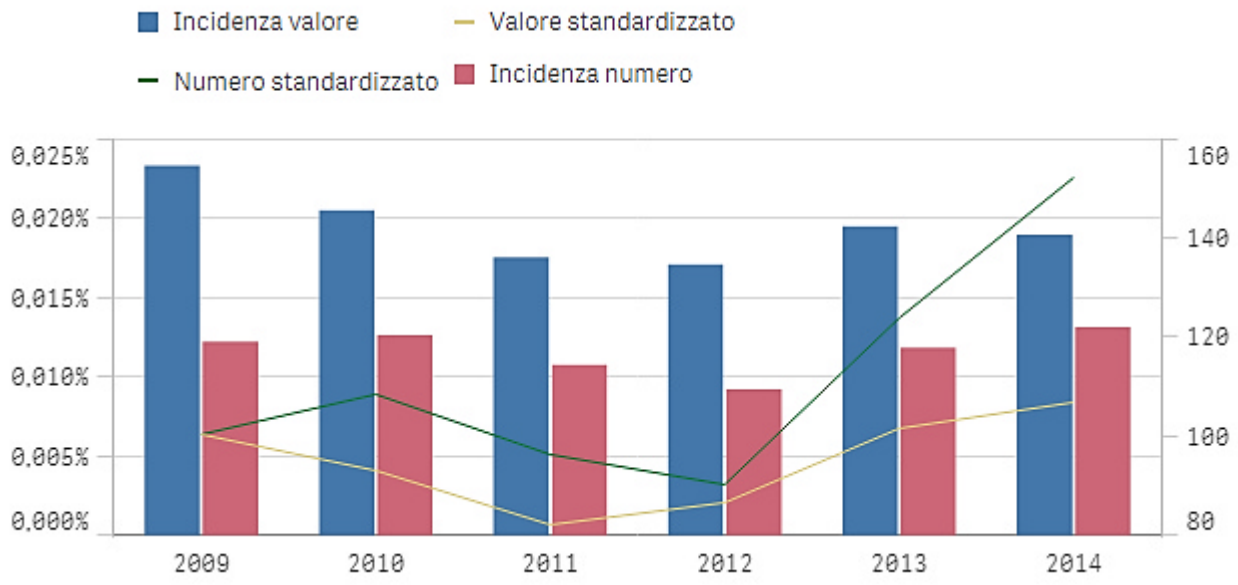


Figura 1: Incidenza e frodato in termini di valore e numero, serie storica

Incidenza valore: Valore in euro delle transazioni non riconosciute su carte emesse in Italia diviso per il valore di tutte le transazioni genuine effettuate con carte italiane.

Incidenza numero: Numero delle transazioni non riconosciute su carte emesse in Italia diviso per il numero di tutte le transazioni genuine effettuate con carte italiane.

Valore standardizzato: Valore delle transazioni non riconosciute su carte emesse in Italia dell'anno di riferimento diviso per il valore del 2009. Un valore di 100 significa che il valore è pari a quello del 2009, un valore di 110 significa che è aumentato del 10% rispetto al 2009.

[1] Dal 2009 al 2014 il totale dei pagamenti genuini, sia in valore sia in numero, è costante aumentato a riprova di un maggior utilizzo degli strumenti di pagamento alternativi al contante. L'aumento nel periodo è stato pari al 35% in numero e 26% in valore.

Numero standardizzato: Numero delle transazioni non riconosciute su carte emesse in Italia dell'anno di riferimento diviso per il numero del 2009. Un valore di 100 significa che il valore è pari a quello del 2009, un valore di 110 significa che è aumentato del 10% rispetto al 2009.

L'analisi della serie storica 2009-2014 descrive un fenomeno sostanzialmente sotto controllo ma, con riferimento agli ultimi due anni, conferma una forte spinta alla crescita nel numero delle transazioni fraudolente e un ruolo crescente di Internet quale contesto emergente di realizzazione delle frodi.

In termini di **canali di pagamento** utilizzati per finalità di frode mentre Internet si caratterizza per una tendenza alla crescita, i POS e i prelievi su ATM registrano una flessione. Tuttavia, si assiste ad una diminuzione del valore medio delle singole transazioni su tutti i canali.

Canale internet

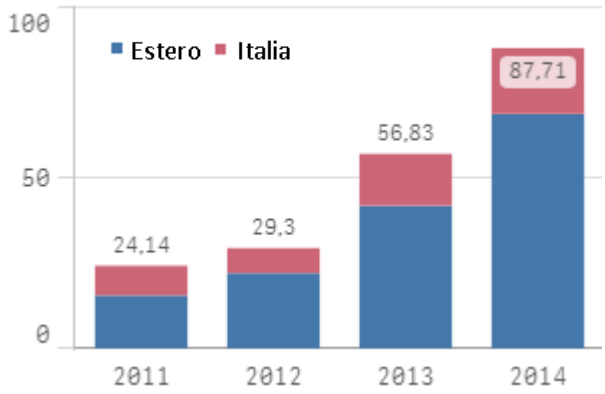


Figura 2: Numero standardizzato di frodi su Internet, estero/Italia

Sul canale **internet** si è verificato un aumento delle frodi (+11% in termini di incidenza valore e +30% come valore del frodato). Per il quinto anno consecutivo l'incremento dell'utilizzo fraudolento della carta in internet corrisponde a un incremento del valore delle transazioni fraudolente.

Dal 2011 il numero di transazioni non riconosciute è cresciuto di oltre 3 volte ed ora incide per oltre la metà sul numero complessivo delle transazioni fraudolente. Il fenomeno si verifica soprattutto all'estero[2].

I valori 2014 delle transazioni non riconosciute su Internet articolati per categoria merceologica non presentano variazioni rilevanti rispetto al 2013, almeno per le categorie a maggiore incidenza.

L'aumento 2014 in termini di numero di transazioni non riconosciute sul canale Internet è superiore al 60%. Le cinque Categorie Merceologiche (MCG[3]: *Miscellaneous Industrial/Commercial Supplies, General Retail and Wholesale, Mail Order / Direct Selling, Leisure Activities Computer Equipment & Services*) con il maggior tasso di crescita in termini di numero transazioni non riconosciute sono quelle con sostanziali riduzioni nel valore medio delle singole transazioni. Per queste stesse MCG si denota una marcata prevalenza per le frodi perpetrate all'estero (86%), in primis nel Regno Unito.

Canale POS

Nel canale **POS** si assiste ad un calo generalizzato del fenomeno a tutti i livelli: incidenza e frodato sia in termini di valore che di numero.

La struttura delle frodi per categoria merceologica non presenta variazioni rilevanti rispetto al 2013. Le categorie merceologiche più attaccate risultano essere: *General Retail and Wholesale, Travel* -

[2] Estero: insieme di tutte le nazioni del mondo esclusa l'Italia
[3] Merchant Category Group: raggruppamento di Categorie Merceologiche secondo la classificazione VISA.

Air/Rail/Road, Leisure Activities, Telecommunication Services. Escludendo la *General Retail and Wholesale*, sulle altre tre categorie si rilevano valori ridotti di circa il 30% in termini di numero di operazioni.

Continuando nell'esame delle categorie merceologiche si nota che la categoria *Miscellaneous Industrial/Commercial Supplies* è aumentata del 60% in termini di numero; un incremento importante che non si riflette nella crescita del valore delle transazioni a causa di una contemporanea contrazione degli importi medi delle stesse.

Canale prelievi su ATM

Anche per il 2014, come già in tutti gli anni precedenti, si conferma una tendenza alla riduzione del fenomeno delle frodi su **Prelievi su ATM**. La riduzione più visibile sul valore (-18% in termini di incidenza e -12% in termini di frodato) rispetto al numero (-6% in termini di incidenza mentre è costante in termini di frodi).

Mentre in Italia è più elevato il valore del frodato, il frodato su carte italiane spese all'estero rileva una percentuale più elevata del numero di transazioni fraudolente (60%), di cui la maggior parte negli Stati Uniti.

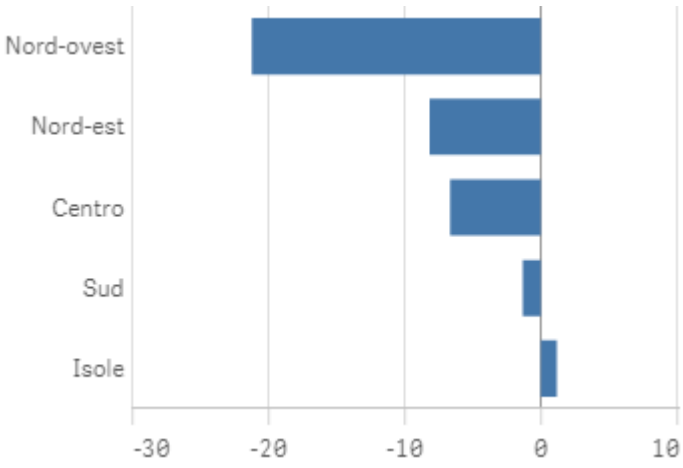
Le regioni italiane su cui insiste maggiormente la diminuzione in valore sono Piemonte e Lombardia, seguono Lazio e Veneto.

Manomissioni ATM

Le **manomissioni di ATM** si riducono di quasi il 60% sia in termini di incidenza che di numero.

Il calo più vistoso è nelle regioni centro-settentrionali. In controtendenza le Isole, dove si assiste ad un leggero aumento.

In forte riduzione il fenomeno del cash Trapping e l'utilizzo di macchina fotografica a distanza per catturare il PIN, fenomeno questo che scompare del tutto nel corso del 2014.



Nel corso dell'ultimo anno i casi di manomissione di sportelli Atm sono da attribuire per lo più a soggetti di nazionalità bulgara, mentre i casi di "skimming" presso esercizi della ristorazione sono da attribuire soprattutto a soggetti di nazionalità romena ed albanese[4].

[4] Fonte: G. di. F. - Nucleo Speciale Polizia Valutaria. Gruppo Antifalsificazione Monetaria ed Altri Mezzi di Pagamento.

Revoche convenzioni POS

Le **revoche convenzioni** POS in Italia diminuiscono, in termini di incidenza[5], dell'8%. A livello regionale si nota un forte aumento dell'Emilia-Romagna e una significativa discesa della Sicilia. La Campania, dove storicamente il fenomeno si concentra, aumenta leggermente.

[5] Numero di revoche di convenzioni di apparecchiature POS rispetto al totale delle convenzioni attive nell'anno.

UCAMP Competenze e attività

Le attività dell'UCAMP

Il Dipartimento del tesoro, nell'ambito delle proprie attribuzioni, è suddiviso in settori omogenei di attività e, tra questi, rilevanza assume l'area della prevenzione dei reati finanziari (Direzione V).

L'Ufficio Centrale Antifrode dei Mezzi di Pagamento (UCAMP) costituisce la struttura operativa, nell'ambito della suddetta area, preposta ai seguenti compiti:

- il monitoraggio delle falsificazioni dell'Euro;
- la prevenzione delle frodi sulle carte di pagamento;
- l'attività di formazione di carattere specialistico, nei settori di competenza, sia a livello nazionale sia internazionale.

L'UCAMP trae origine dal Regolamento (CE) 1338/2001, istitutivo del sistema europeo di protezione dell'Euro, e funge da Ufficio centrale italiano per la raccolta e lo scambio dei dati statistici su banconote e monete sospette false al fine di effettuare un'analisi strategica del fenomeno delle falsificazioni e valutarne l'impatto sul sistema economico e finanziario. Per lo svolgimento di tali funzioni l'UCAMP si è dotato di un Sistema Informatizzato Frodi Euro (SIRFE), che consente la trasmissione telematica dei verbali di sequestro delle banconote sospette di falsità.

Con la legge n.166/2005, istitutiva del Sistema di prevenzione delle frodi sulle carte di pagamento, e con il relativo Regolamento di attuazione (D.M. n.112/2007) sono state attribuite all'UCAMP le attuali competenze in materia di prevenzione, sul piano amministrativo, delle frodi sulle carte di pagamento.

In attuazione della richiamata normativa l'UCAMP ha curato la realizzazione del Sistema Informatizzato per la Prevenzione delle Frodi sulle carte di pagamento (SIPAF), che permette la consultazione e la condivisione, in tempo reale, di dati e informazioni riguardanti esercizi commerciali sospetti e operazioni con transazioni non andate a buon fine. In tale ambito è stato costituito un gruppo di lavoro con funzioni consultive (GIPAF), al quale partecipano esperti nel settore delle frodi designati dalle Amministrazioni statali, dalla Banca d'Italia, dall'ABI, dalle Forze di Polizia, dalle società segnalanti, nonché esperti provenienti dal mondo accademico e scientifico.

La strategia operativa dell'UCAMP nella realizzazione e nella gestione del sistema di prevenzione mira alla tutela del sistema bancario e delle società emittenti, ma, in ultima analisi, è finalizzata alla tutela del cittadino, che ripone la propria fiducia negli strumenti di pagamento sostitutivi del contante.

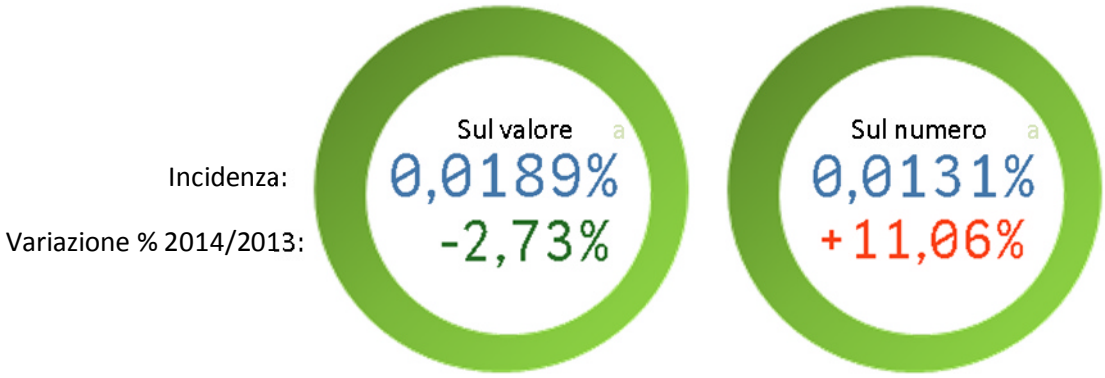
L'UCAMP promuove e coordina attività formative in ambito nazionale e internazionale, in particolare, relativamente alla falsificazione dell'Euro, ha organizzato numerosi seminari e workshop indirizzati a tutte le categorie coinvolte nel fenomeno della contraffazione monetaria, in attuazione del programma comunitario di formazione denominato Pericles. Dal 2009, inoltre, ha avviato un programma formativo in collaborazione con le Amministrazioni locali, per fornire le informazioni utili per la prevenzione delle frodi.

Analisi del fenomeno

Trend e statistiche

Incidenze

L'incidenza si definisce come il rapporto tra le transazioni frodate e il totale delle transazioni genuine avvenute nell'anno.



Nel corso dell'anno 2014 l'incidenza in valore ha subito una lieve diminuzione (-2,73%) mentre è cresciuta come numero di transazioni (+11,06%). Dunque il valore medio delle singole transazioni si è sensibilmente ridotto.

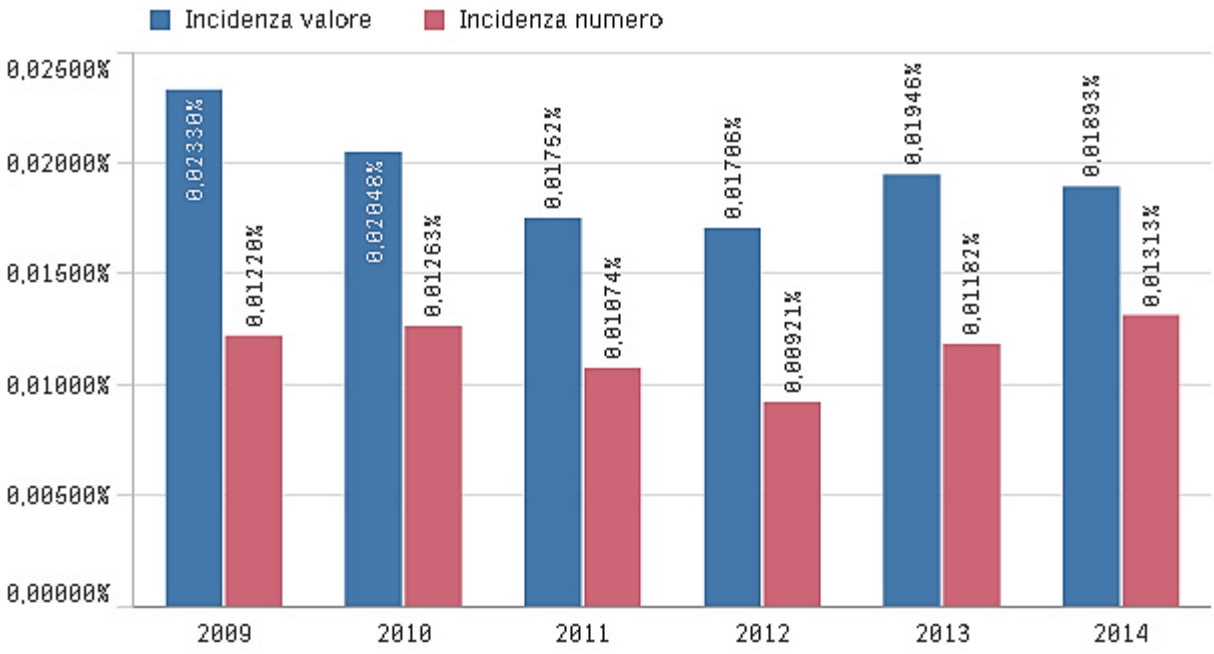


Figura 3: Incidenza delle frodi sul totale transazioni in numero e valore

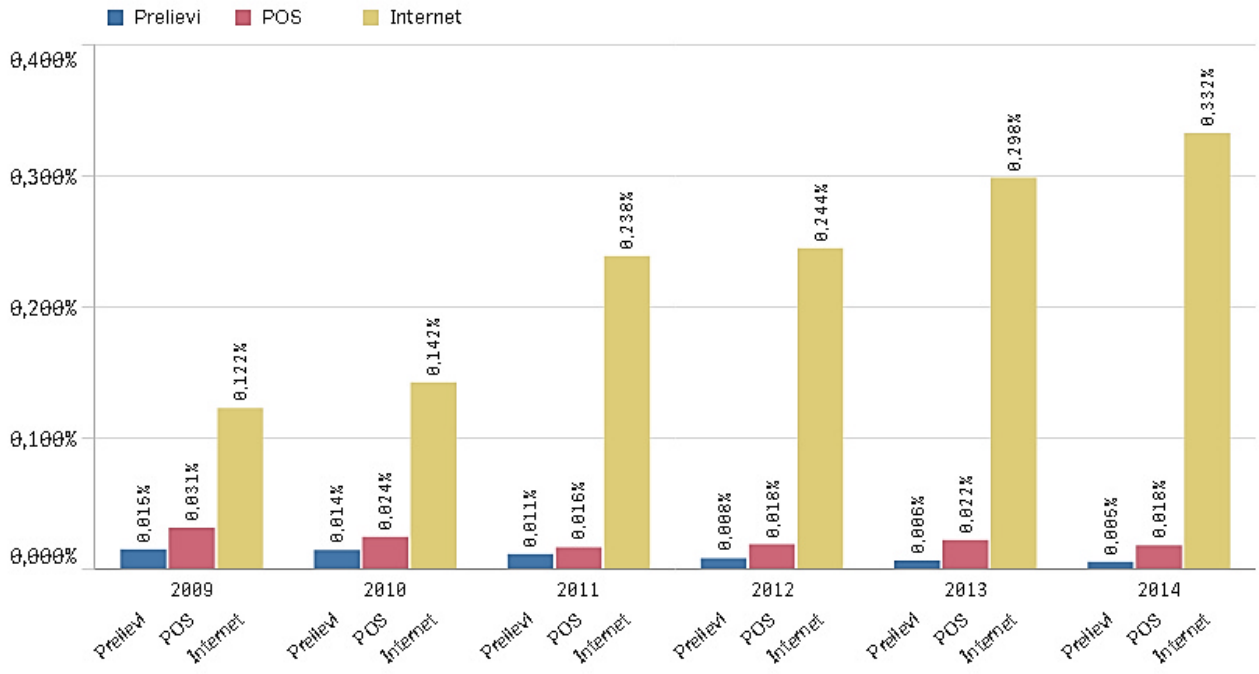


Figura 4: Incidenza per canale di pagamento

Variazione percentuale 2014/2013 del valore delle incidenze per canale

Internet: +11,36% POS: -18,68% Prelievi su ATM: -17,94%

Continua la crescita dell'incidenza delle frodi su Internet mentre si conferma la diminuzione su POS e Prelievi su ATM. Le incidenze delle frodi in valore per Debito/Credito restano sostanzialmente stabili.

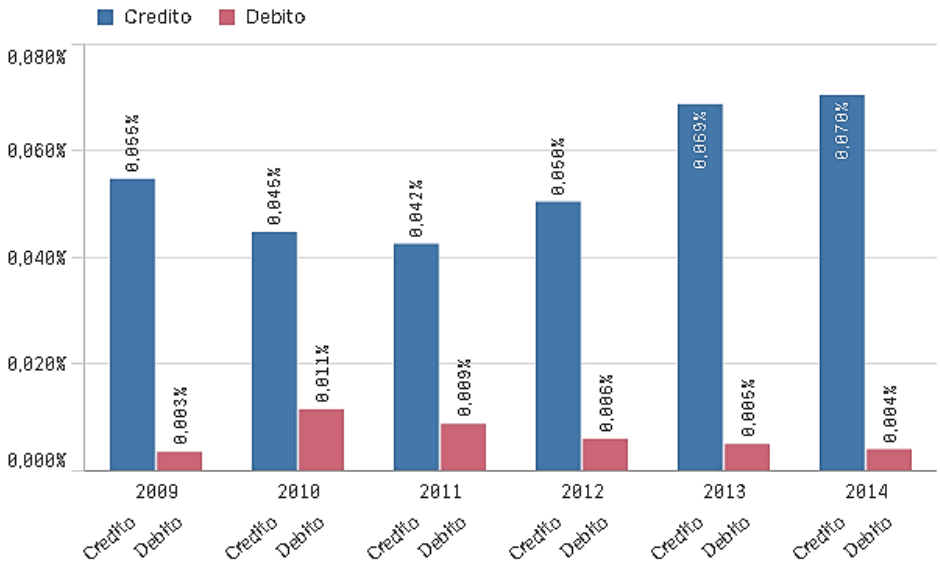
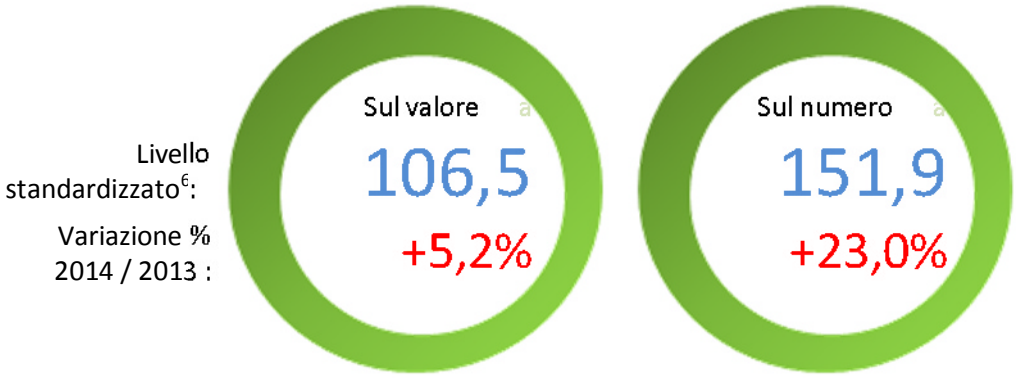


Figura 5: Incidenza per debito e credito

Andamento generale



In valore le frodi sono molto simili (106,5) al livello del 2009 mentre in numero sono aumentate del 50% (151,9). Il valore medio è diminuito durante tutto il 2014.

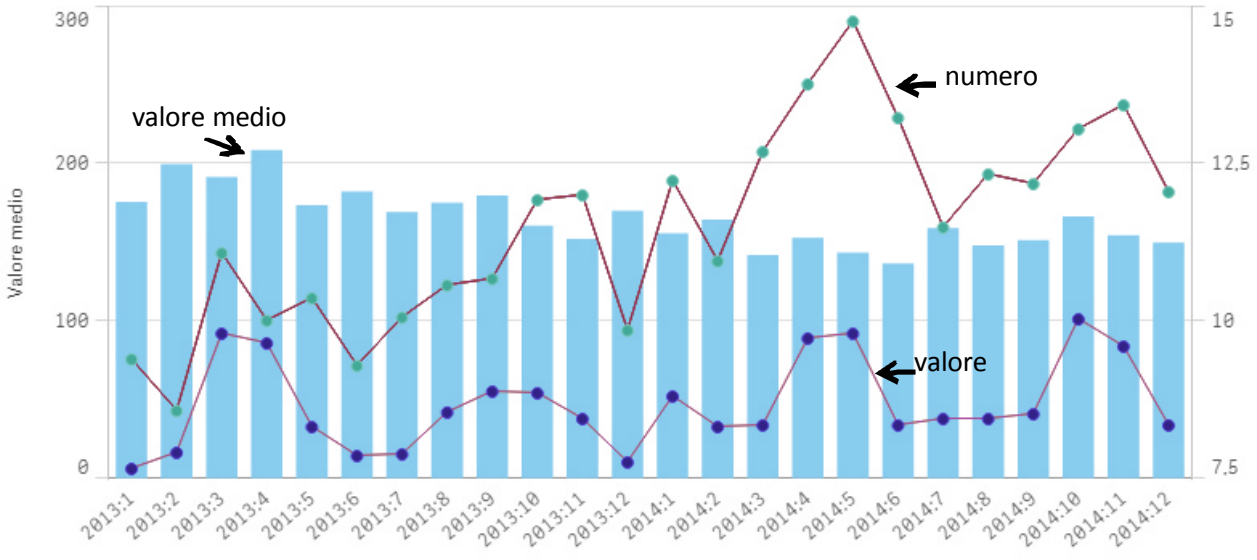


Figura 6: Andamento mensile di numero e valore standardizzati, valore medio

[6] Valore standardizzato: Valore delle transazioni non riconosciute nell'anno di riferimento diviso per il valore del 2009, su carte emesse in Italia. Un valore di 100 significa che il valore è pari a quello del 2009, un valore di 110 significa che è aumentato del 10% rispetto al 2009.
Numero standardizzato: Numero delle transazioni non riconosciute nell'anno di riferimento diviso per il numero del 2009, su carte emesse in Italia. Un valore di 100 significa che il valore è pari a quello del 2009, un valore di 110 significa che è aumentato del 10% rispetto al 2009.

Frodi per canale di pagamento

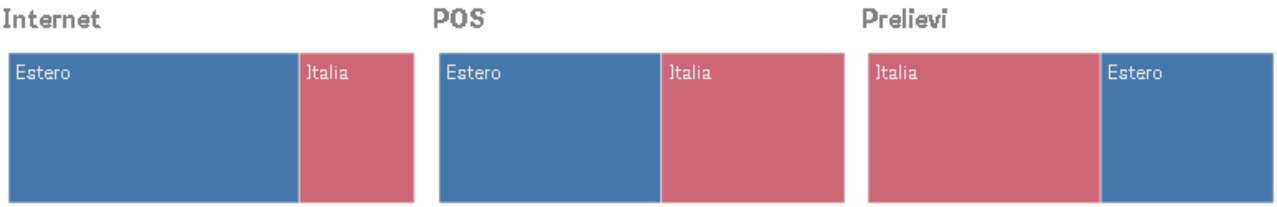


Figura 7: Composizione del frodato in valore in base al luogo in cui le carte sono spese (Italia/estero), distinto per canale

Variazione percentuale 2014/2013

Internet: +30,7% POS: -10,9% Prelievi su ATM: -12,4%

In termini di frodato, senza tenere conto delle transazioni totali genuine, si conferma quanto già visto nelle incidenze: Internet è in crescita mentre scendono gli altri canali.

La maggior parte delle frodi su internet risulta avvenuta all'estero.

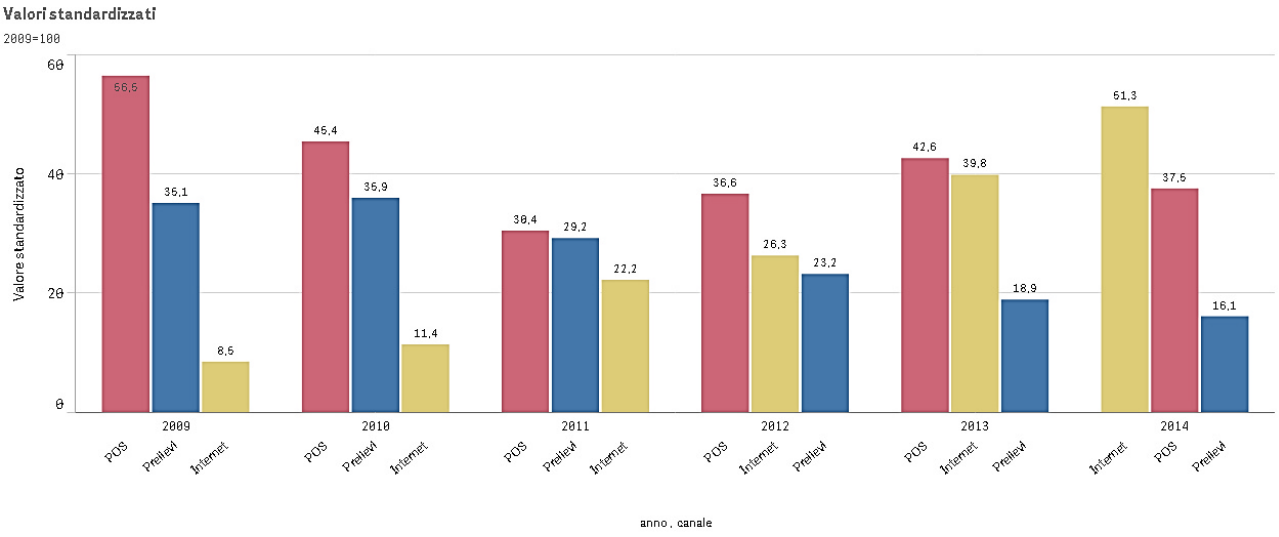


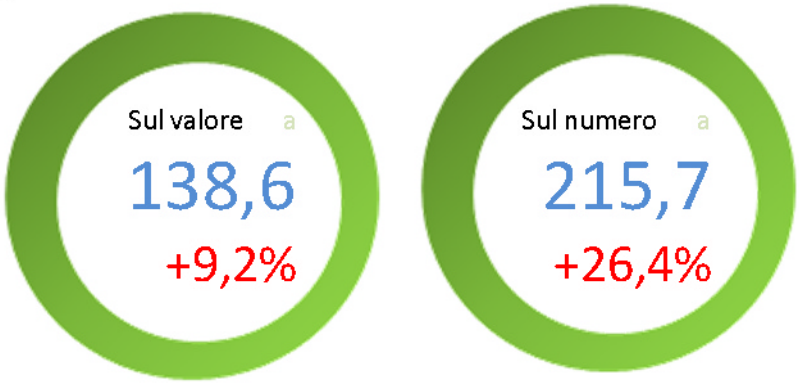
Figura 8: andamento frodi per canale

Categorie merceologiche

Canali di pagamento POS e Internet.

Livello standardizzato[7]:

Variazione % 2014/2013:



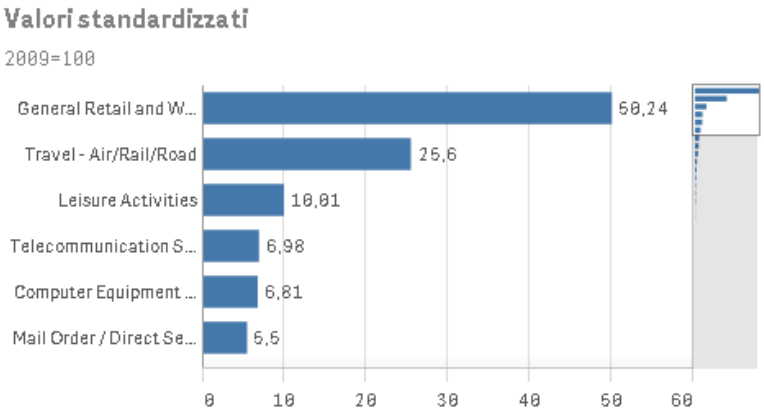


Figura 9: Le 6 Merchant Category Group più importanti in termini di frodato

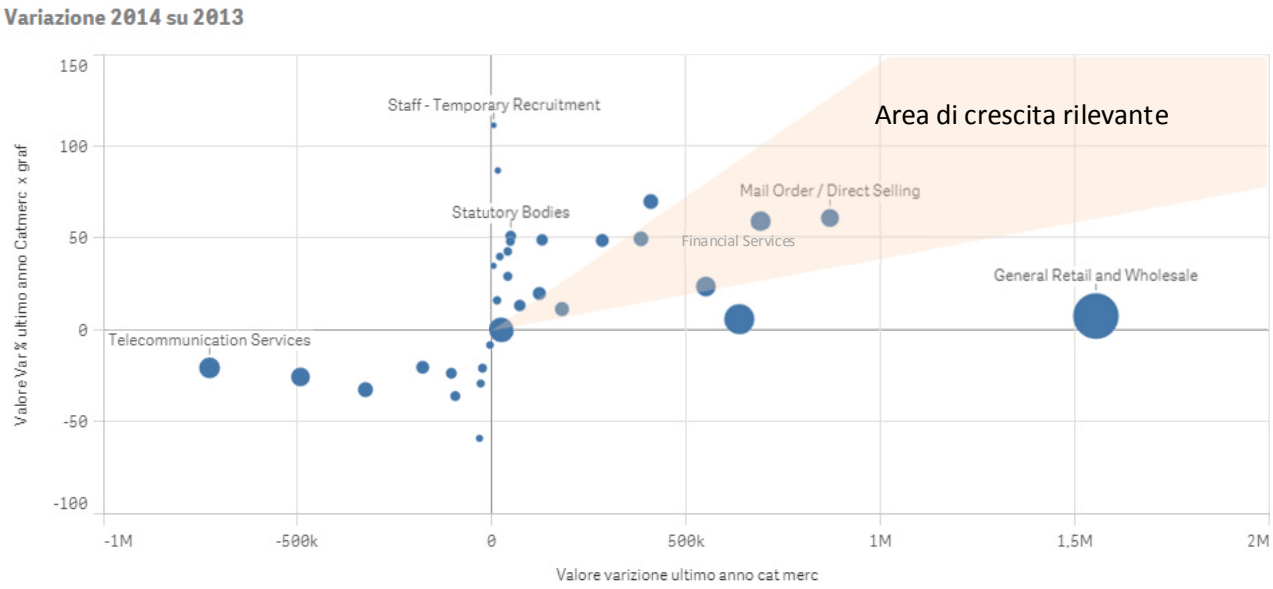


Figura 10: Le Merchant Category Group in valore (dimensione bolla, in variazione assoluta (asse x) e variazione percentuale (asse y)

[7] Vedi nota 6.

Distribuzione Geografica

Canali di pagamento POS e Internet.

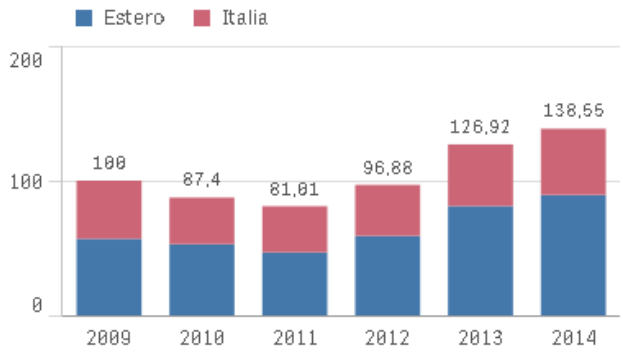


Figura 11: Valore standardizzato canali POS e Internet in base al luogo in cui le carte sono spese (Italia/estero)

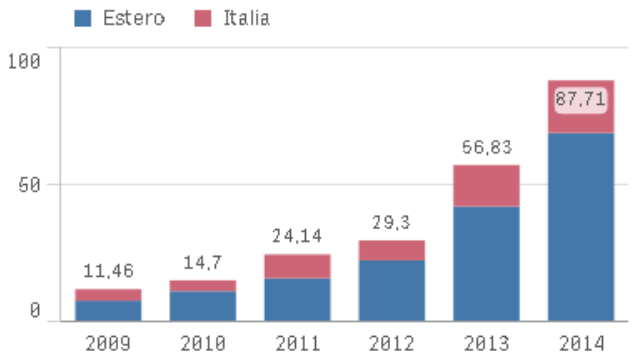


Figura 12:: Numero standardizzato canali POS e Internet in base al luogo in cui le carte sono spese (Italia/estero)

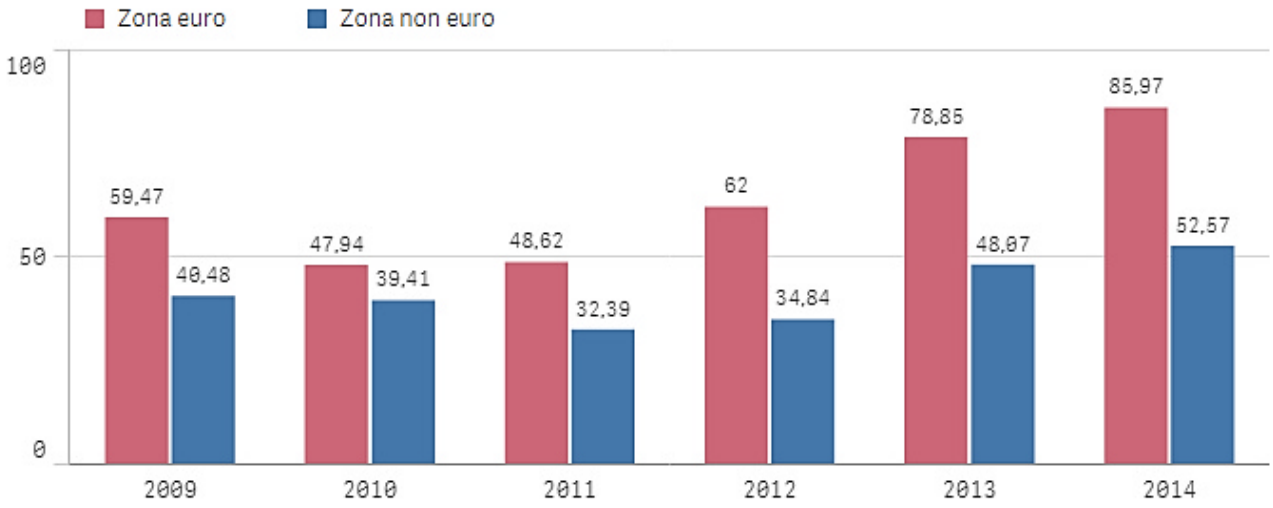


Figura 13: Valore standardizzato canali POS e Internet, carte emesse in Italia e spese in zona euro/non euro

Variazione percentuale 2014/2013

Valore

Zona euro: +13,3% Zona non euro: +8%

Numero

Zona euro: +14,1% Zona non euro: +49,1%

Canali di pagamento POS e Internet - Estero

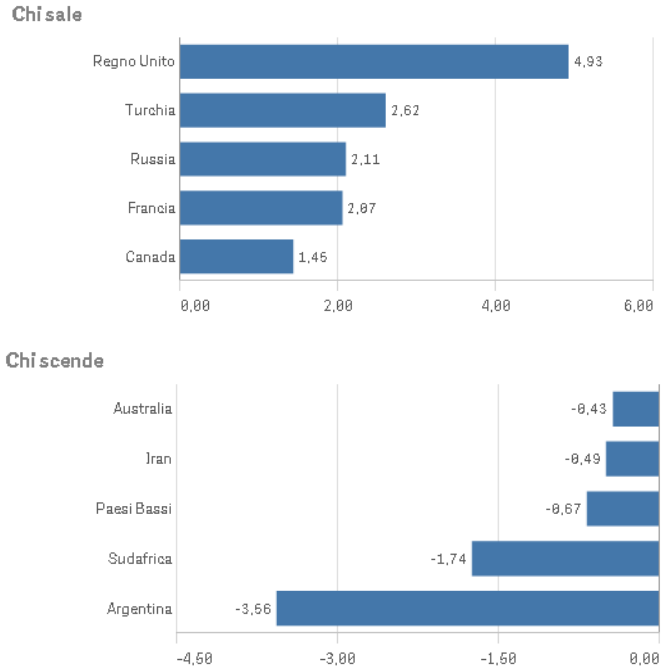


Figura 14: Variazioni 2014 - 2013 del valore standardizzato, primi 5 paesi

Estero: Variazione percentuale 2014/2013

Valore: +10,2% Numero: +40,4%

I grafici in alto mostrano i cinque paesi che esteri con la maggiore crescita (o diminuzione) di frodi sui canali POS e Internet. In basso invece la mappa riporta la distribuzione delle frodi nel 2014.

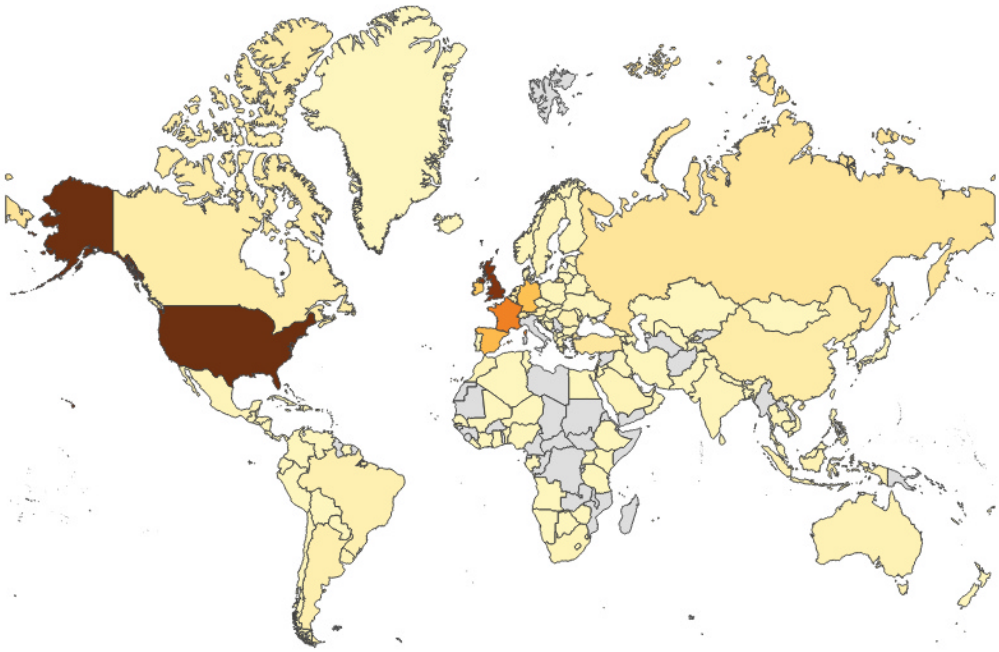


Figura 15: la mappa per valore delle frodi 2014 all'estero (il colore esprime l'intensità del fenomeno)

Tipologia di disconoscimento

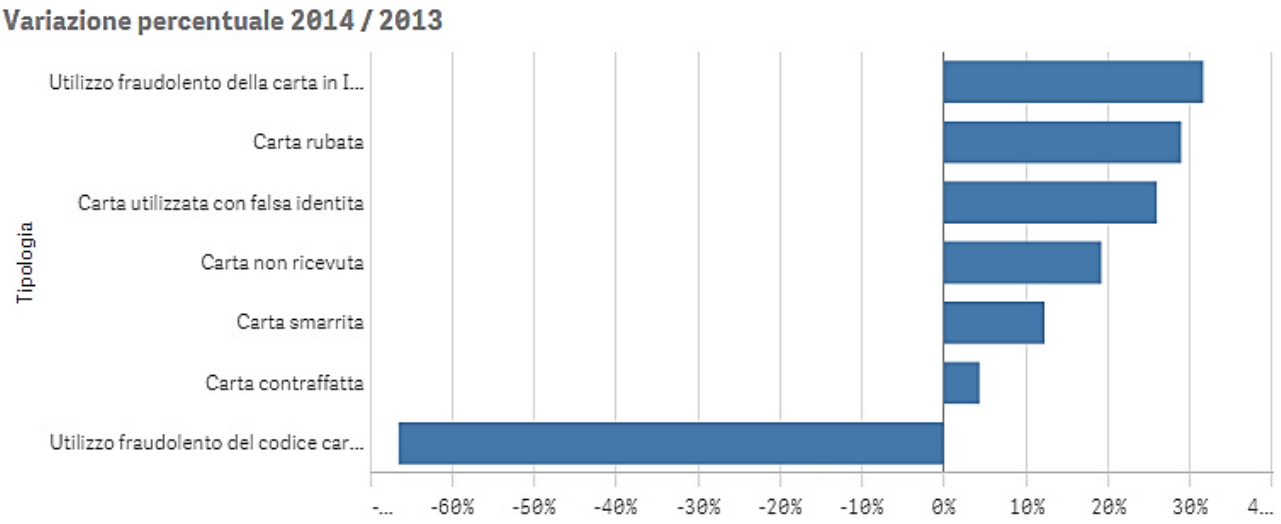


Figura 16: Variazione percentuale valore del frodato per tipologia di disconoscimento

Anche quest'anno si conferma l'aumento della tipologia su Internet mentre si ferma la discesa della contraffazione della carta.

Da un punto di vista criminologico permane la casistica di soggetti di provenienza africana e cinese dediti all'utilizzo di carte di credito clonate compromesse all'estero (soprattutto USA); si stima a seguito di hacking[8].

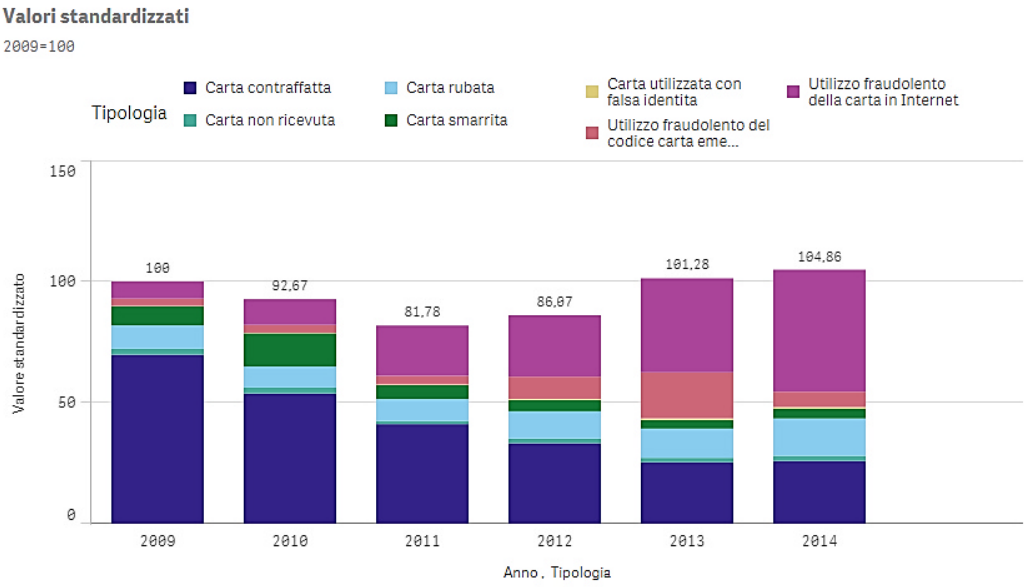


Figura 17: Andamento annuale del valore standardizzato per tipologia di disconoscimento

[8] Fonte: Forze di Polizia

Prelievi su ATM Italia

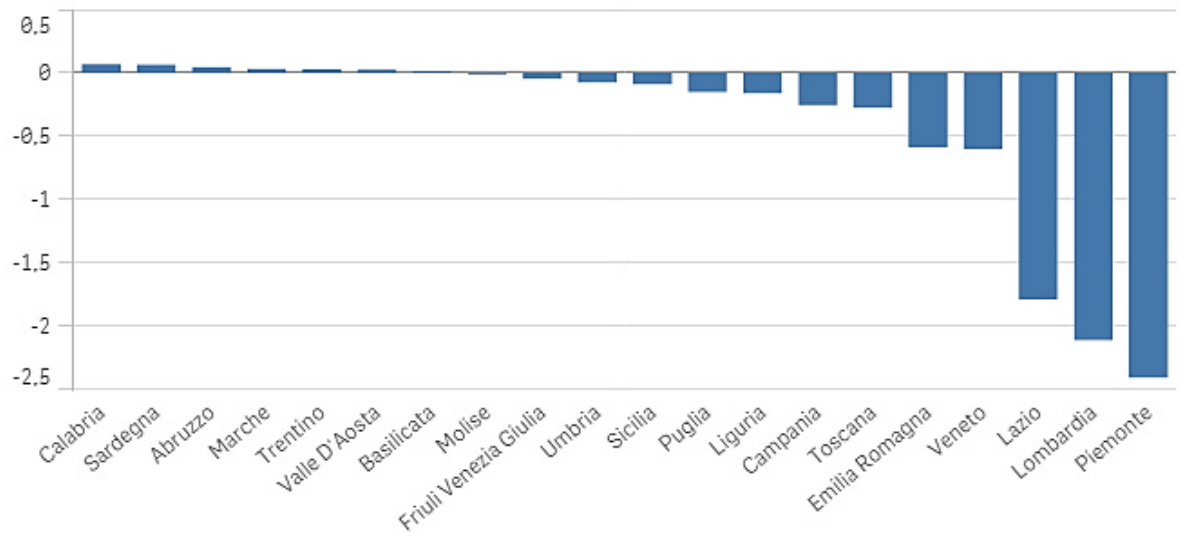


Figura 18: variazione del valore standardizzato dei prelievi in Italia

Variazione percentuale 2014/2013

-24%

Anche quest'anno le frodi su prelievi diminuiscono quasi ovunque. Com'era prevedibile le regioni dove le frodi diminuiscono di più sono quelle dove il fenomeno è più rilevante.

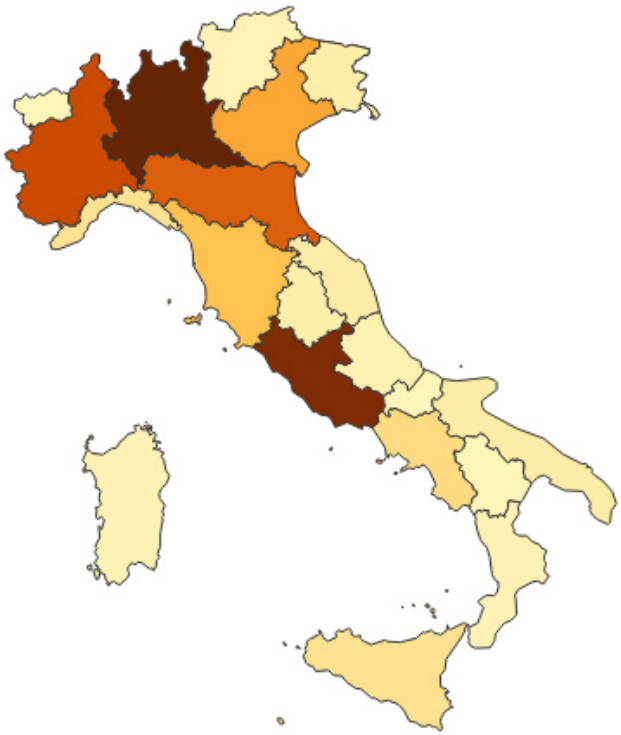


Figura 19: Mappa delle frodi su prelievi in Italia (il colore esprime l'intensità del fenomeno)

Prelievi su ATM all'Estero

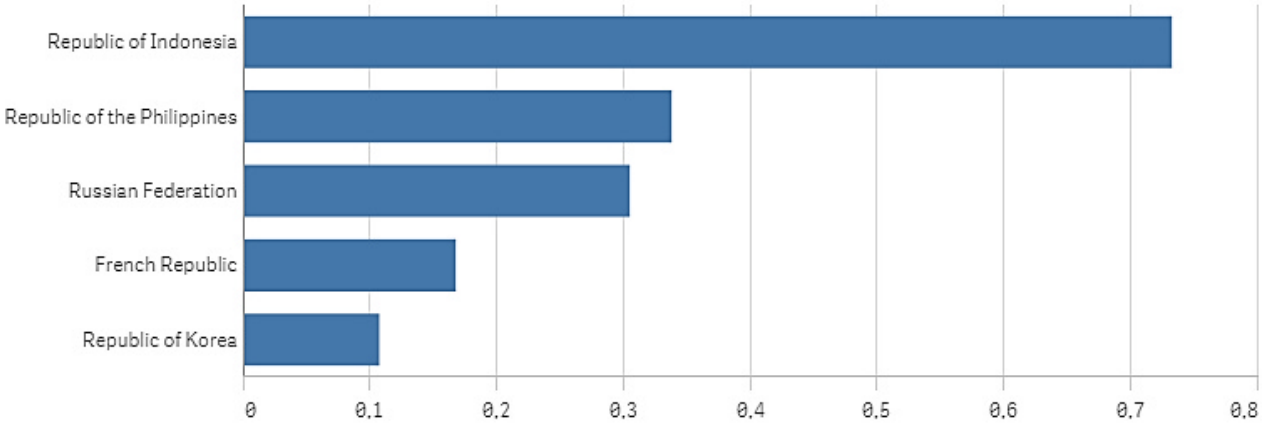


Figura 20: i 5 paesi con la maggiore crescita delle frodi su Prelievi

Variazione percentuale 2014 / 2013

Valore: +11%

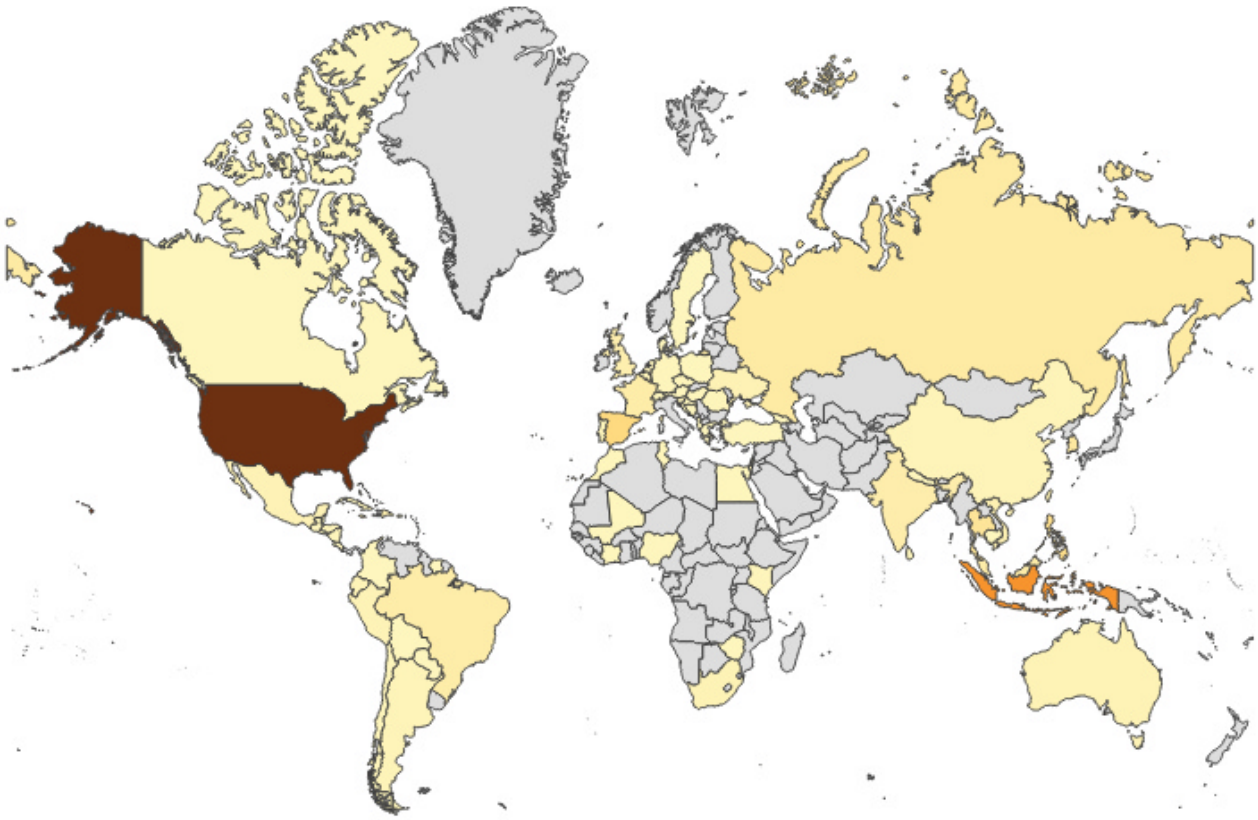


Figura 21: Mappa delle frodi su Prelievi nel resto del mondo (il colore esprime l'intensità del fenomeno)

Valori medi

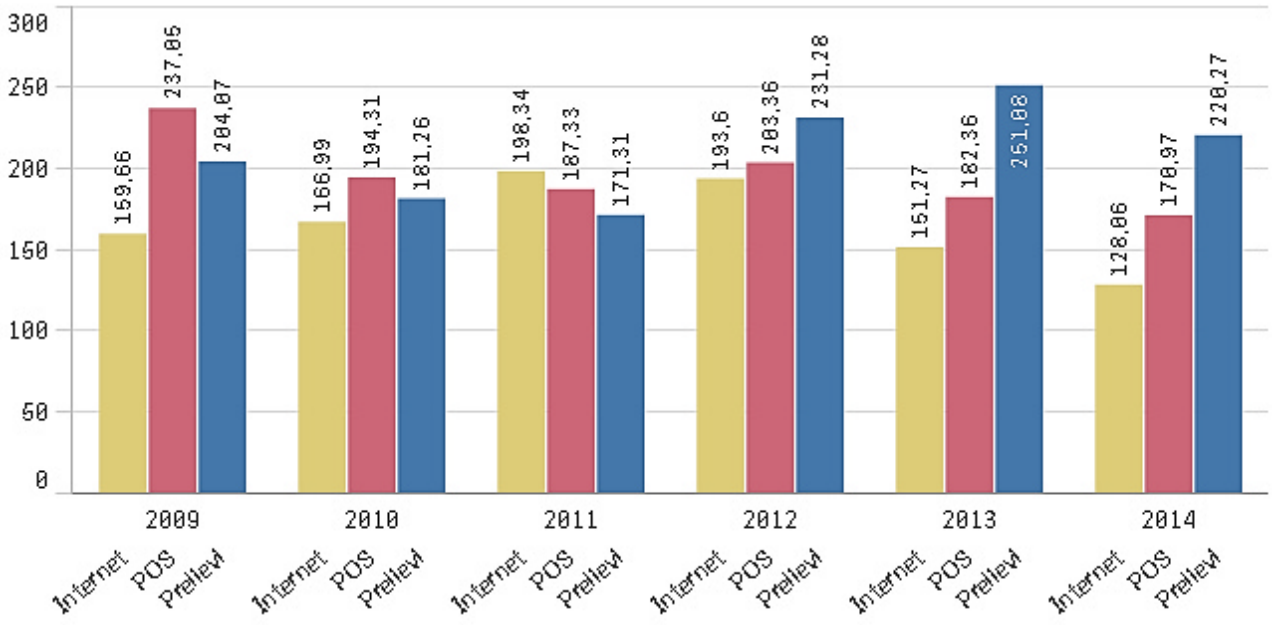


Figura 22: valori medi delle transazioni per canale

Variazione del valore medio delle transazioni 2014 – 2013 in euro

Internet: -23€ POS: -11€ Prelievi: -31€

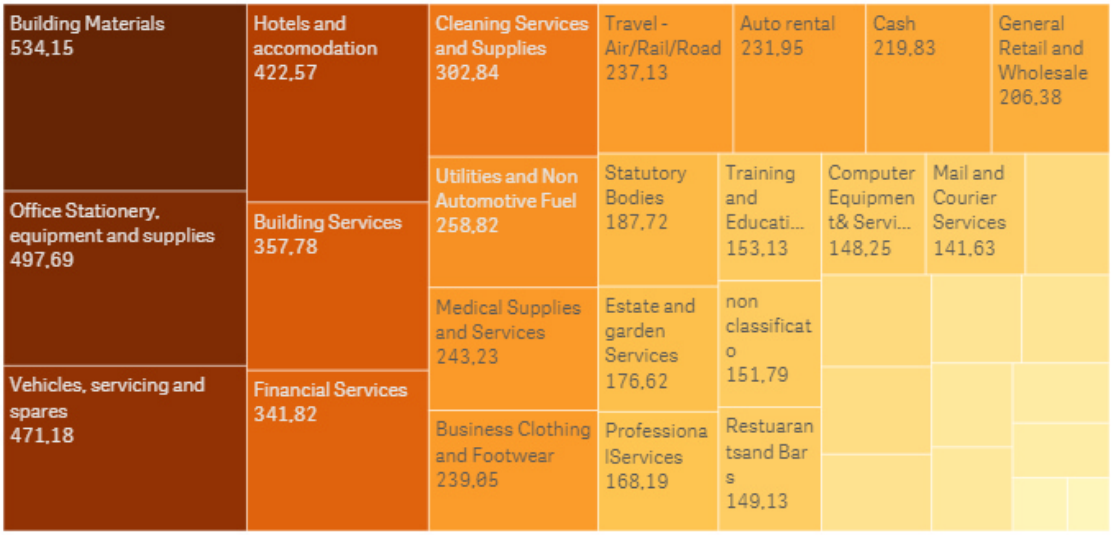


Figura 23: Valori medi per categoria merceologica

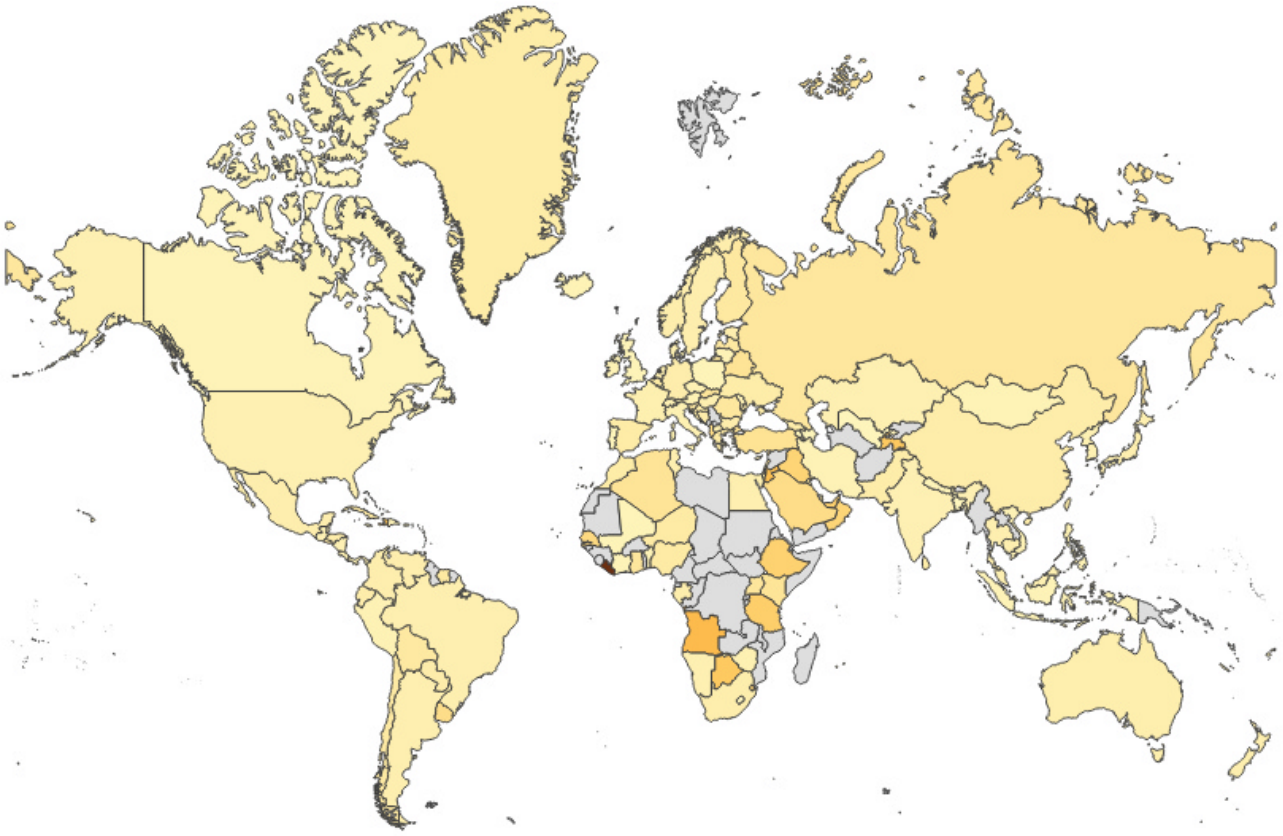
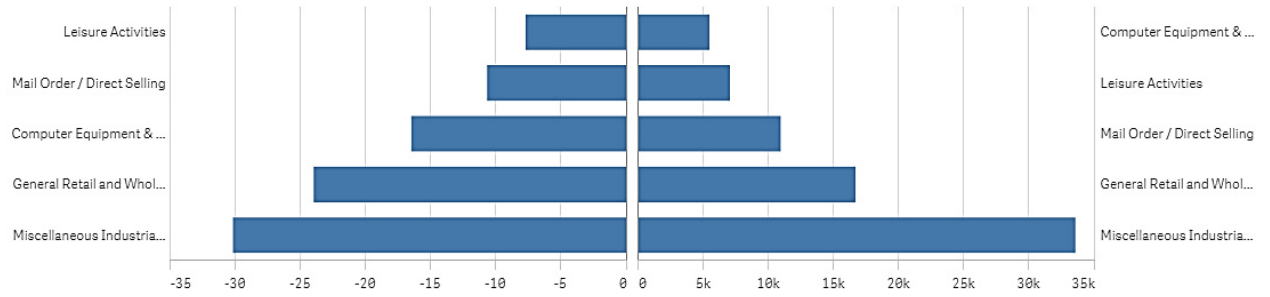


Figura 24: Valori medi per nazione (il colore esprime l'intensità del fenomeno)

I paesi con valori medi di transazioni frodate più elevati appartengono tutti ad Africa e Medio Oriente.

Un approfondimento

Le cinque categorie merceologiche che aumentano di più su internet come numero di transazioni (grafico di destra) sono le stesse che hanno la più forte diminuzione di valore medio (grafico di sinistra).



Confronti internazionali

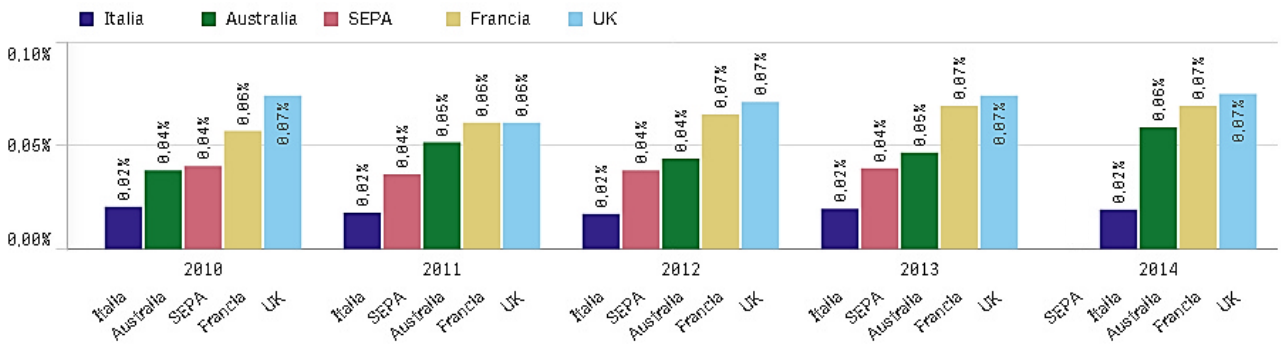


Figura 25: Confronto dell'incidenza in valore per i principali paesi

Nel 2014 si assiste ad un considerevole aumento dell'incidenza in Australia, gli altri paesi, Italia compresa, rimangono sostanzialmente stabili.

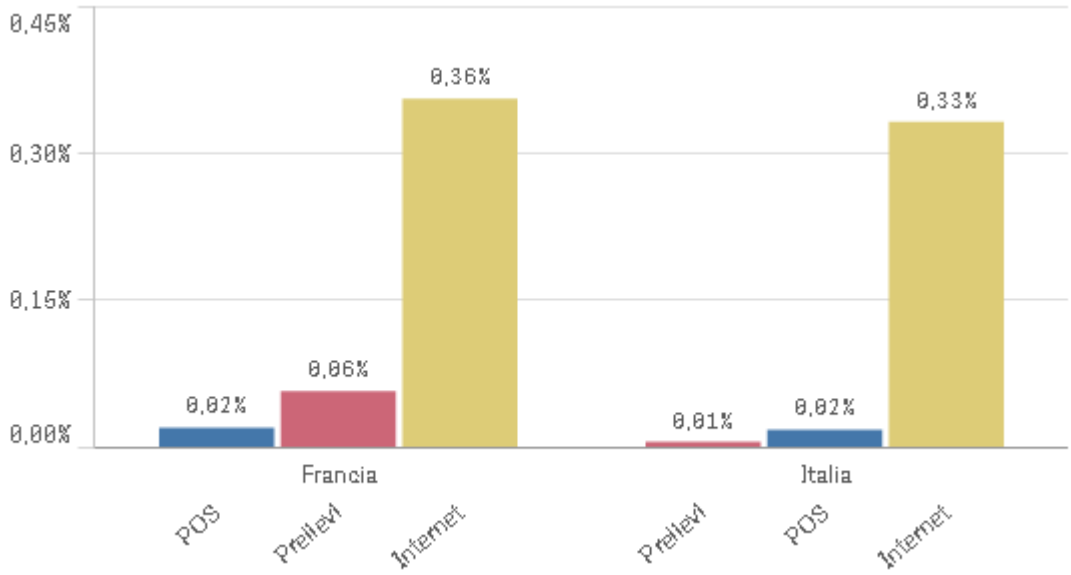


Figura 26: Confronto dell'incidenza in valore per canale Italia - Francia[9]

[9] I dati pubblicati dai vari paesi consentono il confronto dell'incidenza in valore per canale con la sola Francia.

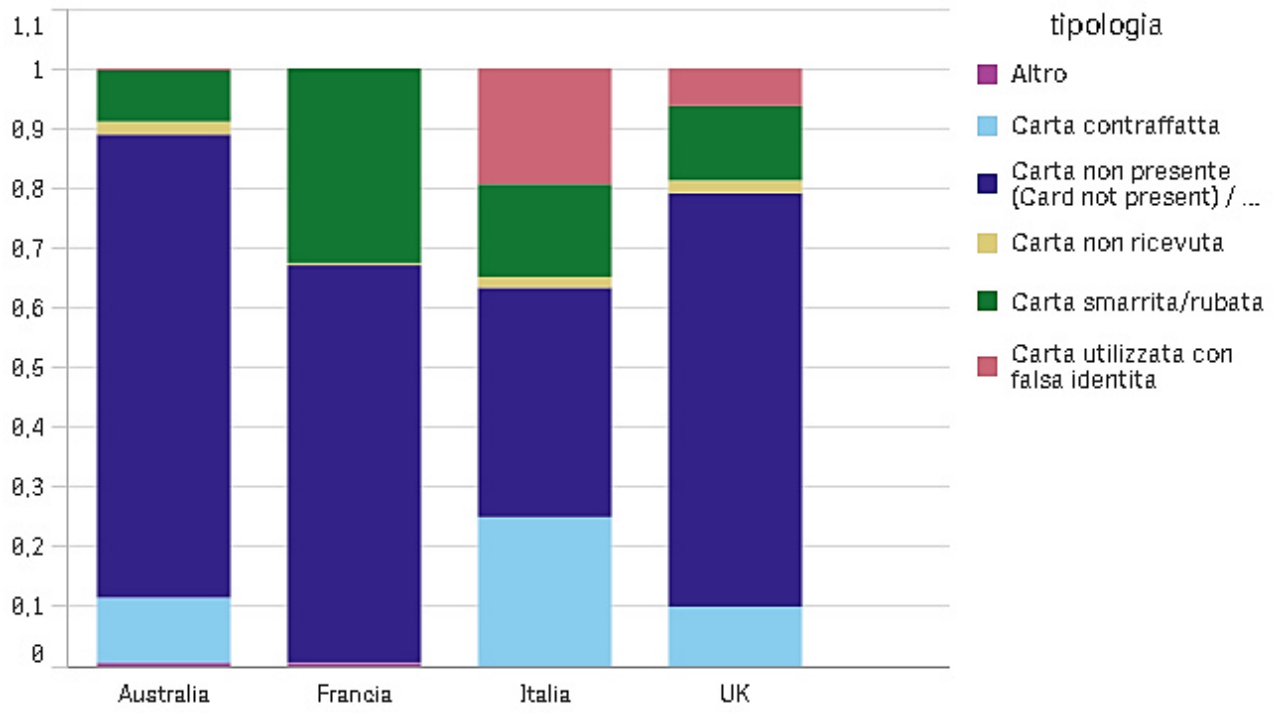


Figura 27: Tipologia di disconoscimento per nazione, anno 2014 composizione percentuale

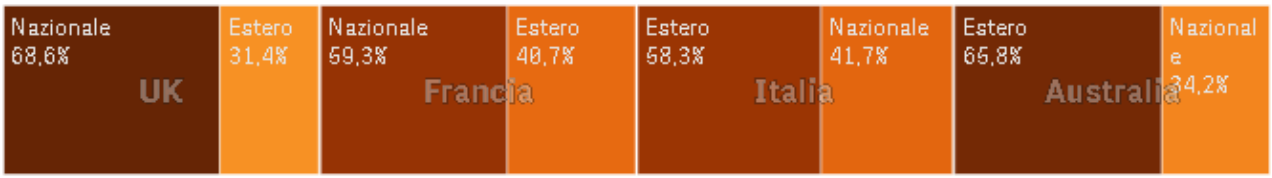


Figura 28: Nelle diverse nazioni composizione del frodato in valore in base al luogo in cui le carte (emesse nel paese di provenienza) vengono spese

Manomissioni ATM

Incidenza: rapporto fra il numero di manomissioni ATM ed il numero di ATM attivi.

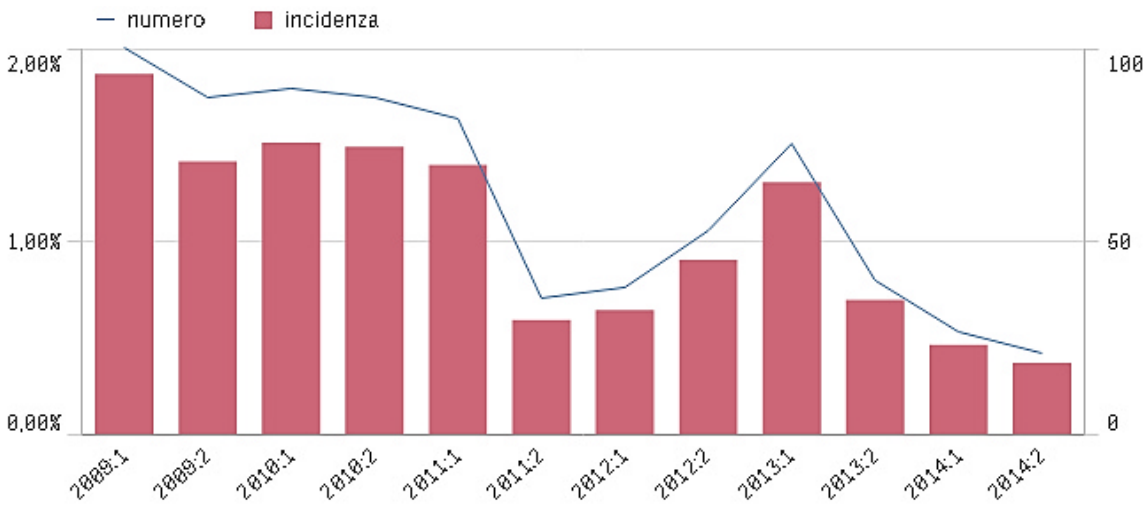


Figura 29: Numero di attacchi (linea) e incidenza (istogramma)

Incidenza 2014: 0,42 variazione percentuale 2014/2013 -59%

Figura 30: mappa dell'incidenza degli attacchi ad ATM regionale 2014 (il colore esprime l'intensità del fenomeno)

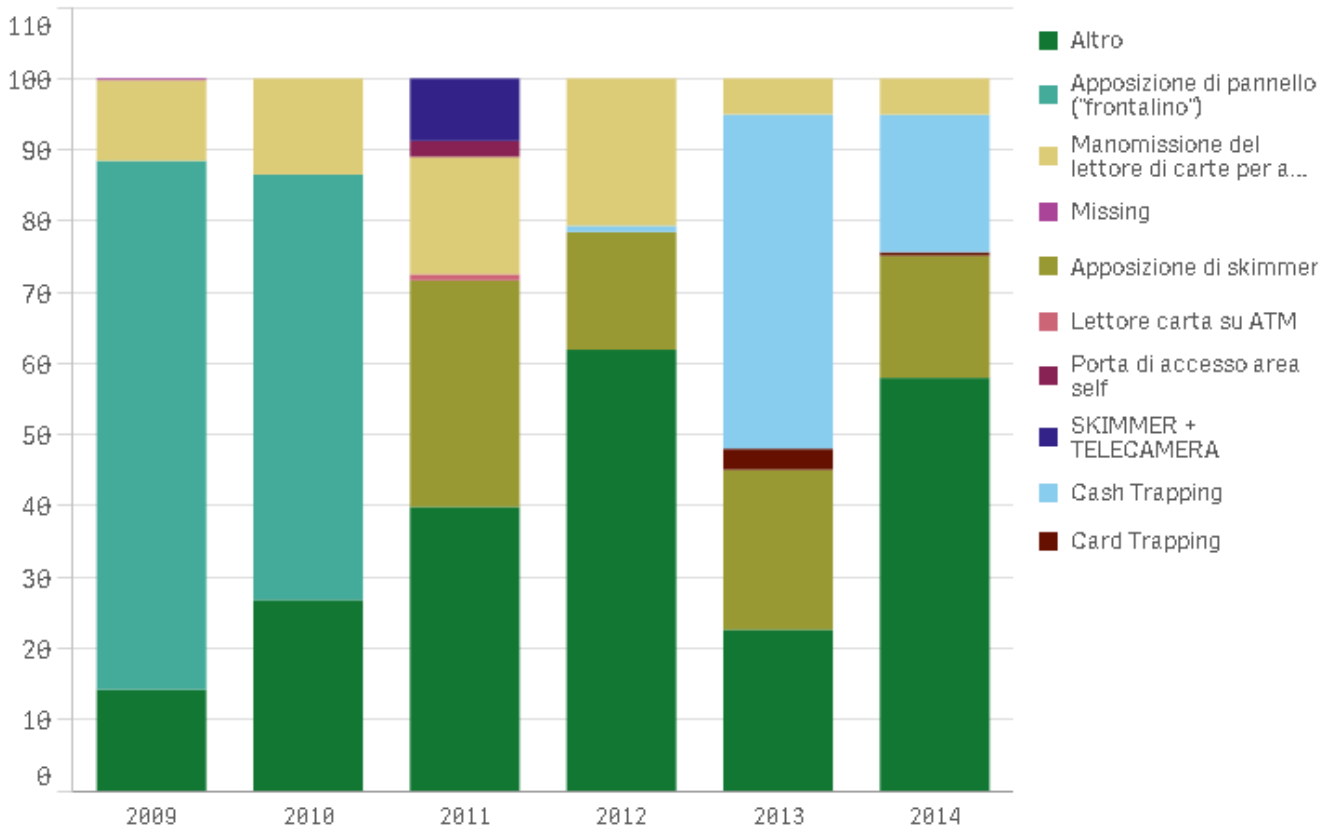


Figura 31: Tipologie di manomissione, composizione percentuale

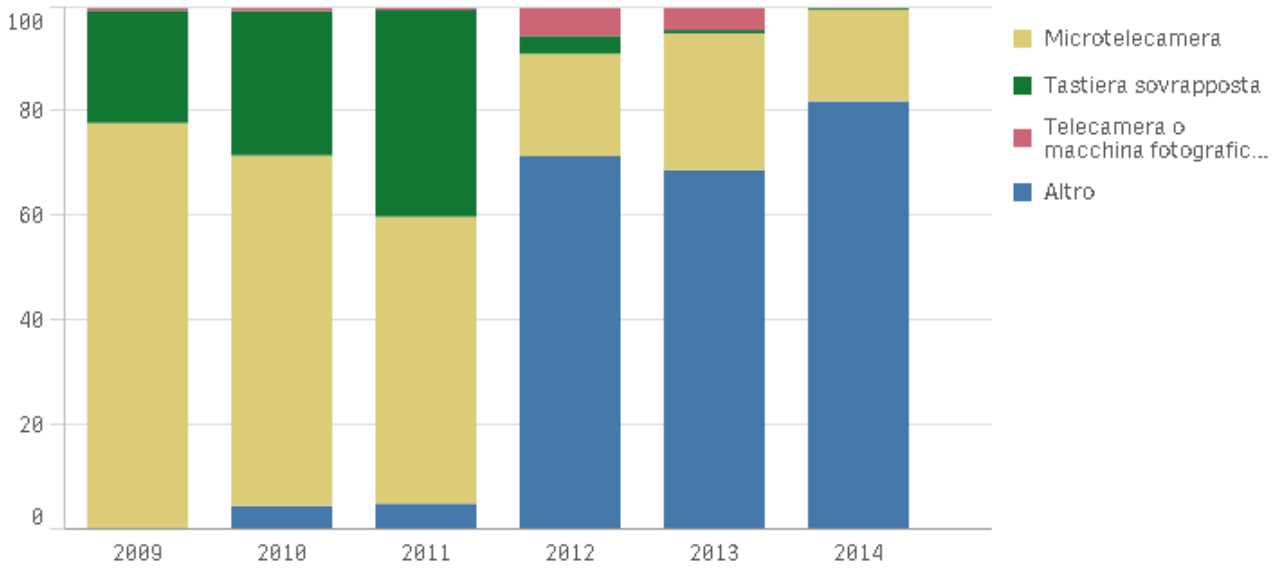


Figura 32: Tipologia di cattura del PIN

Revoche convenzioni POS

Incidenza: rapporto fra il numero revoche convenzioni su totale convenzioni attive

Numero standardizzato: Numero delle transazioni non riconosciute su carte emesse in Italia dell'anno di riferimento diviso per il numero del 2009. Un valore di 100 significa che il valore è pari a quello del 2009, un valore di 110 significa che è aumentato del 10% rispetto al 2009.

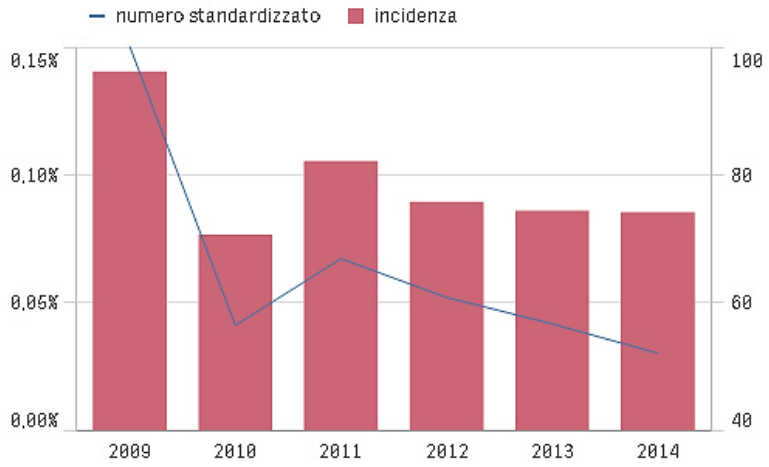


Figura 33: Numero revoche convenzioni e incidenza delle revoche su totale convenzioni attive

Incidenza 2014: 0,09 variazione percentuale 2014/2013 -8%

Figura 34: distribuzione regionale revoche convenzioni (il colore esprime l'intensità del fenomeno)

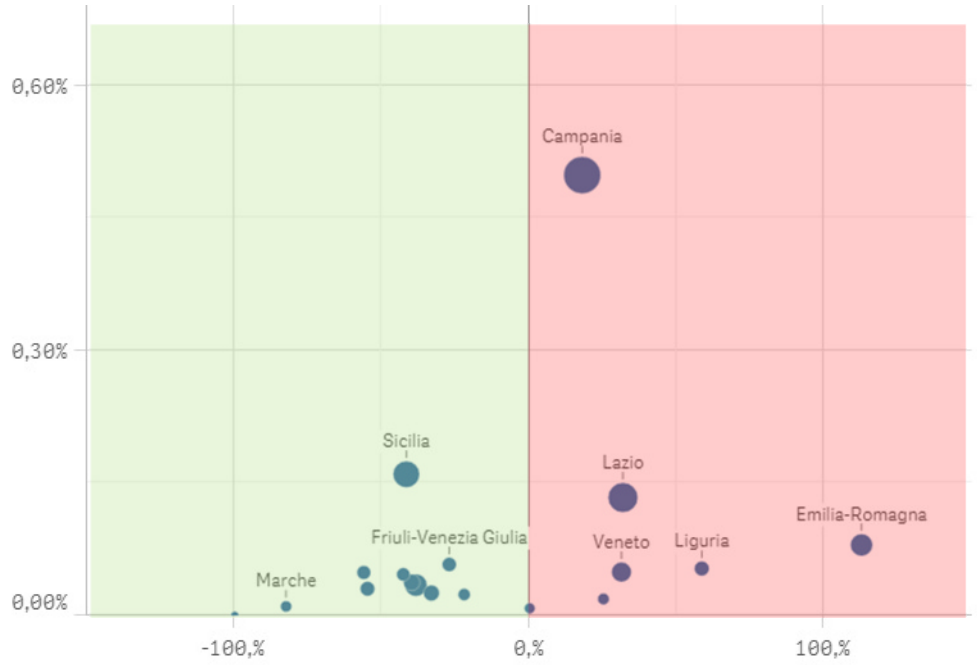


Figura 35: Variazione percentuale 2014/2013 (asse x), incidenza (asse y) e dimensione del fenomeno (dimensione bolla)

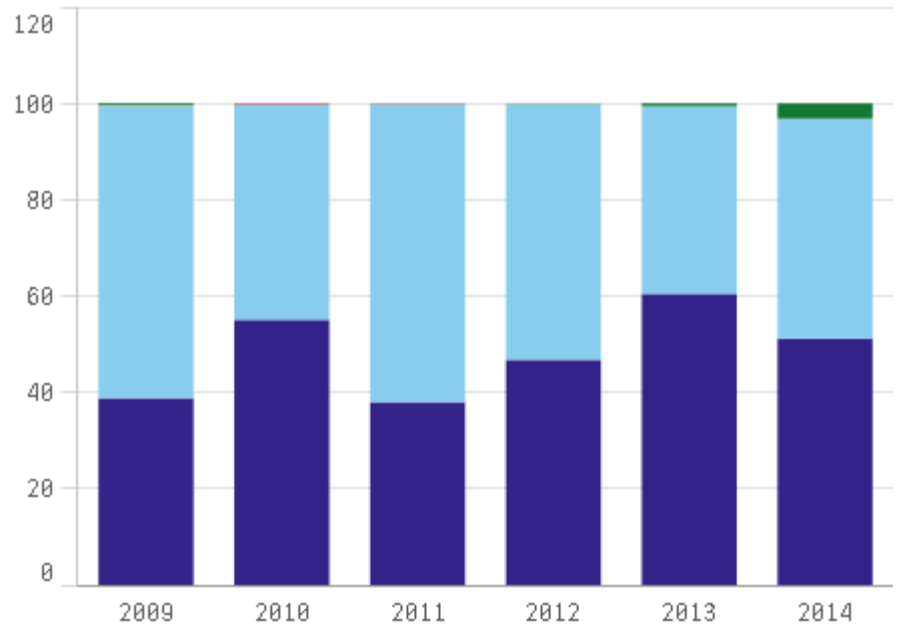


Figura 36: composizione percentuale delle causali di disconoscimento

- *Coinvolgimento dell'esercente in attività che la società segnalante ha ritenuto essere sospette ,in base a verifiche o controlli o riscontri da essa stessa effettuati*
- *Motivi di sicurezza generici*
- *Ricezione di comunicazione, proveniente da altre società che emettono o gestiscono carte di pagamento, concernente l'inosservanza colposa o dolosa dell'esercente alle norme che regolano l'accettazione in pagamento delle carte*
- *Qualificazione del punto vendita come "sospetto punto di compromissione", in base a verifiche o controlli o riscontri effettuati dalla società segnalante*
- *Ricezione di comunicazione, proveniente dalle società che gestiscono i circuiti di pagamento, concernente l'inosservanza colposa o dolosa dell'esercente alle norme che regolano l'accettazione in pagamento delle carte*

Nota criminologica

I dati relativi alle frodi in danno delle carte di pagamento emesse in Italia, riferiti sia all'anno 2014 sia al periodo 2009-2014, mettono in evidenza alcuni aspetti di particolare importanza non solo per la conoscenza e l'analisi del fenomeno, ma anche per la definizione dei possibili scenari di rischio sul breve-medio termine. In particolare, confermano la necessità di porsi in una prospettiva di più ampio respiro per poter cogliere le molteplici sfaccettature del fenomeno che emergono dai dati, come anche gli elementi di contatto con altre tipologie di illeciti. Esistono, infatti, importanti interdipendenze ad esempio tra le "payment frauds", il furto di identità, le frodi in danno dei consumatori e gli stessi cyber-crime.

La conferma del progressivo aumento del numero delle transazioni fraudolente nell'ultimo biennio e, di contro, la diminuzione del valore medio di ciascuna transazione, lasciano sottintendere la volontà di individuare ed aggirare le soglie di attenzione utilizzate dagli emittenti delle carte, riducendo così il rischio di essere identificati e condannati (cosiddetto law enforcement risk). Del resto, la parcellizzazione dei pagamenti in transazioni più frequenti, ma di importi più contenuti, rappresenta una delle tecniche più diffuse, già ampiamente sperimentate nell'ambito del riciclaggio del denaro proveniente da illecito.

In aggiunta, la maggiore frequenza con cui le carte vengono frodate per acquisti via Internet rispetto ai canali di vendita del "mondo fisico", collocano anche il contesto italiano in una tendenza che, negli ultimi anni, è divenuta sempre più globale. Viste in una "prospettiva criminale", infatti, le frodi realizzate online sono più semplici, spesso più redditizie e soprattutto meno rischiose, considerati i limiti oggettivi che ancora caratterizzano l'attività investigativa e giudiziaria e la cooperazione internazionale in materia di reati commessi in Rete. Inoltre, un sensibile aumento delle frodi online – quindi delle cosiddette card not present fraud (CNP) – deve essere letto anche come un inevitabile conseguenza dell'implementazione della tecnologia EMV, che ha rafforzato la protezione delle carte di pagamento nelle transazioni fisiche. Nella pratica, questo "effetto displacement" coincide con la necessità, da parte dei soggetti/gruppi criminali, di individuare contesti ancora vulnerabili e, in questo senso, il Web ed i Paesi con standard tecnologici più bassi rappresentano realtà di estremo interesse.

In particolare, la dimensione digitale ha una duplice peculiarità intrinseca, da un lato permette di gestire tutta la catena criminale e, dall'altro, offre una maggiore garanzia di anonimato e, quindi, di impunità.

Ad esempio, la fase preliminare di acquisizione dei numeri di carta e dei relativi dati di pagamento può avvenire online, in modo più rapido ed agevole rispetto alle tecniche di compromissione solitamente utilizzate offline. Allo stato attuale, infatti, i dati di pagamento delle carte vengono ottenuti con sempre maggiore frequenza attraverso il furto degli stessi dai database di aziende ed esercenti online [10], oppure attraverso l'acquisto nel mercato nero delle informazioni personali, particolarmente fiorente nel Deep Web [11]. Non a caso, negli ultimi due anni, le statistiche segnano un aumento anche dei casi di violazione dei sistemi informatici, con conseguente furto e compromissione dei dati personali di centinaia di migliaia di persone/account e, in determinate situazioni, di milioni di carte di credito [12]. La casistica più sofisticata

[10] EUROPOL, Situation Report. Payment Card Fraud in the European Union. Perspective of Law Enforcement Agencies, 2012.

[11] R.J. Sullivan, The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options, Economic Review, Second quarter 2010.

[12] Negli Stati Uniti, per il 2014, è stato stimato in 783 il numero di casi identificati, con un aumento del 27,5% rispetto all'anno precedente. Nel 2010 erano stati 662. Identity Theft Resource Center (ITRC), 2014 ITRC Breach List. Gennaio 2015. Inoltre, Ponemon Institute, 2015 Cost of Data Breaches Study. Global Analysis. Maggio 2015.

riporta, poi, casi di clonazione di siti e di generatori di falsi siti per trarre in inganno i consumatori e ottenere così dati di pagamento riferiti a carte attive [13].

Dopo l'acquisizione dei dati, la spendita fraudolenta della carta segue spesso una valutazione razionale dei costi e dei benefici. Il fatto che la vendita al dettaglio e all'ingrosso siano i settori più vittimizzati si pone in linea di continuità con le tendenze delle frodi a livello globale. Infatti, sebbene la spesa online abbia registrato un aumento di quasi 30 miliardi di dollari nel 2014, sono i grandi operatori di eCommerce e di mCommerce (mobile Commerce) ad essere stati maggiormente vittimizzati dalle frodi. Se i costi delle frodi sono rimasti stabili, le perdite percentuali per frode sul fatturato sono invece sensibilmente aumentate per questo segmento (da 0,51 del 2013 a 0,68 del 2014), con un incremento nel numero delle frodi stesse (133 al giorno, in aumento del 46% rispetto al 2013)[14]. Anche la vulnerabilità del settore dei viaggi – soprattutto dei trasporti – rilevata dai dati italiani trova conferma a livello europeo ed internazionale [15]. Nel trasporto aereo, le frodi corrispondono a circa 1% - 1,5% delle entrate, fino ad un massimo del 3% - 4% per le compagnie attive soprattutto nel Medio Oriente e in America Latina [16]. In questo settore, le frodi sono spesso sistemiche e perpetrate contemporaneamente verso più operatori, attraverso siti diversi ed in modo organizzato, di regola utilizzando dati rubati attraverso data breaches avvenuti negli Stati Uniti. Di recente, però, è aumentato il numero dei casi di attacchi informatici e di frodi perpetrati in ambito domestico. Ad esempio, i dati relativi al contesto britannico, evidenziano come il 53% delle carte di credito e il 76% delle utenze telefoniche utilizzate per finalità di frode sono usati più volte (in due o più casi), di contro al 33% degli indirizzi IP e al 10% degli indirizzi e-mail. Nell'85% dei casi, poi, il codice di avviamento postale fa riferimento alla città di Londra.

Infine, la Rete gioca un ruolo di primaria importanza anche per il riutilizzo dei proventi illeciti realizzati attraverso le frodi in danno delle carte di pagamento. La conversione in moneta virtuale rappresenta una nuova frontiera, ma sembra esistere una correlazione consolidata anche con il finanziamento illecito al terrorismo, con il gioco d'azzardo illegale e con i reati di traffico, soprattutto di armi e di esseri umani [17]. Del resto, la contraffazione e la falsificazione dei documenti, così come delle carte di pagamento, risultano strumentali alla maggior parte dei crimini.

Le tendenze globali delle frodi in danno delle carte di pagamento, ma anche dei cyber-crime - in particolare degli accessi abusivi ai sistemi informatici - mettono in evidenza il carattere organizzato e transnazionale dei soggetti criminali coinvolti. L'aspetto associativo, la sempre maggiore specializzazione in attività o segmenti specifici della catena criminale, la capacità di networking e collaborazione tra gruppi diversi a livello internazionale, il ricorso all'acquisto di servizi criminali attraverso il Web, sono alcuni dei tratti caratterizzanti emersi più di recente, quale risultato anche di un processo di consolidazione tra payment frauds e tecniche di hacking [18].

[13] P. Richhariya, P K Singh, Evaluating and Emerging Payment Card Fraud Challenges and Resolution, in International Journal of Computer Applications (0975 – 8887) Volume 107 – No 14, Dicembre 2014.
[14] LexisNexis, 2014 LexisNexis®, True Cost of Fraud Study. Post-Recession Revenue Growth Hampered by Fraud As All Merchants Face Higher Costs. Agosto 2014.
[15] National Fraud Intelligence Bureau, Avoiding Payment Fraud within the UK Travel Industry. Risk Factors. A case study to help eliminate credit card charge-backs. 2013.
[16] Fonte: CAPA - Centre for Aviation.
[17] A. Acharya, Targeting Terrorist Financing: International Cooperation and New Regimes, Routledge, 2009.
[18] Nel 2008, ad esempio, degli hackers riuscirono ad entrare nei sistemi informatici di RBS Worldpay – sussidiaria della Royal Bank of Scotland per la gestione dei pagamenti – accedendo ai dati di circa 1.5 milioni di titolari di carte. I dati vennero poi distribuiti nell'ambito di una rete globale di cashiers confederati, per procedere con la creazione di carte

Queste riflessioni sulle ultime tendenze nazionali e globali delle frodi lasciano presupporre uno scenario che, a breve, evolverà verso una sempre maggiore incidenza delle frodi da remoto, confermando la necessità di maggiori sforzi sia tecnologici sia – soprattutto – di cooperazione pubblico-privato. Infatti, la capacità di condivisione (in tempo reale) dei dati sulla casistica delle frodi, degli alert di rischio così come degli attacchi in corso continua ad essere strategica, perché consente di raggiungere due obiettivi fondamentali: la conoscenza e il monitoraggio della fenomenologia criminale e il rafforzamento della capacità di fare fronte comune nell'ambito della prevenzione e della gestione delle emergenze.

contraffatte. Nel frattempo, gli hackers modificarono i sistemi informatici della RBS Worldpay per aumentare il plafond delle carte e i limiti di prelievo agli ATM. Successivamente, nel giro di 12 ore, i cashiers prelevarono circa 9 milioni di dollari, da 2100 ATM, in circa 280 città.

Rischi futuri

Tra i fenomeni di maggiore interesse legati alle frodi relative alle carte di pagamento osservati nello scorso anno, vi è un rapido aumento dei reati operati in rete.

In rete esistono numerosi forum e siti internet che offrono ogni genere di prodotto, soluzione e servizio finalizzato alla realizzazione di frodi informatiche relative alle carte di pagamento.

Nei differenti forum in rete specializzati in questo genere di attività è possibile reperire lotti di dati relativi a carte di pagamento rubate, codici malevoli per infettare i sistemi di pagamento da cui estrarre i dati relativi alle carte, noleggiare botnet composte da migliaia di PC infetti da utilizzare per le campagne di spam, servizi di riciclaggio del denaro e persino guide per criminali neofiti che desiderano avviarsi a questa nuova redditizia attività.

Tra le attività più popolari nell'ecosistema criminale vi è senza dubbio quella del "carding," ovvero della commercializzazione o scambio dei dati relativi alle carte di pagamento. Queste informazioni suscitano un elevato interesse da parte di gruppi criminali e sono utilizzabili per fini come ad esempio la clonazione di carte, effettuare acquisti in rete oppure rimetterle sul mercato integrandole anche con servizi accessori. I Luoghi di scambio preferiti dalla criminalità organizzata sono sicuramente i Black Market.

Nei black market è possibile reperire non solo i dati relativi alle carte di pagamento, ma sempre con maggior frequenza è facile imbattersi in venditori che offrono anche altri servizi per agevolare le operazioni dei propri clienti o per compiere frodi più evolute.

Uno dei fenomeni che desta maggiore preoccupazione nell'ecosistema criminale è lo sviluppo di modelli di vendita di servizi illegali noto come Cybercrime-as-a-Service (CaaS).

Un numero crescente di criminali informatici ha cominciato a fornire prodotti e servizi per un'ampia gamma di attività illegali. In questo modo le organizzazioni criminali che non dispongono delle competenze indispensabili per realizzare frodi informatiche possono acquisire tutto quanto necessario nel mercato nero. Questo fenomeno rappresenta un elemento di attrattiva per il crimine ordinario che può reinvestire i proventi di altre attività illecite nel cybercrime.

Nell'underground criminale è facile incontrare venditori che offrono i propri servizi a prezzi vantaggiosi, una possibile classificazione potrebbe essere:

- Servizi relativi alla diffusione di Malware, quali lo sviluppo/personalizzazione di codici malevoli, la gestione delle infrastrutture di controllo, il noleggio di botnet, etc.
- Exploit kit, ovvero la vendita di codici malevoli che una volta installati su domini gestiti dalle organizzazioni criminali consentono di sfruttare falle all'interno di applicazioni comuni (e.g. Adobe Flash) o nei Web Browser per installare malware di vario genere.
- Servizi professionali, come servizi di hacking, riciclaggio di denaro, servizi per il cash out, training e tutorial.

Il modello CaaS risulta particolarmente efficace per la realizzazione di ogni genere di attività legata alle frodi per le carte di pagamento. Escludendo i servizi di e-learning e "formazione" sulle attività di carding o di cash out, senza dubbio i servizi di maggior interesse per la realizzazione di frodi relative alle carte di pagamento sono i servizi di carding e tutto quanto concerne lo sviluppo e la diffusione di malware per infettare sistemi

di pagamento. In numerosi forum è possibile reperire i codici sorgenti di tali malware ed è possibile pagare affinché sia installata e gestita l'infrastruttura di controllo, ovvero la componente che gestisce i codici malevoli che hanno infettato i sistemi di pagamento e che collezionano i dati relativi alle carte di pagamento.

Anche in questo caso i prezzi sono estremamente variabili, la personalizzazione del codice sorgente di un malware per infettare i sistemi PoS può arrivare a costare anche un migliaio di euro, mentre il costo dei soli codici sorgenti oscilla tra i 500 ed i duemila dollari.

Il costo di un drive-by download web toolkit, comprensivo di aggiornamenti e supporto di 24 ore su 24 per sette giorni su sette è compreso tra i $100 ed i $700 a settimana. Gruppi criminali possono noleggiare anche banking malware come SpyEye che è offerto per una cifra che oscilla tra i $150 to $1,250 per semestre.

Un altro tipo di servizi molto popolare nell'ecosistema criminale sono i servizi di riciclaggio dei proventi delle attività illegali mediante monete virtuali.

Le monete virtuali come i Bitcoin sono uno strumento privilegiato per gruppi di criminali che intendono riciclare denaro. Sebbene tale attività può essere gestita depositando e prelevando moneta virtuale in uno dei numerosi servizi di cambio online (exchanger) online, tipicamente le organizzazioni criminali preferiscono rivolgersi a servizi specializzati nell'underground che operano riciclando denaro attraverso molteplici canali e metodi, incluse carte di pagamento virtuali e reti di account presso servizi di exchanger che convertono monetica virtuale.

Particolarmente interessanti sono servizi di riciclaggio offerti da alcuni operatori attraverso la rete Tor, servizi in genere denominati 'tumblers' o 'mixers'.

I tumblers ("Bicchieri") sono servizi che operano prevalentemente attraverso la rete Tor e che consentono agli utenti di trasferire i propri fondi virtuali (e.g. Bitcoin) in un pool di fondi che poi rientrano attraverso account leciti una volta ripuliti. Le organizzazioni dietro questa attività trattengono per se una piccola commissione.

In ognuno dei numerosi black market o hacking forum presenti in rete è possibile noleggiare intere infrastrutture per gestire una botnet oppure per organizzare varie tipologie di frodi online.

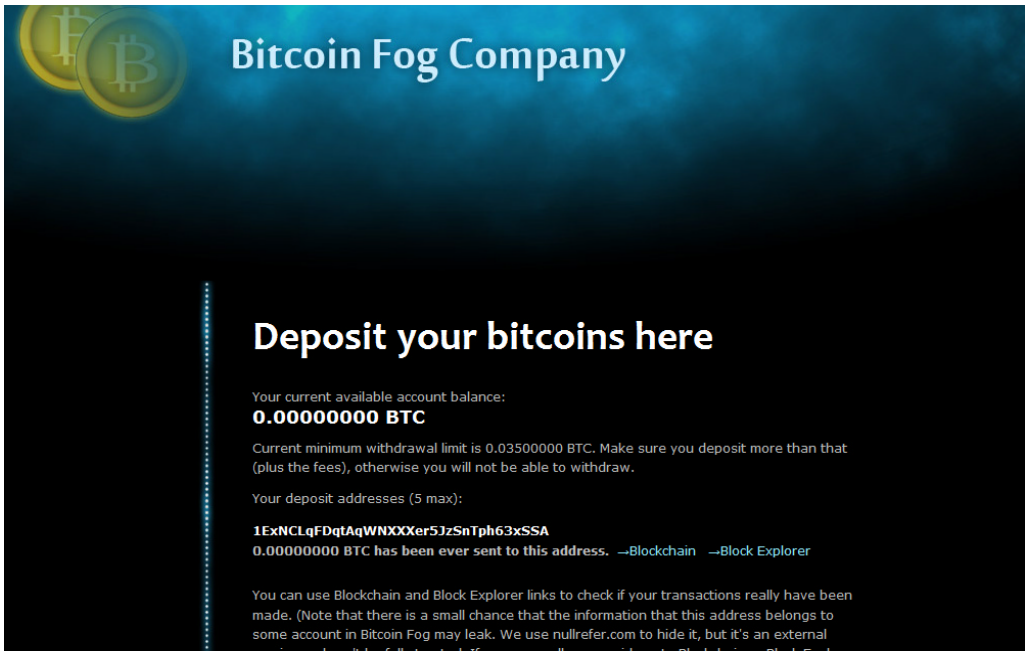


Figura 37 - Bitcoin Fog Onion Service

Di solito servizi come Bitcoin Fog ripartiscono l'ammontare depositato da ciascun utente in un numero casuale dei pagamenti. I versamenti di rientro sono distribuiti su un arco temporale causale così come casuali sono gli importi dei versamenti.

Altra opzione per gruppi di criminali dediti al riciclaggio sono i servizi di gioco d'azzardo on-line. Gruppi di criminali riciclano proventi illegali pagando, giocando e incassando con monete virtuali oppure utilizzando direttamente dati relativi a carte di pagamento rubate.

Alcune di queste piattaforme sfruttano il livello di anonimato offerto dalla rete Tor.

Il modello del cybercrime-as-a-service è destinato a consolidare la sua popolarità nell'ecosistema criminale ed a divenire un volano per ulteriori attività illecite. Le frodi relative alle carte di pagamento sono tra le attività che più di tutte possono beneficiare dall'adozione di questo modello.

Approfondimento monotematico

I Black Market

2014 I Black Market e Operation Onymous

Molti forum in internet offrono prodotti relativi ad attività illegali connesse alle carte di pagamento, la maggior parte di questi servizi web è nascosto all'interno di reti di anonimizzazione come la rete Tor.

Tra le comunità più attive nella commercializzazione di dati relativi a carte di pagamento in rete, potremo citare *embargo.cc*, *rescator.cm* e *netsky.bz*, sebbene la maggioranza delle vendite avvenga attraverso mercati specializzati nel Dark Web.

Comunità criminali prediligono le dark net ospitate in reti come Tor per via dell'anonimato che esse offrono, rintracciare venditori e acquirenti è impresa tutt'altro che facile e richiede un notevole sforzo da parte delle autorità competenti.

Altro elemento a favore di questi mercati paralleli è la possibilità di effettuare pagamenti utilizzando moneta virtuale, come il Bitcoin, che fornisce un ragionevole livello di anonimato delle transazioni.

Uno degli elementi che influenzano l'affidabilità di venditori, e talvolta di intere dark net, è la disponibilità di servizi escrowing (Acconto di garanzia).

Il prezzo dei dati relativi alle carte di pagamento si è progressivamente ridotto nel corso degli ultimi anni e tale flessione è principalmente imputabile alla aumentata disponibilità di dati relativi a carte di pagamento rubate. Tale disponibilità è conseguenza degli innumerevoli incidenti occorsi negli ultimi anni e che hanno portato al furto di dati relativi a diverse centinaia di milioni di carte di pagamento in tutto il mondo.

Navigando nei principali siti che offrono dati relativi alle carte di pagamento è facile imbattersi in termini come "CVV" e "Dump." Il termine CVV, che non deve essere confuso con il codice composto da tre cifre e presente sul retro della carta di credito, è utilizzato dagli operatori dell'underground criminale specializzati nella commercializzazione delle carte di pagamento per indicare i record relativi alla carta e che possono includere il nome dell'intestatario, l'indirizzo dell'intestatario, la data di scadenza ed il CVV2 che è il codice presente dietro la carta. I CVV possono essere utilizzati solo per frodi online, anche dette "Card No Present fraud" (CNP). Il prezzo medio di un CCV relativo ad una carta di credito statunitense è di poco superiore alla decina di dollari.

Il termine Dump è invece utilizzato per indicare i dati grezzi immagazzinati nella banda magnetica di una carta di credito, informazioni di solito catturate mediante attività di "skimming" oppure attraverso l'uso di malware che infettano i sistemi di pagamento PoS.

I dati componenti un DUMP possono essere utilizzati dai criminali informatici per clonare carte di pagamento e utilizzare le carte prodotte per prelievi presso gli ATM delle banche o per pagamenti in cui è necessaria la presenza fisica della carta. I prezzi dei DUMP sono generalmente superiori a quelli dei CVV in quanto i criminali possono utilizzarli per acquistare beni di valore superiore. Il Dump di una carta di credito può arrivare anche a superare i 100$ se la carta è relativa ad un cliente Top e quindi ha disponibilità finanziari superiori.

Riassumendo, il prezzo dei dati relativi a carte di pagamento statunitensi (CVV US) arriva fino a 10 dollari mentre per una carta relativa ad un cittadino europeo si può arrivare a spendere una cifra che varia dai 5 ai 25 dollari. Il prezzo è superiore se i dati includono il contenuto delle tracce presenti nella banda magnetica della carta (DUMP), per cui si potrebbe arrivare a pagare ciascun pezzo diverse decine di euro.

Prima di analizzare la diffusione delle attività illegali relative alle carte di pagamento nel deep web è opportuno citare gli eventi che maggiormente hanno influenzato l'ecosistema criminale lo scorso anno.

Uno degli eventi che ha avuto il maggiore impatto sull'ecosistema criminale lo scorso anno è stata l'operazione condotta dalle forze dell'ordine di vari paesi, denominata Operazione Onymous. Nel Novembre 2014 l'operazione è culminata con il sequestro di decine di "black market" nascosti nei meandri nella rete di anonimizzazione Tor. Tra i siti posti sotto sequestro vi è il popolare Silk Road 2.0, nato settimane dopo l'arresto da parte dell'FBI del gestore della piattaforma Silk Road, Ross Ulbricht.

Fortunatamente la ricerca di soluzioni per la messa in sicurezza delle operazioni relative alle carte di pagamento sta compiendo passi da gigante rendendo l'utilizzo delle carte sempre più sicuro. I dati dimostrano che le principali organizzazioni europee sono all'avanguardia nella ricerca e nell'adozioni di nuovi sistemi per la prevenzione, l'identificazione e la mitigazione delle frodi relative alle carte di pagamento.

Approfondimento sui Black Market nella rete Tor

Alla stesura del presente rapporto i principali black marker attivi in rete TOR erano i seguenti:

Black Market	Indirizzo Onion rete Tor	N° prodotti	N° prodotti per frodi con carte di pagamento	%
Abraxas	abraxasdegupusel.onion	7590	60	0,79%
Agora	agorahooawayyfoe.onion	24110	80	0,33%
AlphaBay	pwoah7foa6au2pul.onion	16150	735	4,55%
Nucleus	nucleuspf3izq7o6.onion	17361	80	0,46%
Outlaw	outfor6jwcztwbpd.onion	NA	NA	NA
Italian DarkNet Community	2qrdpvonwwqnic7j.onion	104	28	26,92%
Dream Market	ltxocqh4nvwkofil.onion	2068	30	1,45%
Haven	havenpghmfqhivfn.onion	720	10	1,39%
Middle Earth	mango7u3rivtwxy7.onion	5256	22	0,42%

Tabella 1 Black Market analizzati

La tabella riporta per ciascuna comunità il numero totale di prodotti offerti e quali tra essi è riconducibile a frodi relative alle carte di pagamento.

Dall'analisi dei dati si evince che le comunità Italian Darknet Community ad AlphaBay sono quelle più attive per quanto concerne la vendita di prodotti relative a carte di pagamento.

Percentuale dei prodotti inerenti frodi con carte di pagamento per singolo Black Market

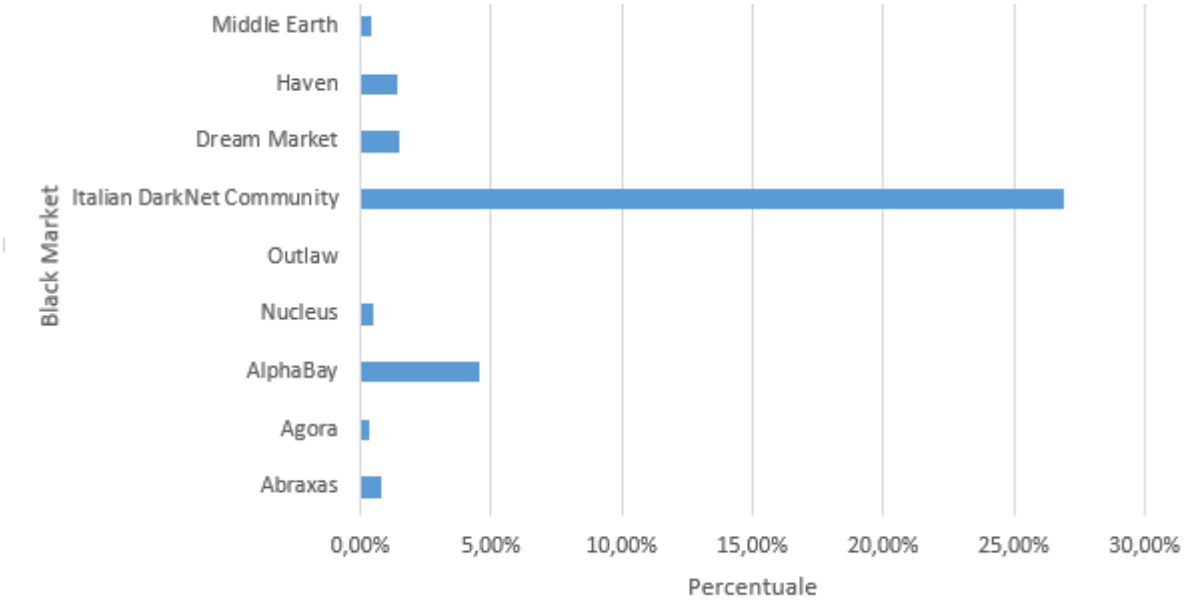


Figura 38 - Principali black market che offrono prodotti relative alle frodi con carte di pagamento

Sebbene la comunità "Italian Darknet Community" non sia comparabile per volume di affari ad AlphaBay vale la pena analizzarla per comprendere come attori italiani si stiano posizionando nell'ecosistema criminale. I venditori del mercato Italian Darknet Community offrono carte di pagamento e carte prepagate per i principali circuiti internazionali ad un prezzo che varia da poche decine di dollari sino a circa 125 dollari. Interessante notare la disponibilità di carte prepagate che offrono la possibilità di creare carte virtuali collegate al medesimo conto e che sono ricaricabili anche in Bitcoin. Tali carte rappresentano uno strumento indispensabile per le organizzazioni criminali che le utilizzano per i processi di cash out, ovvero di conversione in valuta delle proprie attività illecite. Tali carte sono di solito utilizzate per prelevare fisicamente il denaro presso gli sportelli bancomat, spesso sono anche utilizzate per truffe su eBay o per acquistare beni di vario genere nel dark web (e.g. droga, armi, beni, soldi e documenti contraffatti).

In quasi tutti i mercati analizzati è possibile acquistare corsi di carding che spiegano come operare in sicurezza, preservando l'anonimato delle transazioni. Tali corsi sono offerti ad un prezzo che oscilla dai 250 ai 500 euro e offrono una durata variabile sino al raggiungimento dell'autonomia dei corsisti.

In comunità come Italian Darknet Community le carte non italiane sono offerte a prezzi che variano da 15 euro ai 40 euro, in mesi di osservazione solo pochi utenti hanno offerto carte di pagamento statunitensi a prezzi che oscillano tra gli 8 ed i 25 euro, mentre i prezzi per FULLZ statunitensi non superano i 35 dollari. I prezzi della comunità italiana in taluni casi appaiono superiori rispetto ad altri black market, situazione che suggerisce che alcuni degli attori del black market italiano rivendano a loro volta dati relativi a carte di pagamento rubate ed acquistati su altri market.

In molti dark market i venditori offrono servizi di carding su commissione in cui il cliente deve esprimere la propria preferenza per un oggetto (e.g. Uno smartphone, un pc, un notebook) ed il venditore provvede ad acquistarlo per soddisfare la richiesta. L'oggetto è tipicamente rivenduto ad un prezzo molto inferiore di quello originale, tipicamente il prezzo di vendita varia dal 40 al 60 percento del valore di mercato dell'oggetto.

Altri servizi acquistabili nei principali marketplace sono i servizi di consegna, anche detti Full Drop Service, che sono forniti da un numero limitato di venditori i quali offrono anche la possibilità di escrowing per i loro servizi.

Caso Studio – Il mercato nero AlphaBay Market

Analizzando i dati collezionati sui principali black market è possibile verificare che AlphaBay è tra i principali mercati per quanto riguarda frodi relative alle carte di pagamento. I venditori che affollano il mercato propongono praticamente tutto il necessario per la realizzazione di frodi relative alle carte di pagamento. L'offerta include credenziali di accesso per gli account dei principali servizi di online banking, CVV e DUMP di carte di pagamento, plastiche, e servizi di vario genere che agevolano il compito delle organizzazioni criminali.

Come in molti altri dark market, i prodotti più venduti sono le sostanze stupefacenti, tuttavia il mercato AlphaBay è caratterizzato da una comunità di venditori molto attiva nell'offerta di prodotti per la realizzazione di frodi di vario tipo.

Categoria Merceologica	Numero offerte
Frodi	3.693
Droghe e sostanze chimiche	7.367
Elementi contraffatti	373
Prodotti Digitali	1.229
Oro e preziosi	213
Armi	205
Elemento relativi a carte pagamento	251
Servizi	816
Software & Malware	132
Security ed Hosting	45
Guide e Corsi	1.511
Altro	315

Tabella 2 Categorie merceologiche del Black Market AlphaBay

Analizzando in dettaglio la categoria Frodi si evince che circa un prodotto su cinque tra quelli offerti è relativo ad attività illegali inerenti le carte di pagamento.

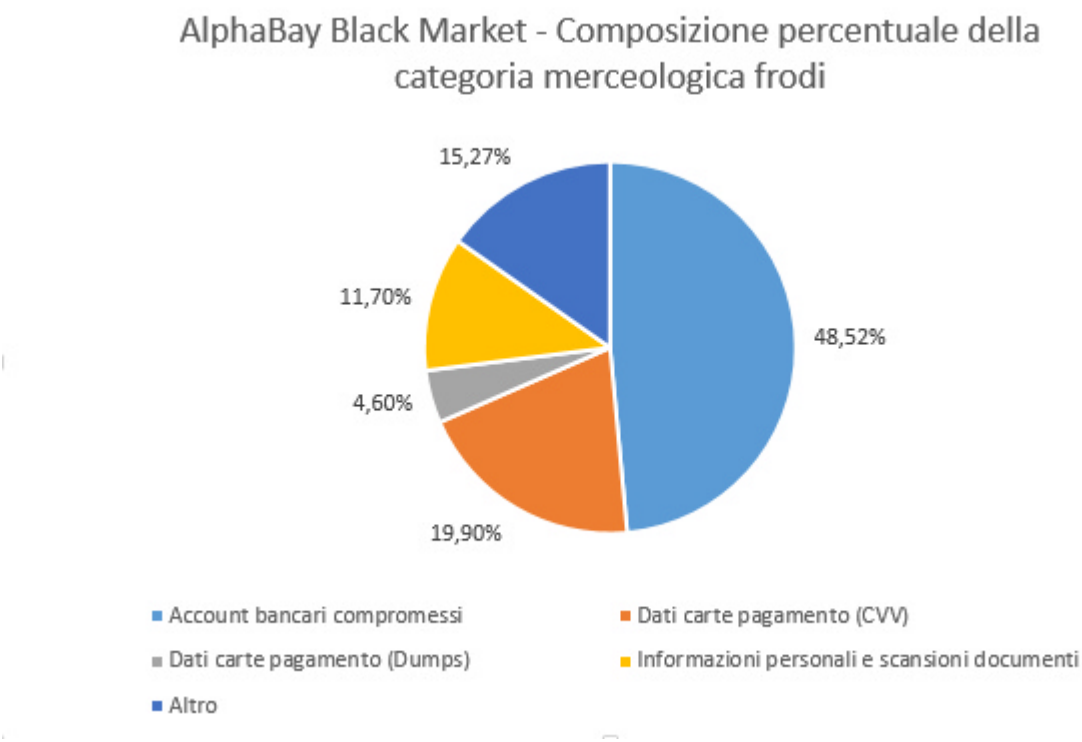


Figura 39 AlphaBay Black Market - Analisi Categoria Merceologica Frodi

Il servizio AlphaBay offre dati relativi a carte di pagamento di tutto il mondo, tra i venditori si riconoscono molti dei principali attori che già operavano in molti dei principali black market colpiti dalle forze dell'ordine nel 2014 grazie all'operazione Onymous.

AlphaBay premia i migliori venditori attraverso un meccanismo di reputazione basato su feedback, i principali "seller" in alcuni casi hanno effettuato diverse migliaia di vendite concluse con la totale soddisfazione dei propri clienti.

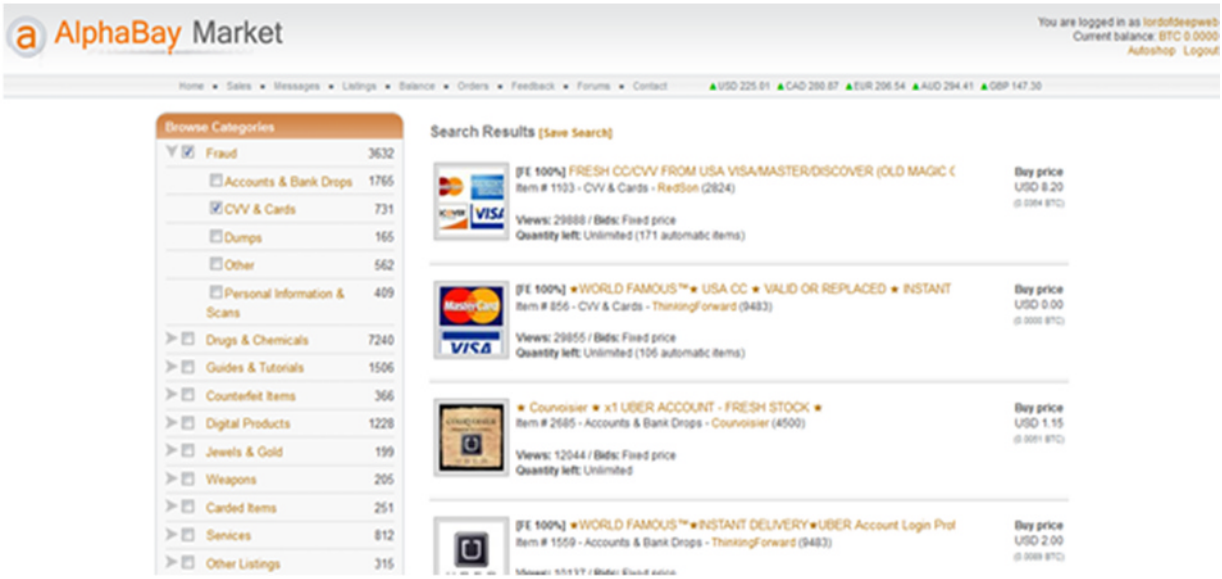


Figura 40 - AlphaBay Market

Analizzando i venditori in base alla loro reputazione è possibile rendersi conto che il maggior volume di affari è legato ad offerte relative a carte di pagamento di cittadini britannici, seguite da USA ed Australia.

Tali informazioni sono in linea con i dati proposti nei precedenti rapporti SIPAF relative alla connotazione geografica delle attività criminali legate alle carte di pagamento. Nel precedente Rapporto statistico carte 2014, nella sezione "Confronti internazionali" si evidenziava come a parità di tipologia disconoscimento, la Francia ed il Regno unito, a partire dal 2011, subivano più del triplo delle perdite rispetto all'Italia. La principale tipologia di frode risultava essere di tipo "Carta non presente". Nel Regno Unito, in Francia ed in Australia le transazioni non riconosciute con questa causale risultavano maggiore del 60%, questo dato trova riscontro nella disponibilità di dati relativi alle carte di questi paesi, nell'underground criminale. Risulta tutt'ora semplice reperire CVV e DUMP relativi a carte provenienti dalle nazioni sopra citate rispetto a paesi come l'Italia.

I "FULLz" relativi a carte provenienti da vari paesi, in particolare dal Regno Unito, sono venduti in AlphaBay ad prezzo che oscilla da poco più di 20 euro a 60 euro. Per quanto concerne i dati relative a carte di pagamento associate a conti con elevate disponibilità garantita dai venditori (Credit limit compresi tra un minimo di 10,000 euro e 200,000 euro), si osservano prezzi da 40 euro a salire per un FULLz. Anche in questo caso il maggior numero di CC Fullz è proveniente dal Regno Unito, ma non mancano altre nazioni. Nel seguente grafico sono riportate le percentuali relative all'offerta dei venditori di AlphaBay di dati relativi a carte di pagamento appartenenti a clienti di istituti finanziari di diversi paesi. Per la composizione del grafico sottostante è stato analizzato circa il 25 percento delle offerte relativi a prodotti inerenti le frodi con carte di pagamento.

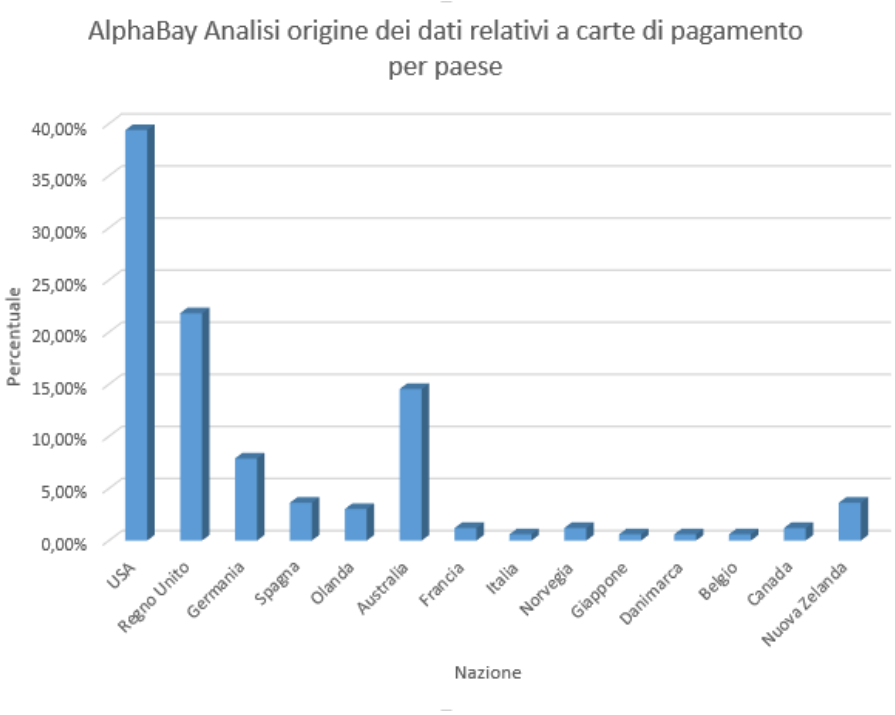


Figura 41 – Analisi origine dati relativi a carte di pagamento per Paese offerte nel black market AlphaBay

Alcuni venditori aventi migliaia di feedback positivi offrono "validity rate" (garanzia di validità dei dati relativi alla carta di pagamenti negoziata) superiori al 90 percento, sebbene in taluni casi essi non forniscono garanzie sulla disponibilità finanziaria dei conti legati alle carte i cui dati sono in vendita.

In AlphaBay è possibile pagare per tutorial e servizi di carding personalizzati, proprio quest'ultimi sono offerti con percentuali più basse rispetto ad altri mercati.

Altra caratteristica che contraddistingue i venditori di questo mercato è l'elevata turnazione della merce in vendita, alcuni venditori riescono ad aggiornare le proprie scorte una o due volte la settimana, mentre altri sostengono di poter offrire merce nuova su base giornaliera.

Non vi è dubbio, l'offerta di AlphaBay Market per le frodi relative a carte di pagamento è tra le più complete di quelle reperibili nel web.

Black Markets – Riepilogo

Completata l'analisi dei principali black market e delle relative offerte, riassumiamo ora, quali sono i principali servizi e prodotti disponibili ed i relativi costi.

I prezzi riportati nella tabella seguente sono relativi ai differenti prodotti disponibili nei vari mercati analizzati nel corso della nostra indagine. I prezzi sono riferiti a pezzi singoli e sono da ritenere indicativi in quanto le quotazioni restano estremamente variabili e possono essere oggetto di variazione qualora gli acquirenti intendano acquistare lotti contenenti dati di centinaia o migliaia di carte di pagamento.

Tali prezzi, come sottolineato in precedenza, dipendono da molteplici fattori, tra cui la provenienza geografia dei dati, l'importo minimo garantito e la data di scadenza delle carte di pagamento, la disponibilità di servizi accessori come l'escrowing oppure il carding personalizzato.

Prodotto	Prezzo
CVVs	
Vista and Master Card CVV (US)	$3-$20
American Express CVV (US)	$5-$20
Vista and Master Card CVV (EU)	$15-$30
Vista and Master Card CVV (Australia)	$8-$10
Vista and Master Card CVV (Canada)	$6-$15
DUMPs	
Vista and Master Card Dump (US)	$20-$45
American Express DUMP (US)	$25-$50
Vista and Master Card DUMP (EU)	$35-$60
Vista and Master Card DUMP (Australia)	$45-$50
Vista and Master Card DUMP (Canada)	$35-$50
FULLz	
US FULLz	$25-$100

EU FULLz	$30-$125

Tabella 3 Prezzi medi dei dati relativi a carte di pagamento

Il caso SNAI

SNAI è uno dei principali operatori del mercato del gioco autorizzato e proprio in virtù di questa sua visibilità nel corso del 2013 (in particolare nel periodo febbraio-giugno 2013) il sito di gioco SNAI è stato oggetto di sistematiche aggressioni da parte di organizzazioni criminali che utilizzavano – esclusivamente su piattaforme di gioco di abilità a torneo - la tecnica della "*collusion*" e soprattutto del "*chip dumping*".

Nella *collusion* due o più persone che siedono a un tavolo collaborano insieme per ottenere un vantaggio sugli avversari. Nel chip dumping, invece, due soggetti, il *dumper* (il giocatore perdente) e il *receiver* (il giocatore vincente) si passano deliberatamente i fondi di gioco, non attuando quindi un comportamento di gioco conforme con quello tenuto da un normale giocatore (es. il dumper passa la mano facendo vincere il receiver malgrado abbia un poker vincente).

La modalità di frode tipica in sostanza consiste nell'aprire un nuovo conto di gioco usando credenziali fittizie o rubate, alimentarlo attraverso carte di pagamento sottratte e giocare con l'obiettivo di perdere velocemente la somma caricata sul conto nuovo verso un giocatore titolare di conto di gioco regolarmente profilato (evidentemente colluso con il precedente). Il giocatore vincente provvede poi a prelevare la vincita nei tempi e nei modi consentiti.

Il ruolo del Concessionario di gioco on-line è quello di amministrare i conti di gioco dei propri clienti, garantire che i depositi e i prelievi avvengano in sicurezza e nei termini stabiliti e offrire ai giocatori un'offerta di gioco attrattiva e di semplice utilizzo, assicurando nel contempo il monitoraggio del processo di gioco a tutela degli stessi giocatori. Questa tipologia di frodi prevede che sia le identità utilizzate sia gli strumenti di pagamento siano frutto di furti operati al di fuori del sito di gioco e prima di effettuare le frodi stesse.

Benché SNAI sia uno storico Concessionario di Stato e abbia da sempre osservato rigorosamente tutte le normative in vigore, ha dovuto studiare a fondo il fenomeno al fine di adottare una serie di accorgimenti per limitare e auspicabilmente evitare i tentativi di frode. Per fare ciò SNAI ha collaborato sistematicamente con le forze dell'ordine su più piani:

- indentificare e implementare ogni ulteriore accorgimento per contrastare il fenomeno;
- creare un sistema capace di fornire alle forze dell'ordine ogni informazione utile al contrasto all'illegalità in tempi rapidi e garantendo il massimo dettaglio e quantità di informazioni utili;
- collaborare attivamente con le istituzioni per suggerire interventi normativi volti al contenimento del fenomeno.

Il lavoro è stato svolto con il contributo del Compartimento Polizia Postale di Firenze tramite la Sezione della Polizia Postale di Lucca e ha portato all'identificazione di una serie di interventi, tecnici e di presidio.

Tutti gli accorgimenti tecnici sviluppati da SNAI non sono standard normativi. Questo rende le scelte operate da SNAI a volte impopolari, in quanto i limiti imposti possono determinare la percezione nel giocatore di ricevere un'offerta commerciale meno accattivante di quella di altri operatori che non abbiano assunto i medesimi provvedimenti.

Grazie agli interventi apportati, la situazione relativa alle frodi sul sito di gioco SNAI è rapidamente rientrata nella norma, ma è comunque necessario un continuo e costante monitoraggio per evitare che gli accorgimenti attuati vengano bypassati.

Misure di prevenzione e contrasto, iniziative e novità tecnologiche

Nello scorso anno gli eventi fraudolenti occorsi nel mondo delle carte di pagamento hanno visto cambiare sia le metodologie sia le tecniche di attacco.

La diffusione dei servizi web, infatti, unita all'utilizzo sempre più massivo degli *smartphone* ha portato alla nascita di nuove modalità di pagamento come ad esempio "*One Click*" per i pagamenti da remoto, le *App* e i *Wallet* per la telefonia mobile e gli HCE (*Host Card Emulation*) per i pagamenti in prossimità. Sono stati inoltre resi disponibili altri servizi di pagamento che sfruttano i vari aspetti della multicanalità, integrandoli tra di loro, come ad esempio la possibilità di acquistare beni tramite web ma confermare i dati del pagatore con un "*wallet*" gestito tramite il canale mobile.

Parallelamente allo sviluppo di questi nuovi servizi abbiamo quindi assistito ad un vero e proprio "salto di qualità" delle organizzazioni criminali che hanno assunto negli ultimi anni una connotazione sempre più globale: il business criminale infatti si avvale di strutture organizzate e specializzate, con ramificazioni a livello mondiale. Tali strutture poi possono operare in modo sinergico, sfruttando le proprie competenze, allo scopo di creare prodotti e servizi con i quali svolgere l'attività malavitosa.

Con queste premesse, a contrasto delle frodi, diventa necessario e fondamentale introdurre iniziative ad alto contenuto tecnologico e che permettono di intervenire, ove possibile, fin dai processi autorizzativi.

Con l'introduzione di sistemi di pagamento da remoto, basati sul possesso di credenziali di accesso, il riconoscimento del titolare del rapporto assume un aspetto molto più delicato rispetto a quello che si può avere in un contesto in cui c'è la presenza fisica della carta. Si ritiene, pertanto, molto importante che l'autorizzazione ad operare nel mondo dei pagamenti virtuali sia legata al riconoscimento del cliente non solo tramite la "*strong authentication*" ma anche attraverso uno serrato monitoraggio dell'attività del titolare della carta in fase di utilizzo del servizio.

In questo contesto un'altra attività che può supportare in modo efficace la prevenzione delle frodi è quella che riguarda l'analisi relativa all'integrità della sicurezza dei dispositivi utilizzati. Ad esempio, se prendiamo in considerazione la vulnerabilità di alcuni sistemi operativi presenti negli *smartphone*, poter rilevare anticipatamente il livello di sicurezza dello strumento potrebbe portare a decidere quali funzionalità di un'*App* concedere o addirittura se consentire a quell'apparecchiatura mobile l'utilizzo della stessa. Si fa presente che il livello di sicurezza rientra spesso nel calcolo dello "*scoring*" della transazione ovvero del complesso di valutazioni che portano un soggetto a concedere/negare l'autorizzazione di una transazione.

Il processo autorizzativo di un'operazione di pagamento è senza dubbio uno dei momenti più critici della transazione. In pochissimo tempo, il sistema di "*Fraud Management*" deve dare un responso in termini di rischiosità della transazione. Da qui la necessità di disporre di validi elementi in grado di determinare lo *scoring* di rischio e decidere, eventualmente, anche per il blocco dell'operazione.

Se andiamo invece ad analizzare le casistiche dove si riscontra la presenza "fisica" della carta, si osserva che negli ultimi tempi sono stati rilevati degli attacchi fraudolenti effettuati tramite apparecchiature POS che fino a poco tempo fa erano considerati puramente casi di scuola.

Al fine di aggirare la difficoltà di "leggere" i dati contenuti nei chip – cosa che non è possibile se non con tempi molto lunghi e tecnologie estremamente sofisticate, che rendono "antieconomica" la frode – i frodatori hanno sviluppato una nuova tecnica che prevede una prima fase in cui vengono catturati i dati relativi ad alcune carte attraverso la "lettura" dei messaggi autorizzativi generati in occasione di una transazione su POS e una seconda nella quale replicano o costruiscono ad arte i messaggi di "richiesta di autorizzazione", completandoli con i dati carpiti e immettendoli direttamente nel circuito. Per contrastare questo fenomeno, scoperto e segnalato dai circuiti di pagamento internazionali, occorre effettuare una disamina puntuale dei tracciati dei messaggi, sia per quelli gestiti direttamente dagli *issuer* sia per quelli la cui gestione viene demandata a terzi, delle transazioni per scoprire eventuali anomalie.

In ultimo, ma non certo per ordine di importanza, nel corso del 2014 sono state rilevate una serie di violazioni ai sistemi informatici di soggetti emittenti, di soggetti che accettano i pagamenti, di esercenti commerciali, finalizzati alla cattura dei database contenenti i dati delle carte di pagamento. Tale violazione è funzionale non solo alla sottrazione dei dati delle carte ma anche per variare i parametri autorizzativi delle carte (già in possesso dell'organizzazione criminale), aumentando considerevolmente i massimali di spesa e in parallelo definire un profilo prodotto in grado di bypassare i controlli autorizzativi o di prevenzione frode.

La sicurezza degli accessi ai sistemi informatici e la protezione delle informazioni sono ormai diventate condizioni essenziali per poter operare in sicurezza nel mondo dei sistemi di pagamenti.

La prevenzione nel settore privato ha visto, nel recente passato, il consolidarsi degli strumenti "passivi" quali:

- AVS (*Address Verification System*) è un dispositivo di sicurezza che controlla che l'indirizzo utilizzato dall'utente in fase di ordine coincida con quello associato effettivamente alla carta di credito, così come risulta nel database delle società emittenti. Questo sistema non è attualmente utilizzato in Italia;

- richiedere obbligatoriamente un numero telefonico di rete fissa, se si sospettasse una frode o se il cliente stia acquistando per la prima volta;

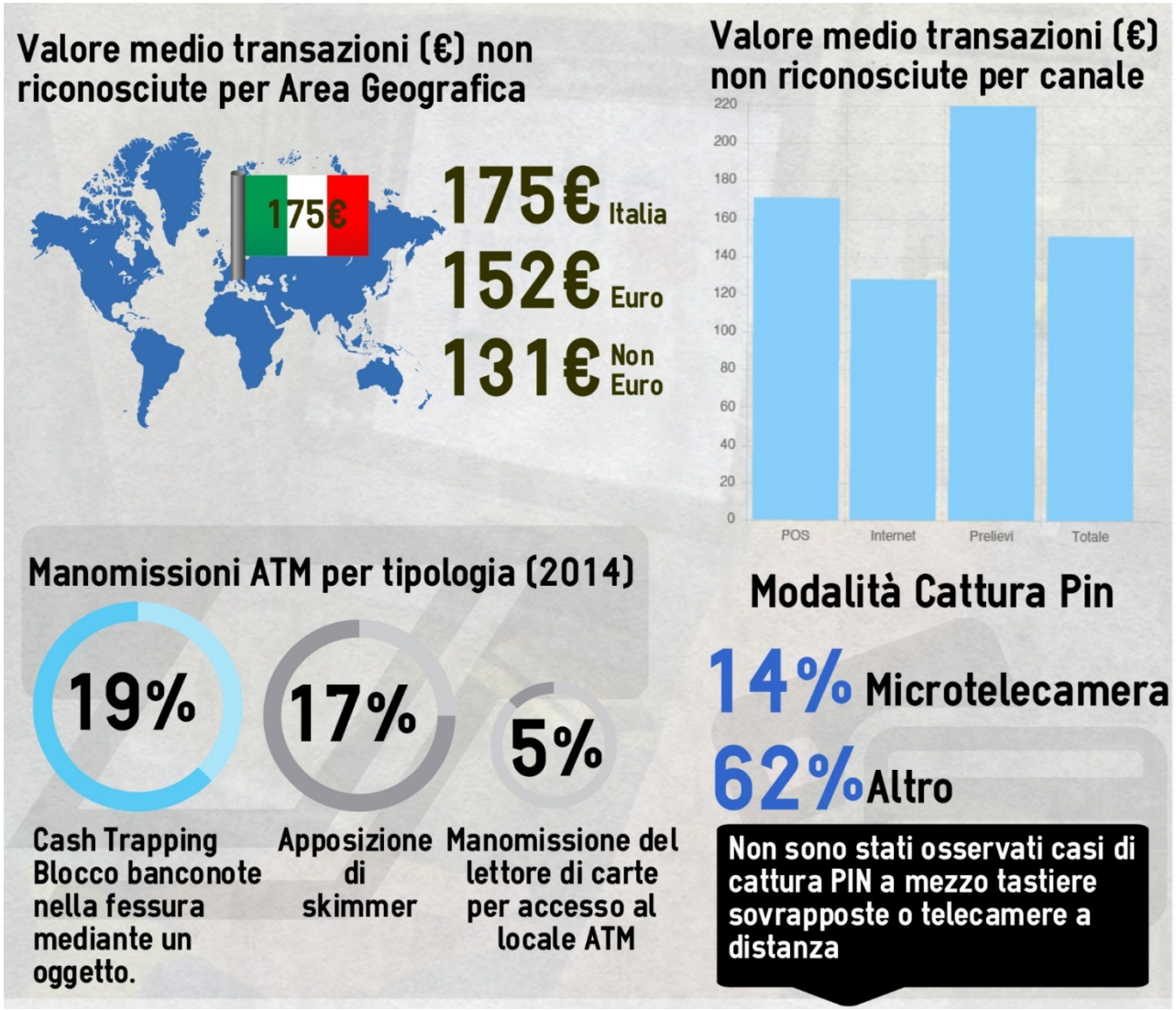
- esaminare l'indirizzo inserito per la spedizione e se possibile, l' indirizzo IP da cui proviene l'ordine, per verificarne l'effettiva corrispondenza all'area di destinazione della merce;

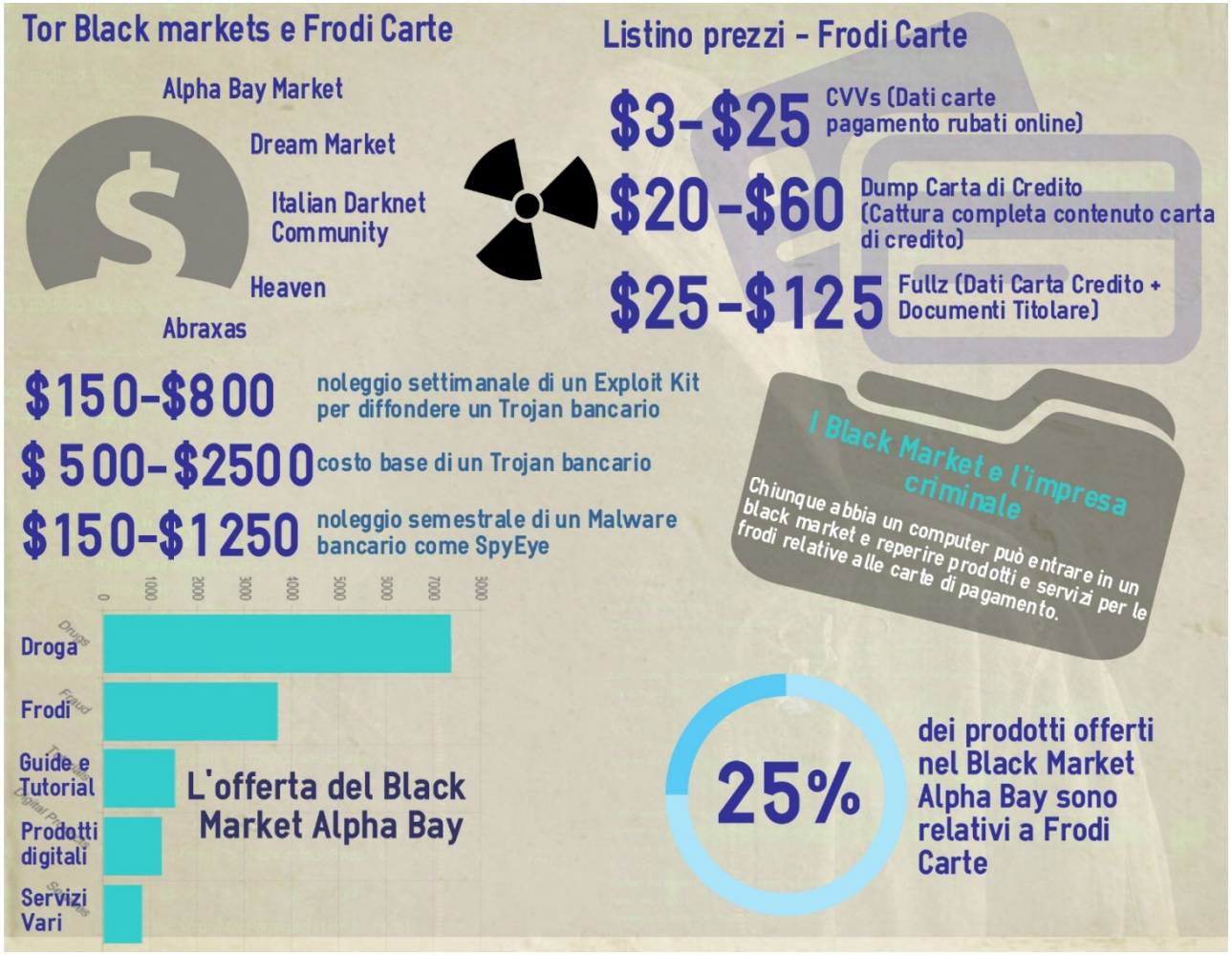
- richiedere in fase di presentazione del viaggiatore presso il banco della compagnia aerea, l'esibizione della carta di credito utilizzata per il pagamento del viaggio (riscontrato al momento con Alitalia);

- utilizzare, se possibile, i nuovi sistemi di sicurezza messi a disposizione da alcuni circuiti o emittenti.

Il settore pubblico, lato forze di polizia garantisce gli standard di prevenzione e repressione attraverso l'incremento della presenza del personale sul territorio nazionale nonché attraverso l'analisi dei dati "on line" (quest'ultima ad opera principalmente dei Compartimenti di Polizia Postale e delle Comunicazioni) di pari passo con l'addestramento del personale nello specifico settore.

Infografiche




Tor Black markets e Frodi Carte
Alpha Bay Market
Dream Market
Italian Darknet Community
Heaven
Abraxas
Listino prezzi - Frodi Carte
$3-$25 CVVs (Dati carte pagamento rubati online)
$20-$60 Dump Carta di Credito (Cattura completa contenuto carta di credito)
$25-$125 Fullz (Dati Carta Credito + Documenti Titolare)
$150-$800 noleggio settimanale di un Exploit Kit per diffondere un Trojan bancario
$500-$2500 costo base di un Trojan bancario
$150-$1250 noleggio semestrale di un Malware bancario come SpyEye
I Black Market e l'impresa criminale
Chiunque abbia un computer può entrare in un black market e reperire prodotti e servizi per le frodi relative alle carte di pagamento.
0
1000
2000
3000
4000
5000
6000
7000
8000
Droga
Frodi
Guide e Tutorial
Prodotti digitali
Servizi Vari
L'offerta del Black Market Alpha Bay
25%
dei prodotti offerti nel Black Market Alpha Bay sono relativi a Frodi Carte

Nota metodologica

Le Transazioni non riconosciute

Le statistiche sul fenomeno delle transazioni non riconosciute sono essenzialmente di due tipi: per numero e per valore in euro. Le statistiche non vengono fornite in termini assoluti ma in termini relativi. Possono essere espresse in rapporto a quelle genuine e in tal caso si parlerà di incidenze percentuali e si offrirà una misura del rischio di disconoscimento di una generica transazione, oppure, in rapporto a un loro valore osservato nel passato e si offrirà una misura della dinamica temporale del livello dei mancati riconoscimenti.

Le statistiche (relative o meno) sul numero e/o sul valore delle transazioni non riconosciute si riferiscono sempre ad un insieme specifico i cui lineamenti sono individuati e mantenuti invarianti nel tempo al fine di omogeneizzare i confronti delle serie storiche.

Le transazioni di riferimento sono esclusivamente quelle effettuate con carte di pagamento emesse da banche e/o da altri intermediari finanziari, autorizzati e vigilati dalla Banca di Italia[19], attraverso la sottoscrizione di un contratto con clienti titolari di qualsiasi nazionalità e avvenute in ogni Paese tramite l'uso di uno dei seguenti canali: POS, ATM e Internet.

Rientrano nell'insieme di osservazione le carte di credito, di debito e le prepagate.

Nell'insieme delle transazioni di riferimento rientrano anche quelle effettuate senza utilizzo diretto della carta di pagamento (*card-not-present*), sia su carte emesse da banche che da altri intermediari finanziari. Inoltre, qualificate come operazioni di prelievo, rientrano anche gli anticipi di contante con carte di credito.

All'interno di tali transazioni di riferimento sono considerate come non riconosciute tutte e solo quelle ritenute non riconosciute in modo definitivo, escludendo dunque i disconoscimenti annullati in un momento successivo a quello inziale.

Il valore economico di ogni transazione è espresso in euro; per quelle effettuate in altra valuta si opera una conversione sulla base dei tassi di cambio validi per il giorno in cui avviene la transazione e diffusi dalla Banca d'Italia (ex Ufficio Italiano Cambi).

La data in cui avviene la transazione è anche il riferimento temporale della transazione non riconosciuta e non si considera, quindi, come riferimento temporale la data di disconoscimento o di altro evento diverso. Le transazioni non riconosciute sono attribuite ad un determinato intervallo temporale (mese, semestre o anno) in base alla data giornaliera di riferimento, ovvero di transazione.

Oltre alla data ed al valore, alle transazioni non riconosciute vengono attribuite altre caratteristiche: causale di disconoscimento, tipo e luogo di transazione.

La causale di disconoscimento viene attribuita dall'ente segnalante (banca o intermediario finanziario emittente la carte e aderente al SIPAF) e può essere di sette tipi: *Carta contraffatta*, *Carta non ricevuta*,

[19] A questi si aggiungono alcuni Enti Segnalanti, che pur non avendo più l'obbligo continuano ad alimentare l'applicativo SIPAF.

Carta rubata, *Carta smarrita*, *Carta rubata con falsa identità*, *Utilizzo fraudolento del codice carta emessa* e *Utilizzo fraudolento della carta in internet*. Le modalità di attribuzione seguono il manuale operativo predisposto per l'alimentazione del SIPAF. Alle transazioni prive di causale non ne viene riattribuita alcuna e in fase di elaborazione statistica tali casi costituiscono *missing value*.

Il tipo di transazione, o canale, viene attribuito dall' UCAMP sulla base delle informazioni fornite dall'ente segnalante e può essere di tre tipi: *POS*, *Internet* e *Prelievi*[20]. La classificazione avviene attraverso un processo di selezione sequenziale. Le transazioni di tipo *Internet* sono quelle che l'ente segnalante ritiene avvenute su POS e che presentano come attributo località un indirizzo internet e/o come causale di disconoscimento *Utilizzo fraudolento della carta su Internet*. Seguono le transazioni su POS ritenute, da parte dell'ente segnalante, effettuate su POS ma non attribuite alle categorie merceologiche *Cash* o *Automated Cash Disburse*. Queste operazioni POS di tipo *Cash* vengono assegnate al tipo Prelievi, insieme a quelle transazioni ritenute, da parte dell'ente segnalante, effettuate su ATM[21]. Le transazioni ritenute effettuate su *POS* che non presentano valori per la località, per la causale di disconoscimento e per la categoria merceologica mantengono l'attributo di transazione su POS. In definitiva, ad ogni transazione non riconosciuta viene comunque assegnato un canale.

Le transazioni vengono articolate anche in relazione alla funzionalità debito/credito della carta utilizzata. Appartengono alla funzionalità credito le operazioni effettuate sui circuiti American Express, VISA, Mastercard, JCB e Diners; mentre le operazioni effettuate sui circuiti VPAY, VISA Electron, Postamat, Maestro e Bancomat/Pagobancomat vengono classificate come funzionalità debito.

La descrizione del luogo di transizione è fornita da due variabili: una in cui si distingue solamente Italia da Estero e l'altra in cui si descrive la nazione per le transazioni estere, o la località per quelle italiane. L'articolazione fra Italia ed Estero viene effettuata per ogni tipo di transazione in base a quanto attribuito dall'ente segnalante in termini di codici ISO delle varie nazioni. Le mancate valorizzazioni dello Stato in cui si è effettuata la transazione generano dei *missing value* che non vengono riattribuiti, salvo rimanere in capo alla modalità Estero.

Per le transazioni italiane si attribuisce la località, in particolare il comune, solamente per la tipologia prelievi. L'attribuzione viene effettuata dall'UCAMP mediante l'uso dei codici ABI e CAB relativi all'ATM su cui è avvenuto il prelievo e sulle modalità di raccordo, fornite dalla Banca di Italia, fra tali codici ed i comuni italiani, validi per l'anno in cui è avvenuta la transazione. Dai comuni si risale, poi, alle classificazioni per Provincia e/o Regione secondo i criteri indicati dall'ISTAT validi, anch'essi, per l'anno in cui è avvenuta la transizione. Per le transazioni avvenute su POS ma classificate, come detto, nei prelievi l'assenza dei codici ABI e CAB non consente l'applicazione del metodo esposto. In tali casi si elabora l'informazione relativa alla località in cui è avvenuta la transazione mediante un avanzato processo di *data quality*.

Ultima caratteristica di rilievo delle transazioni non riconosciute è la categoria merceologica. Per essa si fa riferimento alla classificazione MCC (Merchant Category Code) che si basa su un codice di 4 cifre elaborato e utilizzato da MasterCard/VISA per classificare le differenti tipologie di business. Accanto a tale classificazione che prevede circa 600 differenti tipologie, vi è anche una sua aggregazione che indica circa 30 tipologie di business.

[20] Attualmente non è possibile enucleare anche il canale *card non present*.

[21] Eventuali transazioni su POS che presentano località *Internet* e categoria merceologica *Cash* e affini vengono attribuite al tipo *Internet*.

Manomissioni ATM

Il fenomeno degli ATM manomessi è osservato in termini di numero degli eventi in un determinato intervallo di tempo e di area geografica e, nel rapporto statistico, non viene fornito in valore assoluto ma relativo. Esso è espresso in rapporto al numero degli ATM presenti nella stessa area geografica ed intervallo temporale. In tal caso si parlerà di tasso di manomissione specificando la natura dell'intervallo temporale di riferimento (mensile, semestrale, annuale). Il confronto fra tassi osservati in differenti aree geografiche e/o momenti temporali va effettuato sempre con lo stesso tipo di tasso (mensile, semestrale, annuale). Il tasso di manomissione semestrale, ad esempio, indica il numero di possibili attacchi che un singolo ATM può ricevere nell'arco di un semestre. Quando è pari all'1% significa che un singolo ATM riceve un attacco mediamente ogni 100 semestri; oppure significa che ogni 100 ATM, 1 riceve un attacco nell'arco di un semestre.

Il numero delle manomissioni può essere rapportato anche a quello osservato in un altro momento temporale (numero indice), in tal caso, offre una misura della dinamica temporale del livello assoluto degli attacchi.

Le statistiche, relative o meno, al numero delle manomissioni si riferiscono sempre ad un insieme specifico i cui lineamenti sono individuati e mantenuti invarianti nel tempo al fine di omogeneizzare i confronti delle serie storiche.

Le manomissioni di riferimento sono tutte quelle dichiarate come tali dall'ente segnalante (banca o intermediario finanziario aderente al SIPAF) e si riferiscono ad ATM collocati nel territorio italiano ed associati a banche e/o da altri intermediari finanziari autorizzati e vigilati dalla Banca di Italia.

La data di riferimento per la manomissione è la data di inizio dello stato di manomissione dell'ATM interessato ed è dichiarata dall'ente segnalante. Essa coincide o precede la data di scoperta della manomissione ed è una stima della data effettiva di manomissione (solitamente ignota).

Il luogo di riferimento per la manomissione è, naturalmente, quello in cui è collocato l'ATM e viene dichiarato dall'ente segnalante.

Oltre alla data ed al luogo, alle manomissioni vengono attribuite altre caratteristiche quali: tipologia manomissione e modalità cattura PIN. Entrambe vengono attribuite dall'ente segnalante in base ai criteri illustrati nel manuale operativo predisposto per l'alimentazione del SIPAF.

La tipologia manomissione può essere di cinque tipi: *Apposizione di skimmer*, *Manomissione del lettore di carte per accesso al locale interno ove è dislocato lo sportello stesso*, *Cash trapping*, *Card trapping*, *Altro*. La modalità cattura PIN può essere di quattro tipi: *Microtelecamera*, *Tastiera sovrapposta*, *Telecamera o macchina fotografica a distanza*, *Altro.* Alle manomissioni prive del tipo modalità cattura PIN non viene riattribuito alcun tipo di modalità e in fase di elaborazione statistica tali casi costituiscono *missing value*. Spesso in tali modalità rientrano casi in cui è avvenuta una manomissione ma non un cattura del PIN, come nel caso del *Cash trapping*.

Revoche convenzioni POS

Il fenomeno delle convenzioni revocate viene osservato essenzialmente in termini di numero degli eventi in un determinato intervallo di tempo e di area geografica e, nel rapporto statistico, non viene fornito in valore assoluto ma relativo. Esso può essere espresso in rapporto al numero complessivo delle convenzioni presenti nella stessa area geografica ed intervallo temporale. In tal caso si parlerà d'incidenza percentuale (%), specificando la natura dell'intervallo temporale di riferimento (mensile, semestrale, annuale). Il confronto fra incidenze osservate in differenti aree geografiche e/o momenti temporali deve essere effettuato sempre con lo stesso tipo di incidenza % (mensile, semestrale, annuale).

Il numero delle revoche può essere rapportato anche a quello osservato in un altro momento temporale (numero indice). In tal caso si offre una misura della dinamica temporale del livello assoluto delle revoche.

Le statistiche, relative o meno, al numero delle revoche si riferiscono sempre a un insieme specifico i cui lineamenti sono individuati e mantenuti invarianti nel tempo al fine di omogeneizzare i confronti delle serie storiche.

Le revoche di riferimento sono tutte quelle dichiarate come tali dall'ente segnalante (banca o intermediario finanziario aderente al SIPAF) e si riferiscono a convenzioni stipulate fra l'*acquirer*, istituzione finanziaria autorizzata e vigilata da Banca Italia, e l'esercente, dove il titolare di una carta di pagamento effettua la spesa. Gli esercenti di riferimento sono tutti quelli che operano nel commercio iscritti nel registro delle imprese delle Camere di Commercio. Ad un esercente convenzionato solitamente corrisponde un solo punto vendita e un solo terminale POS, ma può anche corrispondere più punti vendita sul territorio e/o più terminali POS.

Ad un esercente cui è stata revocata una convenzione può esserne assegnata, successivamente, una nuova Quindi, ad un esercente possono corrispondere, nel tempo, più revoche di convenzioni.

La data di riferimento per la revoca e la località sono quelle dichiarate dall'ente segnalante. La località è quella indicata per l'esercente convenzionato.

Ad una revoca viene attribuita, dall'ente segnalante, una causale che può essere di due tipi: *Coinvolgimento dell'esercente in attività sospetta* e *Motivi generici di sicurezza*.

Alle revoche prive di causali non viene riattribuito alcun tipo di causale e in fase di elaborazione statistica tali casi costituiscono *missing value*.

Confronti Internazionali

I dati relativi ai confronti internazionali sono disponibili presso i seguenti siti:

http://www.apca.com.au
http://www.banque-france.fr
http://www.cardwatch.org.uk
http://www.ecb.int
http://www.observatoire-cartes.fr
http://sdw.ecb.europa.eu
http://www.theukcardsassociation.org.uk

Il dato sul controvalore delle transazioni non riconosciute relativo a UK comprende anche le transazione avvenute per telefono e per posta, che vengono aggregate nel canale internet.

Il dato sul controvalore delle transazioni non riconosciute, disaggregato per tipologia di disconoscimento, fa riferimento, per la Francia, alle sole transazioni avvenute in Francia.

Per quanto riguarda l'Australia, i dati sul controvalore delle transazioni non riconosciute sono pienamente coerenti con le classificazioni adottate per l'Italia.

Glossario Termini

Bitcoin – Il Bitcoin è una moneta basata sull'utilizzo di un database distribuito tra i nodi della rete che tengono traccia delle transazioni e che sfrutta processi crittografici per gestire gli aspetti funzionali, come la generazione di nuova moneta e l'attribuzione di proprietà dei bitcoin. La rete Bitcoin consente il possesso ed il trasferimento anonimo delle monete, la gestione delle informazioni necessarie all'utilizzo della moneta elettronica possono essere salvati su un PC sotto forma di "portafoglio" digitale o mantenuti presso terze parti che operano in maniera non dissimile ad una banca.

Black Market – Sono luoghi in rete (e.g. Forum, piattaforme di e-commerce) gestiti da gruppi criminali per la commercializzazione di prodotti e servizi illegali, quali armi, droga e servizi di hacking.

Carding – Termine usato per indicare nell'ecosistema criminale la commercializzazione e lo scambio dei dati relativi alle carte di pagamento.

CVV - Il termine CVV è utilizzato dagli operatori dell'underground criminale specializzati nella commercializzazione delle carte di pagamento per indicare i record relativi alla carta e che possono includere il nome dell'intestatario, l'indirizzo dell'intestatario, la data di scadenza.

Dark net - Una dark net è una rete virtuale privata dove gli utenti connettono solamente persone di cui si fidano. Riferendo il crimine informatico, una dark net è un gruppo chiuso e privato di persone che interagiscono, molto spesso utilizzando reti basate su protocolli peer-to-peer (p2p).

Deep Web - Il Deep Web è la parte del World Wide Web non indicizzata dai principali motori di ricerca (e.g. Google).

Dump - Il termine Dump è utilizzato per indicare i dati grezzi immagazzinati nella banda magnetica di una carta di credito, informazioni di solito catturate mediante attività di "skimming" oppure attraverso l'uso di malware che infettano i sistemi di pagamento PoS.

Escrowing – E' un accordo tra acquirente e venditore nel quale il bene reale o virtuale è depositato da una parte presso il conto di una terza parte neutrale (agente), fino al completamento delle operazioni di pagamento da parte dell'acquirente. All'adempimento del pagamento, l'agente consegnerà all'altra parte il bene depositato.

FULLz – Il termine "Fullz" è utilizzato nell'ecosistema criminale per indicare l'insieme completo delle informazioni relative ad un particolare individuo che comprende i suoi dati personali, dati relativi alle carte di pagamento, il numero di previdenza sociale e una collezione di informazioni accessorie, tra cui eventuali bollette delle principali utenze dell'intestatario della carta.

Onion è uno pseudo-dominio di primo livello generico, utilizzato dalla rete Tor.

Tor (acronimo di The Onion Router) – Tor è un sistema di comunicazione anonima per Internet basato sulla seconda generazione del protocollo instradamento, noto come "onion routing."

Gruppo di lavoro

COORDINATORE DEL RAPPORTO

Antonio Adinolfi

GRUPPO OPERATIVO

Sogei S.p.A.:
Francesca di Brisco
Stefano Grossi
Alessandra de Castro
Massimo Palombi

G. di. F. - UCAMP
Angelo Raffaele Pisani
Marco Mastrorillo

GRUPPO CONSULTIVO

Banca d'Italia
Servizio Supervisione sui Mercati e sul Sistema dei Pagamenti, Divisione Strumenti e Servizi di Pagamento al Dettaglio

ABI – ASSOCIAZIONE BANCARIA ITALIANA
Ufficio Sistemi e Servizi di Pagamento

Enti aderenti al SIPAF

Contributi esterni

CISO Bit4ID
Ing. Pierluigi Paganini

SNAI S.p.A.
Dr Silvia Caprioli | Direttore New Business

G. di. F. - Nucleo Speciale Polizia Valutaria
Gruppo Antifalsificazione Monetaria ed Altri Mezzi di Pagamento

RISSC - Centro Ricerche e Studi su Sicurezza e Criminalità