



Frauds: some facts

DIREZIONE V:
Prevenzione dell'Utilizzo del Sistema Finanziario per Fini Illegali

UCAMP:
Ufficio Centrale Antifrode Mezzi di Pagamento

Newsletter n° 9 - Marzo 2015

In questo numero:

Frodi con le carte di pagamento

◆ Le transazioni non riconosciute: dinamica per categoria merceologica
p. 1

◆ Carte di pagamento: dalla violazione di dati alla monetizzazione
p. 4

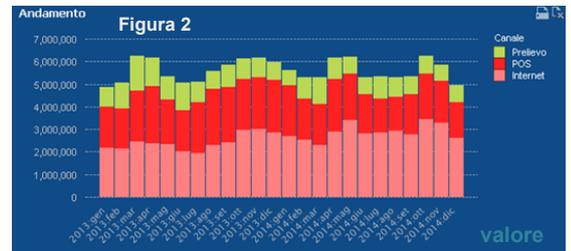
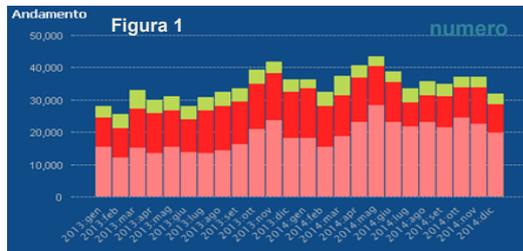
Euro

◆ La tutela dell'autenticità delle monete metalliche in Euro:
p. 8

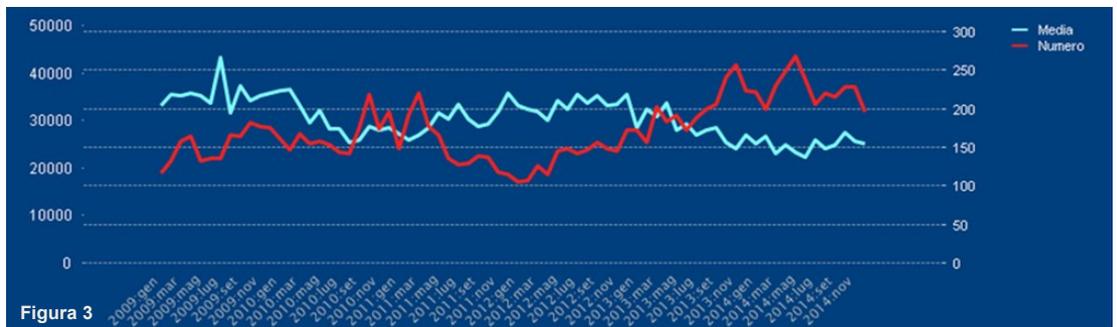
Le transazioni non riconosciute:

Dinamica per categoria merceologica - approfondimento di MCC- Travel air road.

Nel 2014 il numero delle operazioni non riconosciute (figura 1) è aumentato, lasciando inalterato il rispettivo controvalore in euro (figura 2). Si assiste ad un calo dell'importo medio per operazione. Lo stesso fenomeno accadde nel 2013.



Il grafico in figura 3 mostra che ad aprile 2013 l'importo medio della transazioni non riconosciute è stato di 208 euro, da quel momento in poi, il valore ha iniziato tendenzialmente a scendere fino a raggiungere il minimo di 138 euro (giugno 2014). Dal 2009 non si era mai scesi sotto soglia 150 euro, se non a marzo 2014. Tale valore è stato il più basso dall'inizio delle rilevazioni del fenomeno. specularmente al calo dell'importo medio, si è verificato un incremento del numero di operazioni. In 5 anni l'indice delle operazioni non aveva mai superato il valore di 33 mila. A maggio 2014 l'indice delle operazioni ha raggiunto il suo massimo storico, superando quota 40 mila.



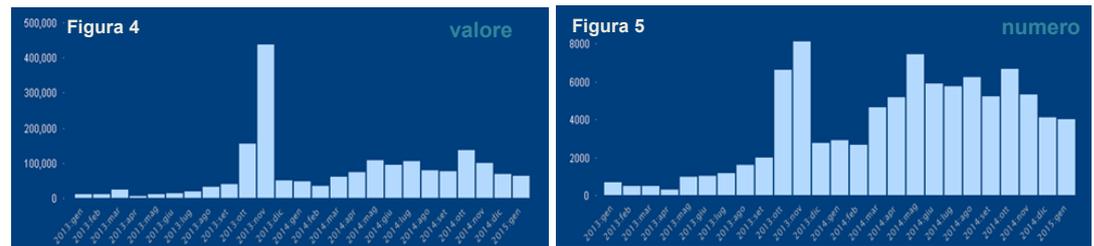
E' interessante sottolineare che le principali motivazioni da attribuire a tale fenomeno sono dovute in gran parte all'aumento delle operazioni sul canale internet, caratterizzate da importi medi per operazioni inferiori rispetto alle operazioni effettuate sul canale POS e prelievi.

¹Fonte SIPAF, Sistema Informatizzato Prevenzione Amministrativa Frodi Carte di Pagamento, Ministero dell'Economia e delle Finanze/Dipartimento del Tesoro. Analisi in collaborazione con Sogei.



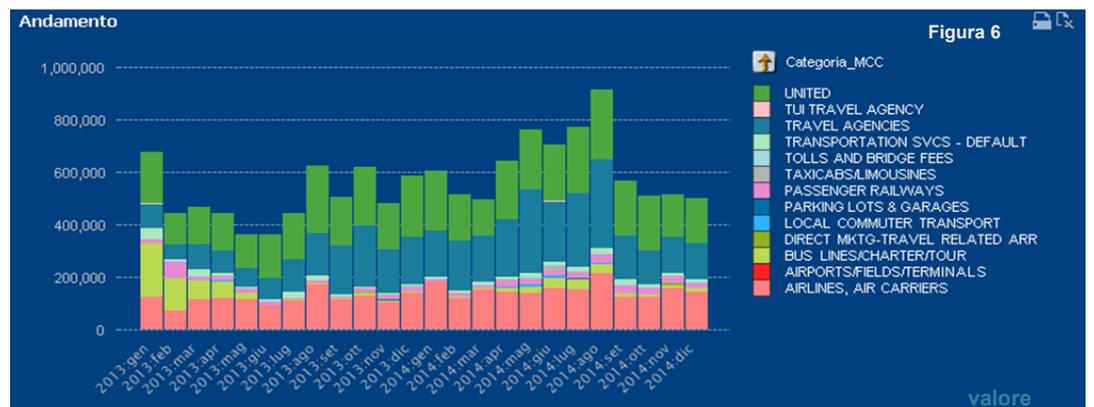
Questa lenta trasformazione della struttura interna delle transazioni non riconosciute rischia di mascherare il fenomeno delle frodi su carte di pagamento. Infatti, in termini di controvalore, si ha un contenimento dei livelli di rischio frode mentre in termini di numero il fenomeno continua a crescere, influenzando, negativamente, la percezione di sicurezza degli utenti.

Un caso esemplificativo è rappresentato dal fenomeno già evidenziato nella precedente newsletter, quando si è parlato di transazioni sconosciute relative ai sistemi di trasferimento denaro e acquisto di app per smartphone che utilizzano la piattaforma di acquisto on line di una delle principali aziende del settore.



Il controvalore di tali transazioni (figura 4) presenta una impennata esclusivamente nel mese di novembre 2013, per assestarsi ai livelli precedenti nei mesi successivi. A partire dalla primavera 2014 ha iniziato una lenta risalita, permanendo però al di sotto della soglia di guardia. Tuttavia, analizzando il grafico in termini di numero di operazioni (figura 5) viene messa in luce una realtà diversa. Difatti, escludendo i primi 3 mesi del 2014, il fenomeno in questione è rimasto sostanzialmente inalterato. Evidentemente i sistemi di contrasto attuati dagli operatori di settore, tollerano l'esistenza di operazioni di piccolo importo, ma la loro elevata frequenza ha prodotto, in termini di frodato, un controvalore superiore al milione di euro.

Il fenomeno delle frodi tuttavia continua ad essere un universo eterogeneo. Al suo interno è possibile trovare situazioni opposte a quella descritta precedentemente. Un esempio interessante è quello relativo alle transazioni effettuate per la categoria merceologica Travel air road (figura 6) che, a fronte di una sostanziale invarianza del numero di operazioni nel biennio 2013-14, presenta una significativa variabilità in termini di controvalore in euro. Infatti dal minimo di circa 400 mila euro, osservato nel periodo maggio-giugno 2013, si raggiunge in circa 12 mesi quota 900 mila euro. Le oscillazioni di Travel air road sono dovute principalmente alle tre principali sotto-categorie che la compongono: Travel Agency, United e Airlines/Air Carriers.



Interessante appare anche la distribuzione geografica (figura 7) del controvalore di queste operazioni, la quale non sembra riflettere la distribuzione generale.



Figura 7



Carte di pagamento - Dalla violazione di dati alla monetizzazione

Il furto e la commercializzazione di dati relativi a carte di pagamento rappresenta una delle principali attività dell'ecosistema criminale. L'elevato numero di violazioni perpetrate ai danni di aziende del settore Retail e finanziario nel 2014 ha reso disponibile nel black market un quantitativo impressionante di informazioni relative a carte di credito/debito. Tra le aziende colpite ricordiamo il colosso finanziario JPMorgan e le catene di negozi Target, Neiman Marcus ed Home Depot, ma la lista è davvero lunga. Tutti i dati confluiscono nell'underground criminale in cui complesse organizzazioni dedite ad attività illecite operano con profitti da capogiro.

Ma come operano queste organizzazioni? Quali sono le metodiche in uso per il furto delle informazioni relative alle carte di pagamento e come monetizzano i loro sforzi?

Ovviamente tutto ha inizio con il furto dei dati relativi ad una carta di pagamento che tipicamente comprendono il numero di carta e tutte le informazioni necessarie al completamento di una transazione finanziarie incluso il PAN (primary account number), nome del titolare, data di scadenza e codici di CVV (Card Validation Code) e CVC (Card Verification Code)

Le principali metodiche con le quali un criminale informatico ruba i dati relativi ad una carta di credito sono:

"Skimming" della carta di pagamento: I criminali utilizzano dispositivi in grado di leggere i dati relativi alle carte di credito, detti skimmer, quando l'utente effettua qualunque operazione presso gli sportelli automatici di una banca oppure effettua un pagamento presso un qualunque esercizio commerciale. Uno skimmer presenta la forma di una finta fessura per l'inserimento della carta e si sovrappone a quella legittima dell'ATM. Esistono numerosi tipi di skimmer, tutti accomunati dalla capacità di leggere la banda magnetica della carta per copiare i dati in essa memorizzati. I dati acquisiti possono essere memorizzati in una memoria locale oppure trasferiti in tempo reale attraverso un modem integrato nel dispositivo. Per la lettura del PIN esistono diverse opzioni per i criminali, tra cui l'uso di microcamere che registrano l'introduzione del codice oppure l'uso di tastiere finte che si sovrappongono a quella legittima.

Attacchi mediante l'uso di malware: Altro metodo comune per il furto di dati relative alle carte di credito è l'utilizzo di codici malevoli. Tipicamente i criminali informatici infettano i sistemi di pagamento presso esercizi commerciali, questi codici sono in grado di catturare le informazioni relative alle carte ogni qual volta il possessore effettua un acquisto. Esistono numerose tipologie di malware acquistabili su forum specializzati, tra i più popolari ricordiamo Dexter, vSkymmer, Alina e Chewbacca.

Phishing: Il phishing è una metodica estremamente diffusa e, sebbene sia elevato il livello di percezione della minaccia, risulta ad oggi uno dei metodi più efficaci per il furto di dati relativi alle carte di credito. La metodica evolve quotidianamente ed i criminali esplorano nuovi vettori per la diffusione di link malevoli a pagine che replicano i siti istituzionali di banche e servizi di pagamento. L'incidenza del phishing è in continuo aumento per la diffusione attraverso piattaforme mobile e social networks. Secondo i principali rapporti di sicurezza, i clienti di istituzioni finanziarie italiane sono tra i più colpiti da questa pratica.



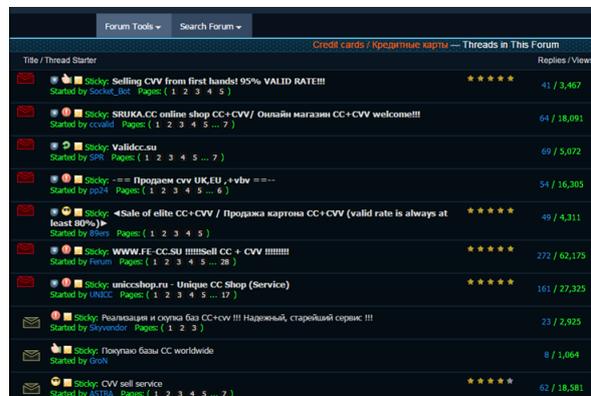
Una volta acquisite le informazioni relative alle carte di pagamento i criminali hanno principalmente due opzioni per monetizzare le loro attività, utilizzare i dati acquisiti per clonare le carte ed effettuare acquisti e pagamenti, oppure rivendere sul mercato underground i dati relativi alle carte di pagamento.

Questa seconda opzione è quella privilegiata da gruppi criminali, operativi soprattutto nell'Est Europa, che si specializzano per la vendita di dati relativi a carte di debito e credito di tutto il mondo. Così come per ogni altro prodotto in commercio, l'offerta criminale è molto variegata, i prezzi delle carte di pagamento dipendono da molteplici fattori, quali la nazionalità del titolare della carta, eventuale garanzia offerta sulla validità della carta, la disponibilità finanziaria associata alla carta e limiti di spesa associati.

Dove acquistare i dati relativi a carte di pagamento e quanto costano?

Non esiste un luogo specifico sul web in cui è possibile acquistare lotti di carte di pagamento, in rete vi sono innumerevoli siti web e forum in cui è offerta la preziosa merce.

Tra le comunità più attive nella commercializzazione di dati relativi a carte di pagamento potremo citare embargo.cc e netsky.bz, mentre numerosi gruppi prediligono forum e black market nel Deep Web, citiamo ad esempio la prolifica EVO community presente nella rete TOR. Alcuni dei siti web ritenuti più affidabili forniscono ai propri utenti servizi di escrowing (Acconto di garanzia) e premiano l'affidabilità dei propri venditori attraverso meccanismi di rating della reputazione basati su feedback.



Title / Thread Starter	Replies / Views
Stickyp: Selling CVV from first hands! 95% VALID RATE!!! Started by Sockel_Sat Pages: (1 2 3 4 5)	41 / 3,467
Stickyp: SRUKA.CC online shop CC+CVV/ Онлайн магазин CC+CVV welcome!!! Started by ccvald Pages: (1 2 3 4 5 ... 7)	64 / 18,091
Stickyp: Validcc.su Started by SPR Pages: (1 2 3 4 5 ... 7)	69 / 5,072
Stickyp: == = Продаж cvv UKEU + vbn == = Started by p024 Pages: (1 2 3 4 5 ... 6)	54 / 16,365
Stickyp: «Sale of elite CC+CVV / Продажа картрона CC+CVV (valid rate is always at least 80%)» Started by Sockel Pages: (1 2 3 4 5)	49 / 4,311
Stickyp: WWW.FE-CC.SU !!!Sell CC + CVV !!!!!! Started by Forum Pages: (1 2 3 4 5 ... 28)	272 / 62,175
Stickyp: uniquecc.ru - Unique CC Shop (Service) Started by UNICC Pages: (1 2 3 4 5 ... 17)	161 / 27,325
Stickyp: Продажи и услуги баз CC+CVV !!! Надежный, старейший сервис !!! Started by Sockendor Pages: (1 2 3)	23 / 2,925
Stickyp: Покупаю базы CC worldwide Started by G001	8 / 1,054
Stickyp: CVV sell service Started by ACTIVA Pages: (1 2 3 4 5 ... 7)	62 / 18,581

Il prezzo delle informazioni relative alle carte di pagamento si è progressivamente ridotto nel corso degli ultimi 3 anni, tale flessione è stata principalmente causata dalla disponibilità di dati relativi a milioni di carte derivanti dai numerosi incidenti. Il prezzo dei dati relativi a carte di credito/debito statunitensi arriva fino a 5 dollari mentre per una carta relativa ad un cittadino europeo si può

arrivare a spendere una cifra che varia dai 5 ai 15 dollari, qualora i dati includano il contenuto delle tracce presenti nella banda magnetica della carta si potrebbe arrivare a pagare sino a 28 \$ per pezzo. L'offerta relativa a lotti di carte di pagamento rubate si completa nell'underground criminale con una ampia gamma di informazioni accessorie che possono essere utilizzate per realizzare frodi finanziarie più evolute. Nella quasi totalità dei forum specializzati nella vendita di carte di credito è possibile acquistare quello che in genere si indica con il termine "Fullz", ovvero una collezione completa di informazioni relative ad un particolare individuo che include i suoi dati personali, dati relativi alle carte di pagamento, numero di previdenza sociale, una collezione di informazioni accessorie e persino una bolletta di una utenza. Il pacchetto completo consente ai criminali di acquisire l'identità della vittima per condurre diverse tipologie di frodi finanziarie. Queste informazioni possono essere utilizzate dalle gang di criminali per aprire conti correnti di appoggio utilizzati per trasferire temporaneamente le somme di denaro ricavate grazie alle attività illecite.



Una volta in possesso dei dati relative alle carte di pagamento rubate oppure di loro cloni, come guadagnano denaro i criminali?

Il processo di monetizzazione delle carte di pagamento rubate è definito Cash-out, tipicamente i criminali una volta in possesso dei dati relativi a lotti di carte li utilizzano per acquisti di prodotti di elevato valore come componenti elettronici (e.g. smartphone, laptop e gaming console) oppure abiti costosi. Gli acquisti sono effettuati su piattaforme di e-commerce con account creati ad hoc.

Tracciare gli acquisti è spesso impossibile per le forze dell'ordine, in molti casi ci si accorge che la merce è stata pagata con carte di credito rubate solo una volta che la merce è già giunta a destinazione. La merce acquistata è poi rivenduta al parallelo a prezzi scontati.

Molto spesso sono utilizzate figure intermedie note come "Mules", ovvero persone che ricevono la merce e la rispediscono, anche all'estero, in cambio di facili guadagni.

Spesso le organizzazioni criminali si rivolgono a gruppi specializzati, detti "Drops for stuff", nella spedizione di beni verso i paesi in cui i gruppi operano. Tali reti contano sul supporto di residenti nella comunità Europea che ricevono la merce e la rispediscono. Mentre i "mules" possono essere anche singoli individui, i "drops" sono solitamente organizzati in gruppi in grado di processare numerose spedizioni al giorno. Tali figure, di solito residenti nello stesso paese dei criminali, sono essenziali per far arrivare la merce oltre i confini e rendere difficile il tracciamento delle spedizioni.

Spesso i retailer non spediscono merce all'estero oppure verso quei paesi che notoriamente ospitano organizzazioni dedite a questa tipologia di crimine, come Est Europa, Russia e Nord Africa. Per questo motivo la merce è indirizzata ai "mules" che provvedono a riorganizzare le spedizione verso l'estero oppure verso indirizzi utilizzati dalle organizzazioni come centri di smistamento. Una volta che la merce giunge a destinazione viene quindi rivenduta su vari canali, tra cui piattaforme di commercio elettronico consumer to consumer, come eBay.

Le forze dell'ordine tipicamente seguono spostamenti e transazioni finanziarie in cerca di tracce che possano evidenziare attività fraudolente, per questo motivo i criminali spesso utilizzano sistemi di pagamento alternativo come il Bitcoin, ritenuti più sicuri nell'ecosistema criminale.

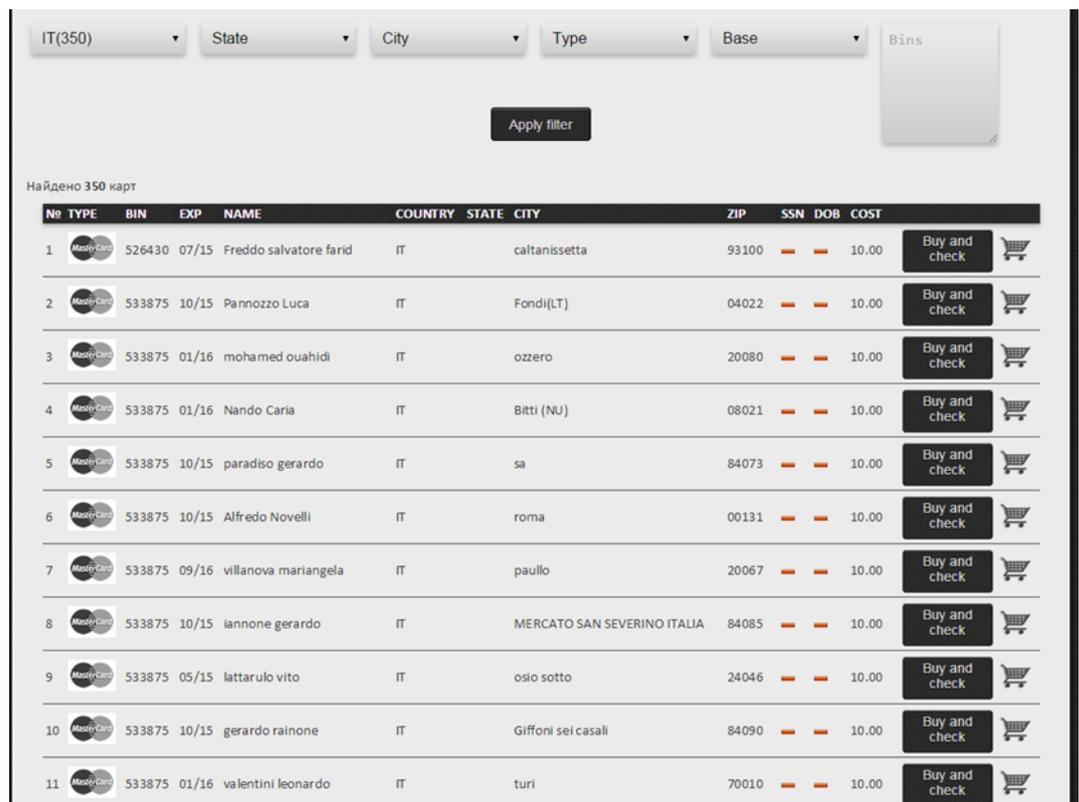


Altro schema di monetizzazione, adottato dalle organizzazioni criminali, consiste nella clonazione fisica delle carte che sono distribuite a gruppi di individui, detti "runner", il cui compito è quello di stampare fisicamente le carte a partire dai dati rubati attraverso malware e procedere all'acquisto di merce dall'alto costo.



Conclusioni

Il furto e la commercializzazione delle carte di pagamento e dei dati relativi continuano ad essere tra le principali attività dell'ecosistema criminale. Il crimine informatico si sta specializzando nella personalizzazione dell'offerta affiancando, ai dati rubati relativi alle carte, informazioni supplementari che consentono di aumentare l'efficacia dell'azione criminale, incrementando i profitti e riducendo i rischi. Proprio mentre ero impegnato nella stesura di questo post, ho ricevuto notizie dai colleghi dell'azienda statunitense IntelCrawler della disponibilità nel black market di lotti di carte relative ad utenze italiane.



IT(350) State City Type Base Bins

Apply filter

Найдено 350 карт

Nº	TYPE	BIN	EXP	NAME	COUNTRY	STATE	CITY	ZIP	SSN	DOB	COST	Buy and check
1	Masbi-CARD	526430	07/15	Freddo salvatore farid	IT		caltanissetta	93100	—	—	10.00	Buy and check
2	Masbi-CARD	533875	10/15	Pannozzo Luca	IT		Fondi(LT)	04022	—	—	10.00	Buy and check
3	Masbi-CARD	533875	01/16	mohamed ouahidi	IT		ozzero	20080	—	—	10.00	Buy and check
4	Masbi-CARD	533875	01/16	Nando Caria	IT		Bitti (NU)	08021	—	—	10.00	Buy and check
5	Masbi-CARD	533875	10/15	paradiso gerardo	IT		sa	84073	—	—	10.00	Buy and check
6	Masbi-CARD	533875	10/15	Alfredo Novelli	IT		roma	00131	—	—	10.00	Buy and check
7	Masbi-CARD	533875	09/16	villanova mariangela	IT		paulo	20067	—	—	10.00	Buy and check
8	Masbi-CARD	533875	10/15	iannone gerardo	IT		MERCATO SAN SEVERINO ITALIA	84085	—	—	10.00	Buy and check
9	Masbi-CARD	533875	05/15	lattarulo vito	IT		osio sotto	24046	—	—	10.00	Buy and check
10	Masbi-CARD	533875	10/15	gerardo rainone	IT		Giffoni sei casali	84090	—	—	10.00	Buy and check
11	Masbi-CARD	533875	01/16	valentini leonardo	IT		turi	70010	—	—	10.00	Buy and check

La scoperta dimostra che gli istituti finanziari del nostro paese, così come quelli di ogni altro stato sono sotto assedio da parte di complesse organizzazioni criminali, per questo motivo è cruciale il monitoraggio di tutti i processi descritti e la condivisione di informazioni tra aziende private, istituti di credito ed autorità.

Pierluigi Paganini



La tutela dell'autenticità delle monete metalliche in Euro: l'attività del C.N.A.C. e la stretta collaborazione con l'UCAMP

Le monete metalliche in Euro sono prodotte con caratteristiche anticounterfeiting atte a tutelare al massimo l'autenticità e anticounterfeiting, a garanzia del cittadino che le utilizza. Ciò nonostante, l'Europa ha investito e continua ad investire risorse per la massima tutela del cittadino contrastando il fenomeno della falsificazione in ogni sua forma. Sin dal 2002 la normativa europea (Reg. UE 1338/2001) ha stabilito la costituzione di un Centro di analisi in ciascun paese membro, denominato C.N.A.C., acronimo inglese di "centro nazionale di analisi delle monete" (l'autorità nazionale preposta all'analisi dei falsi rinvenuti all'interno dei territori italiano, vaticano e sanmarinese).

In Italia, il C.N.A.C. è stato costituito nel 2001 all'interno della Zecca dello Stato dell'IPZS, l'officina monetaria produttrice delle monete in Euro per l'Italia, San Marino e Vaticano. Al C.N.A.C. spetta il compito di effettuare perizie su tutte le monete metalliche sospette di falsità rinvenute in circolazione dai cosiddetti "gestori professionali del contante" (quali banche, poste, soggetti che svolgono attività di custodia, trasporto e trattamento del denaro, cambiali) o dalle forze di Polizia. All'attività di perizia sia associa anche lo studio e la catalogazione di ogni genere di falsificazione, contribuendo ad arricchire un archivio europeo di informazioni utilissime alle Forze dell'Ordine che si occupano di contrastare il fenomeno della contraffazione. Gli elementi delle classi alimentano uno specifico database gestito dalla Banca Centrale Europea. Tali informazioni sono disponibili anche all'UCAMP che svolge un ruolo chiave nella raccolta dei dati a fini dell'analisi statistica sulla falsificazione dell'euro.

Con la legge n. 27 del 24/03/2012 art. 97 (pubblicata in GU n. 71 del 24/03/2012) al C.N.A.C. sono stati attribuiti ulteriori compiti e funzioni derivanti dall'applicazione del Regolamento UE 1210/2010 che introduce il concetto di autenticazione del circolante metallico da parte dei gestori professionali del contante. In base alle nuove disposizioni, il C.N.A.C., continuando a svolgere l'attività di raccolta e analisi delle monete sospette di falsità, è stato incaricato di effettuare verifiche sul corretto funzionamento delle apparecchiature da utilizzare per il ricircolo delle monete, di formare il personale coinvolto nel processo di autenticazione e di svolgere controlli ai gestori del contante (cosiddette "visite ispettive"), effettuando nel contempo i controlli sulle monete ritirate dalla circolazione in quanto ritenute non più idonee, per valutarne la rimborsabilità.

Il Centro di analisi negli anni ha registrato un'espansione enorme in termini di attività: iniziando con meno di cento perizie nell'anno 2002, nel 2014 si sono superate le 20.000 perizie, contando nello stesso anno il maggior numero di monete contraffatte periziate rispetto a tutti gli altri paesi europei. Notevole è stata inoltre l'attività di supporto ai gestori del contante ma soprattutto alle forze di Polizia. Con i primi si sono svolti numerosi corsi di formazione ed informazione finanziati da fondi comunitari (progetto "Pericles") ed è stato reso disponibile, nel sito dell'Istituto, un videocorso per formare il personale coinvolto nel processo di autenticazione. Con le forze di Polizia si è collaborato negli anni a fornire supporto tecnico e scientifico per indagare sulle tecniche di produzione delle Zecche clandestine, che solo in Italia ammontano alla metà di quelle ritrovate a livello europeo ed extraeuropeo.



Curiosità: come si svolge l'analisi dei falsi.

Come già accennato, la perizia riguarda l'accertamento del falso e la sua classificazione. Con questo secondo termine si indica un'attività complessa che si esplica dopo l'accertamento di un falso. Consiste nell'individuare le caratteristiche "rappresentative" di ogni esemplare al fine di individuarne la cosiddetta "classe" di appartenenza. Scopo ultimo di tale processo, che richiede analisi strumentali e visive comparative, è quello di creare una "mappa" dei falsi riconducibili ad una specifica produzione e quindi alla Zecca clandestina che le ha prodotte.

Le visite ispettive ed il ricircolo delle monete

L'introduzione del controllo delle monete, chiamato processo di "autenticazione", ha come scopo la ripulitura del circolante ed è volto ad eliminare dalla circolazione monete sospette di falsità e monete non più adatte alla circolazione, sia a causa della normale usura dovuta all'utilizzo, sia per eventi che ne abbiano alterato le caratteristiche originarie. A garanzia del corretto adempimento della norma, il C.N.A.C. è chiamato a svolgere attività di verifica ai gestori del contante, tramite i cosiddetti "controlli sul posto", in analogia con quanto già in essere sulle banconote in euro, con i controlli regolarmente svolti dalla Banca d'Italia.

L'importanza strategica dello scambio delle informazioni tra CNAC e UCAMP

La stretta collaborazione che da sempre ha contraddistinto i rapporti istituzionali tra CNAC ed UCAMP, entrambi autorità nazionali competenti nella lotta contro la contraffazione dell'euro, ha portato di recente alla progettazione di un sistema di scambio telematico atto rendere il processo comunicazione più celere ma soprattutto più attendibile.

Grazie al nuovo portale SIRFE, a cui tutti i gestori del contante sono tenuti ad accreditarsi per fornire ad UCAMP tutte le informazioni sui sospetti falsi rinvenuti, sarà presto possibile riconciliare le informazioni relative alle monete inoltrate al CNAC con l'esito delle relative perizie. Sarà infatti possibile nel prossimo futuro ricevere da parte del CNAC i dati delle segnalazioni in formato elettronico e mettere a disposizione dell'UCAMP gli esiti delle perizie con analogo sistema, mettendo così in pensione il sistema di fax ormai superato sia per tecnologia sia per efficienza ed affidabilità.

Emilio Bufacchi

©Ministero dell' Economia e delle Finanze, 2015
Dipartimento del Tesoro
Direzione V – Ufficio Centrale Antifrode Mezzi di Pagamento

Responsabile: Dott. Antonio Adinolfi
Dirigente Ufficio VI (UCAMP)

Via XX Settembre, 97
00187 – Roma
Tel. 0647613535
Web: <http://www.dt.tesoro.it>

Tutti i diritti riservati. E' consentita la riproduzione ai fini didattici
E non commerciali, a condizione che venga citata la fonte.

ISSN

